PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

M A E S T R Í A E N R E D E S D E C O M U N I C A C I O N E S

ANÁLISIS DE MÉTODOS CRIPTOGRÁFICOS PARA LA GESTIÓN DE FIRMAS Y CERTIFICADOS DIGITALES DENTRO DE UN CONTEXTO DE SUPERVISIÓN (SBS) PARA ENFRENTAR LOS NUEVOS REQUERIMIENTOS DE SEGURIDAD INFORMÁTICA

MARÍA DE LOS ÁNGELES VALLE C.

"TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN REDES DE COMUNICACIONES"

QUITO, 20 DE FEBRERO DE 2014.

Dedicatoria

A mis Padres Margarita y Lenin Estuardo por darme la vida y porque ellos soñaron con este logro y que hoy se hace realidad, gracias a su esfuerzo, sacrificio y abnegado amor; a mis hermanos por haber confiado siempre en mí y por apoyarme en los momentos más difíciles. Con mucho cariño para todos ellos.

María de los Ángeles

Agradecimiento

Deseo expresar mis más profundos agradecimientos a todos los docentes, ayudantes, administrativos, compañeros y amigos que durante los años de formación universitaria compartieron conmigo momentos de alegría y tristeza.

De manera particular también quiero hacer llegar mi agradecimiento a María Soledad Jiménez por su apoyo constante, su gran paciencia y por sus valiosas sugerencias y aportes que sirvieron para la elaboración del presente trabajo. A mis revisores Gustavo Xavier Chafla y Francisco Balarezo por su colaboración y el tiempo dedicado a la revisión de este proyecto de tesis.

Muchas gracias a Todos!

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

IV

CAPÍTULO I

MARCO REFERENCIAL

Este Capítulo cubre un análisis de los fundamentos básicos de la seguridad informática bajo los Esquemas de Supervisión dados por la Superintendencia de Bancos y Seguros (Confidencialidad, Disponibilidad, Integridad, Irrefutabilidad) sobre los tipos de seguridad existentes tanto en la seguridad física como en la seguridad lógica. Además se plantea lineamientos básicos como propuesta regulatoria sobre el análisis de la normativa vigente.

1.1.- EVALUACIÓN DE LA SITUACIÓN ACTUAL DE LOS SGSI DE LAS INSTITUCIONES FINANCIERAS [1] [2]

La adopción de un Sistema de Gestión de Seguridad de Información (SGSI) en el país no está desarrollado en las instituciones financieras, principalmente debido a la escasa inversión efectuada, se estima que el 15% de las instituciones financieras, de un total de 97 entidades controladas por la Superintendencia de Bancos; han definido actividades mínimas con el fin de establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI) integral. Sin embargo, no se ha planteado un estudio paralelo de las posibilidades y riesgos que permitan definir controles sobre la seguridad de la información, destacando:

a. *Seguridad lógica.-* Se refiere a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. Controles especiales sobre utilidades del sistema y herramientas de auditoría.

b. *Seguridad del personal.-* Orientado a reducir los riesgos de error humano, comisión de ilícitos contra las entidades o uso inadecuado de instalaciones.

c. *Seguridad física y ambiental.-* Destinado a impedir accesos no autorizados, daños e interferencia a las instalaciones e información del organismo.

d. *Inventario de activos y clasificación de la información*.- Permite mantener un inventario de activos asociados a la tecnología de información y asignación de responsabilidades respecto a la protección de estos activos, así como una clasificación de la información, que debe indicar el nivel de riesgo existente para la entidad y las medidas apropiadas de control que deben asociarse a las clasificaciones.

e. *Administración de las operaciones y comunicaciones.-* Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

f. *Adquisición, desarrollo y mantenimiento de sistemas informáticos.-* Cubre la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios: análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales; técnicas de encriptación sobre la información crítica que debe ser protegida; controles sobre la implementación de aplicaciones antes del ingreso a producción, así como control de cambios y vulnerabilidades técnicas.

g. *Procedimientos de respaldo.-* Define los procedimientos que incluyen las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas

medidas serán coherentes con la estrategia de continuidad de negocios de la entidad.

h. *Gestión de incidentes de seguridad de información.-* Permite asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, considerando los siguientes aspectos: procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información, así como procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

Una de las razones más importantes para implementar un SGSI es la de atenuar los riesgos propios de los activos de información de las entidades financieras. Una acertada identificación de tales activos, una definición correcta del alcance y unas políticas de seguridad claras y completas, son determinantes para la correcta implantación del SGSI.

Un SGSI en una entidad financiera no puede ajustarse cada vez que se genera un incidente de seguridad, pues la labor de quienes tienen la función de gerenciar la seguridad de la información en las entidades financieras no puede ser únicamente la de administrar los controles creados para cada situación de riesgo. Se debe actuar de manera proactiva para tratar de anticiparse a tales hechos; y, para ello el SGSI debe estar en capacidad de ayudar a la alta dirección en la definición de acciones que mitigan los riesgos sobre los activos más críticos, sin tener que esperar a que los eventos ocurran.

La implantación de un SGSI requiere de una alta participación a nivel estratégico y su papel es protagónico, pues dicha implantación es un proyecto que reclama tiempos, actividades, recursos, por lo tanto la alta gerencia debe

conocer y ser consciente de la importancia de la seguridad y de las consecuencias de no llevar a cabo su implementación.

Por otro lado, con el incremento de las exigencias del negocio y la evolución de los marcos regulatorios, la seguridad de información se ha convertido en una prioridad para las entidades que prestan servicios en la industria financiera.

Del análisis a la efectuado y resultado de las diversas auditorias de riesgo tecnológico ejecutas por la Superintendencia de Bancos y Seguros se tiene que las instituciones controladas se han vuelto más proactivas en implementar medidas de seguridad innovadoras y en crear mayor conciencia con respecto a la seguridad de la información dentro de su organización. Asimismo, gran parte de las entidades enfrentan un gran desafío:

> *Establecer un equilibrio entre los costos de las iniciativas referentes a seguridad de la información y la materialización de las amenazas e implementación de nuevas tecnologías.*

Debemos considerar además que en el sector financiero siguen predominando las organizaciones de seguridad centralizadas frente a modelos distribuidos o federados, presentes en compañías de otros sectores. Dentro del análisis efectuado sobre las instituciones controladas por la Superintendencia de Bancos se tiene que:

- La percepción de la efectividad de la función de seguridad por parte de las entidades financieras ha mejorado, aunque sólo una de cada tres entidades la consideran muy efectiva.

- El 30% de las entidades financieras cuentan con mecanismos y herramientas específicas para identificar y reportar actividades sospechosas que surjan en la organización, pero tres de cada cinco instituciones no hace nada para cubrir sus vulnerabilidades de seguridad. En el Ecuador la tendencia es reactiva en este sentido en comparación con otros países de la región.
- Las tecnologías líderes (más implantadas) continúan siendo las soluciones de antivirus, cortafuegos y filtrado de spam, destacando la próxima implantación de otras como los sistemas de gestión de vulnerabilidades, el control de accesos a red o la gestión de registros de seguridad.
- La gestión de accesos e identidades y la protección de datos se han convertido en las prioridades de las entidades en materia de seguridad de la información.
- La gran mayoría de las entidades tiene o tendrá una nueva estrategia de seguridad en los próximos doce meses, pero pocas admiten que esté debidamente alineada con los objetivos de negocio.
- Por sectores, las entidades de inversión están más preocupadas por el Gobierno de seguridad[1], considerando que dos de las mayores preocupaciones son el refuerzo del cumplimiento de seguridad y la continuidad de negocio.
- Durante el último año las entidades financieras han percibido un aumento de la sofisticación de los ataques contra la seguridad. En cuanto a las pérdidas estimadas de las entidades consultadas fruto de los ataques recibidos en el último año, una de cada cuatro afirmó no haber sufrido pérdidas, un 22% estimó la cifra en menos de 200.000 dólares y solo 1 de cada 10 afirma no medir la pérdida económica.

[1] ***Gobierno de Seguridad.-*** Disciplina que dice relación con la forma en la que la alta dirección de las organizaciones dirige la evolución y el uso de la seguridad de la información, y se considera una parte del denominado "Gobierno Corporativo", centrada en el desempeño, administración de riesgos y control de la seguridad de la Información.

Dentro de las expectativas a corto y mediano plazo es primordial que la instituciones financieras elaboren un programa de seguridad de información muy potente que incluya una revisión activa del Directorio y de la Gerencia sobre temas de visión general, políticas y procedimientos, sistemas de medición y monitoreo, y controles internos paralelos. El Directorio debe asegurarse de que la inversión en sistemas de protección de datos sea adecuada al nivel de riesgos que se enfrentan en las operaciones. Además, tomando como referencia las recomendaciones dadas por el *Federal Reserve Board*, en su documento *Sound Practices Guidance for Information Security for Networks* (2011), se tiene que:

- *Se debe poner atención especial a la seguridad de la red interna:* Este tema puede ser considerado de menor riesgo para los Directivos de una entidad financiera en relación con las amenazas externas (Internet), pero los ataques provenientes desde el interior de la red de la entidad pueden ser los más dañinos, al tener el personal del banco y los consultores externos acceso a recursos críticos del sistema.
- *La información confidencial debe ser encriptada:* Dado que la transmisión de datos de un punto a otro de la red, se da a través de líneas accesibles públicamente, la información sensible que se envíe a través de ellas debe estar protegida para que sólo el destinatario pueda interpretarla.
- *Las conexiones con Internet deben construirse cuidadosamente*: Cuantos más servicios en línea se ofrezcan, más posibilidades de ataques existirán. El mayor riesgo de las conexiones en Internet es el de permitir el acceso a la red interna del banco. Por lo tanto, es crucial comprobar la seguridad de todos los sistemas desde donde el banco intercambia información con la red, para impedir vacíos que permitan accesos inadecuados a los sistemas internos, así como fallas en la provisión de servicios externos.

- *La Gerencia debe evaluar cuidadosamente los costos y beneficios de implementar sistemas de seguridad que minimicen los riesgos existentes.*

La implantación y operación de un SGSI ofrece ventajas para las entidades bancarias al disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente, contar con un proceso definido para evaluar, implementar, mantener y administrar la seguridad de la información, diferenciarse en el mercado frente a otras entidades financieras, satisfacer requerimientos de clientes, proveedores y organismos de control, formalizar las responsabilidades operativas y legales de los usuarios internos y externos de la Información y ayuda en el cumplimiento de las disposiciones legales nacionales e internacionales. Aunque el procedimiento para la implementación de un SGSI puede parecer genérico en su aplicación para cualquier sector productivo, el recorrido del proceso aplicado al sector financiero afirmará que para este sector su incidencia y su impacto es mayor que para otros sectores, demandando mayor rigurosidad en su aplicación.

1.2.- ANÁLISIS DE GESTIÓN Y RIESGOS DE SEGURIDAD [2]

Si bien el propósito de este proyecto de tesis no es el de dar los lineamientos necesarios para una adecuada Gestión de Riesgos, es pertinente hacer mención a los temas más relevantes identificados por organismos internacionales, que pueden ayudar a una adecuada comprensión de los mecanismos al alcance de las instituciones financieras para protegerse de dichos riesgos. Los temas que se verán a continuación han sido recogidos de distintos documentos publicados por el Comité de Basilea, el *Federal Deposit Insurance Corporation* y el *Federal Reserve*. Sin embargo, la responsabilidad de identificación y gestión adecuada de los riesgos que efectivamente enfrentan las

entidades financieras en sus operaciones dependen mucho del tipo de operaciones adoptadas, por lo que esta labor, en último caso, es de entera responsabilidad de dichas entidades, los que tendrán que adaptar las recomendaciones dadas a sus propios esquemas operativos.

Describiendo más en detalle el tipo de riesgos que afrontan las operaciones financieras, esta sección se enfocará principalmente en el riesgo operacional (entendido en el modo amplio de posibilidad de falla en los sistemas de procesamiento de las operaciones de las entidades, así como de errores o perjuicios cometidos por el personal de la entidad al procesar dichas operaciones), el riesgo legal (posibilidad de verse afectado por posibles violaciones de leyes, reglas, regulaciones o prácticas sugeridas, sobre todo cuando los derechos y responsabilidades de las partes no están bien definidas) y el riesgo reputacional (posibilidad de enfrentar una opinión pública significativamente negativa, que pueda llevar a una pérdida crítica de clientes o de fondeo). Existen otros riesgos que también se ven potenciados de alguna manera con las operaciones financieras, pero el efecto es similar al de cualquier otro nuevo canal o instrumento, por lo que no es necesario enfocarse mucho más allá de las normas prudenciales que se practican actualmente. De todas maneras, hacia el fin de esta sección se examinará, de manera breve, la posible exposición de las operaciones de banca electrónica frente a las demás clases de riesgo identificadas.

La Vulnerabilidades de las Entidades Financieras, son identificadas tanto en sistemas de recepción, procesamiento, ejecución y/o almacenamiento de la información, así como aplican al personal encargado de su manejo. Las consideraciones sobre el tema de seguridad son muy importantes, dado que las entidades pueden sufrir ataques sobre sus sistemas o productos. También puede

aparecer riesgo operacional debido a mal uso por parte de los clientes, o por sistemas de banca electrónica o de dinero electrónico inadecuadamente implementados. Como se verá, buena parte de los riesgos que corresponden a esta categoría son aplicables tanto a las operaciones de banca electrónica como a las de dinero electrónico.

2.2.1.- Riesgos de Seguridad

Estos riesgos tienen en cuenta los controles que se hacen sobre los sistemas centrales de contabilidad, registro y manejo de información relevante para el negocio financiero, infraestructura, así como la información que se transmite a terceros y, en el caso de dinero electrónico, las medidas para disuadir y detectar falsificaciones. Por lo mencionado, controlar el acceso a los sistemas informáticos de las instituciones financieras se vuelve cada vez más complejo debido a las mayores capacidades de las computadoras actuales, dispersión geográfica de puntos de acceso y el uso de vías de comunicación diversas, sobre todo de redes públicas como la Internet. Es importante notar que una brecha de seguridad que afecte a un sistema de dinero electrónico, podría crear falsos pasivos para una institución financiera. En el caso de que el sistema afectado sea de banca electrónica, el acceso no autorizado podría generar pérdidas directas, cambio en los pasivos y activos de los clientes u otros problemas.

Otros tipos de problemas que podría sufrir una entidad financiera relacionados con la seguridad pueden ser causados por ataques externos de hackers[2], quienes podrían penetrar en los sistemas de registro del banco y

[2] Un *hacker* es aquel individuo que intenta ingresar intencionalmente a un sistema informático, a través de Internet o cualquier otro medio de acceso remoto, atravesando las barreras de seguridad de ser necesario, con el fin de revisar y/o alterar, dañar, destruir o cualquier otra forma de afectar el contenido de dichos sistemas, o ganar el control sobre los mismos

obtener información sensible[3] o confidencial sobre sus clientes; o introducir en los sistemas de la entidad algún virus que provoque fallas en el funcionamiento de dichos sistemas o pérdida de información. Esto es especialmente importante cuando el banco también provee a sus clientes de servicios de acceso a Internet.

Además, las entidades financieras están sujetas a riesgos de seguridad por parte de sus empleados, si es que algún empleado con acceso a los sistemas informáticos del banco comete fraude o errores no intencionales. Estos problemas podrían generar acceso a cuentas bancarias de los clientes o extracción de información sensible de éstos. Sobre el dinero electrónico, es de importancia directa para el supervisor tomar en cuenta las operaciones que realicen los emisores de este medio de cambio. Si bien en el Ecuador aún no se ha implementado un sistema multipropósito de dinero electrónico, se debe tener en cuenta los posibles riesgos que conlleva su implementación; en especial, el riesgo de acceso a los sistemas que almacenan y/o transfieren el valor.

2.2.2.- Riesgos de mal uso de los productos por parte de los clientes

Otra fuente de riesgo puede ser el mal uso, o abuso, casual o intencional, de los sistemas y productos por parte de los clientes. En ausencia de métodos de control adecuados, un cliente podría negar una transacción previamente autorizada. Si un cliente usa el producto en un entorno inseguro[4], podría permitir que un hacker acceda a información sensible y causar pérdidas al cliente y al banco. Por último, el riesgo de usar los productos y sistemas del banco para efectuar lavado de dinero puede verse incrementado en ausencia de los controles adecuados.

---

[3] La información *sensible* de un agente es toda aquella información personal que, de recibir mal uso, podría causarle perjuicio directo a éste. Ejemplos de información sensible son: Datos personales, datos de tarjetas de crédito, dirección, teléfono, correo electrónico, gustos y preferencias, flujos de consumo, balances en cuentas bancarias, etc.

[4] En términos informáticos, es aquel entorno en que la transferencia de datos es susceptible de ser interceptada, revisada y/o modificada por un tercero, mientras los datos están en tránsito hacia su destino.

2.2.3.- Riesgos de diseño, implementación y mantenimiento de sistemas

Los sistemas de una institución financiera pueden ser generadores de riesgo si es que no se implementan adecuadamente. Fallas en el sistema de banca electrónica, problemas con la red, controles inadecuados, sistemas obsoletos o sistemas no integrados con los demás procesos del banco pueden causar problemas con los clientes, o rechazo por parte de éstos si es que los sistemas no cumplen con las expectativas, lo cual puede generar, además, una mala percepción de los negocios del banco en general, con lo cual éste caería en riesgo reputacional.

Otro tipo de riesgos aparece cuando la institución financiera contrata a terceros para la provisión de algún servicio conexo a las actividades de banca electrónica. Falta de experiencia y seriedad por parte del proveedor, problemas en la actualización de la tecnología utilizada, problemas serios del proveedor (tales como fallas financieras que lo pongan en peligro de quiebra o similar) que pongan en riesgo la continuidad en la provisión del servicio. Además, como los sistemas informáticos cambian tan rápidamente, los bancos enfrentan riesgos de caer en obsolescencia informática, pero también de actualizar sus sistemas remotos mediante canales inseguros, que permitan que la nueva tecnología sea interceptada y modificada maliciosamente. Por último, el cambio en los sistemas puede ser tan rápido que el personal puede no entender completamente la naturaleza y funcionamiento de los nuevos sistemas, lo cual puede generar problemas operativos con estos últimos.

2.2.4.- Riesgos asociados a dinero electrónico

En el caso de dinero electrónico, sobre todo si los sistemas de dinero electrónico utilizan Tarjetas de Valor Almacenado "TVA", existe riesgo de alterar o duplicar los contenidos de estas tarjetas, tratando así de dañar los sistemas o de incrementar fraudulentamente los balances de éstas; así como los usuarios de estas tarjetas pueden sufrir robos de tarjetas válidas; o el personal de la empresa emisora de las TVA puede cometer fraude alterando internamente los saldos, realizando transferencias o vendiendo los detalles de la tecnología usada en las TVA a terceros, para facilitarles el acceso o modificación de las mismas[5].

1.3.- ANTECEDENTES NORMATIVOS Y CONTROLES DE SUPERVISIÓN TECNOLÓGICA [1]

La Superintendencia de Bancos y Seguros tiene el objetivo de propender a que las instituciones del sistema financiero cuenten con fuertes medidas de seguridad en la tecnología de información y comunicaciones, a fin de que los elementos tecnológicos utilizados para entregar sus productos y/o servicios sean seguros y confiables; por tal razón las instituciones del sistema financiero deben contar con los controles necesarios para proteger los intereses del público, de acuerdo con lo señalado en el artículo 1 de la Ley General de Instituciones del Sistema Financiero.

Entre los eventos de riesgo operativo que enfrentan las instituciones supervisadas en el desarrollo de sus actividades, se encuentran el "fraude interno" y el "fraude externo", los cuales podrían ocasionarse a través del uso

[5] Para mayor discusión sobre dinero electrónico y seguridad, véase BANK FOR INTERNATIONAL SETTLEMENTS. **Security of Electronic Money** – Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Centrtal Banks of the Group of Ten countries. BIS.Basilea, Agosto 1996 (disponible desde la página electrónica del BIS: http://www.bis.org/)

inseguro de la tecnología de información y comunicaciones; siendo de vital importancia que las instituciones del sistema financiero implementen suficientes medidas de seguridad para mitigar el riesgo de fraude por el uso de la tecnología de información y comunicaciones, como elemento fundamental de una administración preventiva que reduzca la posibilidad de pérdidas e incremente su eficiencia, siendo parte de una adecuada gestión de riesgos.

El control por parte del supervisor no consiste únicamente en garantizar que las instituciones controladas posean el capital necesario para cubrir los riesgos de sus actividades, sino también en alentarlas a que desarrollen y utilicen mejores técnicas de gestión de sus riesgos que les permitan ser más eficientes y competitivas en un entorno globalización. Es así que la Superintendencia de Bancos y Seguros del Ecuador emitió la norma sobre "La Gestión del Riesgo Operativo" bajo resolución No. JB-2005-834 de 20 de octubre de 2005, que contiene disposiciones encaminadas a promover en las instituciones financieras controladas la aplicación de los principios y prácticas recomendadas por el Comité de Basilea, para la gestión del riesgo operativo, como un paso necesario y previo para ascender, en el futuro, hacia requerimientos cuantitativos de capital, contemplados en el Nuevo Acuerdo de Capital de Basilea.

La resolución establece que antes de determinar cargos de capital por riesgo operativo, las instituciones financieras deberían desarrollar un ambiente apropiado de gestión de riesgo operativo – tecnológico. Esto implica asegurar una gestión efectiva de los procesos institucionales, recursos humanos y tecnología de la información, estableciendo y validando planes de contingencia y de continuidad de negocio. Una vez que estos aspectos cualitativos sean alcanzados, las instituciones tendrían la capacidad para moverse hacia

requerimientos cuantitativos de capital, como establece el Nuevo Acuerdo de Capital.

Mediante resolución N° JB-2012-2148, publicada en el Registro Oficial de 19 de junio de 2012, la Superintendencia de Bancos y Seguros en Libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, incorpora y reforma disposiciones normativas en el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del Título II "De la organización de las instituciones del sistema financiero privado" y en el Capítulo V "De la gestión del riesgo operativo", del Título X "De la gestión integral y control de riesgos, con el fin de establecer medidas de seguridad en lo relacionado con la tecnología de información y comunicaciones.

La normativa planteada en referencia al tema en estudio, cubre los siguientes numerales [1]:

"4.3.8 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:"

"4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones

de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;"

"4.3.8.4 La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado;"

"4.3.8.19 Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes;"

"4.3.11 Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente:"

"4.3.11.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los

datos transmitidos acordes con los estándares internacionales vigentes;"

La participación activa y la responsabilidad que asuman los máximos organismos de administración de las entidades son cruciales para el éxito del proceso, es por eso que la norma, en el marco de la administración integral de riesgos, define responsabilidades específicas sobre el riesgo operativo para el Directorio, el Comité de Riesgos y la Unidad de Riesgos, así como un plazo de tres años para su cumplimiento.

Por otro lado, se debe considerar que la Industria de Tarjetas de Pago (PCI) ha establecido ciertos requisitos y procedimientos de evaluación de seguridad plasmados en la NORMA PCI – DSS Versión 2.0.[7], como parte de las exigencias del mercado. Del análisis efectuado se tiene que de un total de 52 entidades evaluadas, 30 entidades se encuentran en un proceso de implementación de la mencionada norma.

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con

el uso de controles y prácticas adicionales para mitigar otros riesgos. A continuación, se presenta una descripción general de los 12 requisitos de las PCI DSS.

- Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
- Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores.
- Requisito 3: Proteger los datos almacenados de los propietarios de tarjetas.
- Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
- Requisito 5: Usar y actualizar regularmente un software antivirus.
- Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.
- Requisito 7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
- Requisito 8: Asignar una Identificación única a cada persona que tenga acceso a un computador.
- Requisito 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.
- Requisito 10: Rastrear y monitorear todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
- Requisito 11: Probar regularmente los sistemas y procesos de seguridad.
- Requisito 12: Mantener una política que contemple la seguridad de la información.

Finalmente, considerando la realidad del sistema financiero ecuatoriano, las disposiciones del organismo de control se orientan a exigir de las entidades

requisitos mínimos para la administración de cada uno de los factores de riesgo de operación. En cuanto a la tecnología, la expectativa es que las instituciones cuenten con una tecnología de información que soporte adecuadamente las operaciones y procesos de las entidades. Para esto, es necesario que las entidades planifiquen ordenadamente sus requerimientos actuales y futuros de tecnología bajo un estudio técnico en referencia a temas de encriptación; que establezcan toda una serie de requisitos y condiciones de seguridad y de continuidad del negocio, de manera que, puedan contar en todo momento con información que cumpla con las características de integridad, disponibilidad y confidencialidad; además de asegurar que la tecnología no afecte al normal desenvolvimiento de sus operaciones.

1.3.1.- Legislación de protección de datos en Ecuador [8]

El concepto jurídico de protección de datos, se encuentra íntimamente ligado a los derechos fundamentales a la intimidad, al honor y privacidad personal y familiar, así como la defensa de las libertades públicas, es recogido en las normas fundamentales de la mayoría de los Estados. En el caso de la Constitución Política del Ecuador de 2008, en su artículo 23, inciso 8, se reconoce el "*derecho a la honra, a la buena reputación y a la intimidad personal y familiar (…)*" haciendo una clara referencia a que, la Ley protegerá el nombre, la imagen y la voz de la persona, entendiendo los mismos como signos identificativos y personalísimos del ser humano.

En su artículo 92, la citada Constitución reconoce el "habeas data", es decir, el derecho, en ejercicio de una acción constitucional o legal, que tiene cualquier persona que figura en un registro banco de datos, de acceder a tal registro, para conocer qué información se tiene de sí, y solicitar la corrección de

dicha información si le causara algún perjuicio. La norma Constitucional ecuatoriana dice que "*toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar al funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización*", artículos 30 a 45 de la Ley de Control Constitucional de 1997.

Quedan recogidos por tanto, en el citado precepto, los derechos sobre protección de datos a los que hace referencia nuestra Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, conocidos como derechos ARCO, el derecho de acceso a la información (así como el conocimiento del tratamiento que de la misma se está haciendo), el derecho de rectificación y el derecho de cancelación.

Además, la Asamblea Nacional de la República del Ecuador, tramitó en 2009 el Proyecto de Ley de Datos Públicos de los Registros de la Propiedad, Mercantiles o de Prendas Especiales de Comercio, generando en su tramitación, ciertas controversias sobre la viabilidad de dar cumplimiento al artículo 94 de la Constitución Política de Ecuador y la interrelación con el derecho de los ciudadanos a no ser conocidos en ciertos aspectos de su intimidad.

El derecho a la intimidad, el honor y la privacidad, se encuentra íntimamente ligado a la protección frente a conductas delictivas, tales como injurias, calumnias, … recogidas en el Código de Procedimiento Penal de Ecuador en sus artículos 36, 489 y siguientes. A mayor abundamiento se establecen

prohibiciones relacionadas con el derecho a la dignidad e imagen, entre ellas las relacionadas con menores de edad, en lo referente no sólo a datos de carácter identificativo, sino a la propia imagen de la persona. Dicha protección desde el punto de vista penal, se recoge, a modo de ejemplo, en el artículo 202 del Código Penal de Ecuador, estableciendo que, "*la persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la utilización de su titular o titulares, serán sancionados con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares*".

La Ley Orgánica del Consumidor, en otro ámbito, al referirse a la cobranza de créditos en su artículo 49, dice "*en la cobranza de créditos, el consumidor no deberá ser expuesto al ridículo o a la difamación, ni a cualquier tipo de coacción ilícita ni amenaza de cualquier naturaleza, dirigida a su persona, por el proveedor o quien actúe en su nombre.*"

El artículo 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública de 2004, establece que "*se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal, o su divulgación, dará lugar a las acciones legales pertinentes*".

Sobre este aspecto, la Declaración de Principios sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, establece que, "*la Leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar*

garantizada sólo a través de acciones civiles, en los casos en que al persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas". Generando un debate ya conocido, sobre la controversia entre libertad de información y confidencialidad o privacidad.

Otra ley complementaria de aplicación en la República del Ecuador es la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (firma electrónica, servicios de certificación, contratación electrónica, prestación de servicios, comercio electrónico y protección de usuarios y datos de estos sistemas), que recoge en su artículo 9 que para la elaboración, transferencia o utilización de bases de datos, se requerirá el consentimiento expreso del titular, quien podrá seleccionar la información a compartirse con terceros; dicha recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución de la República. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

Finalmente, queda pendiente la elaboración de una Ley que aglutine todos estos aspectos, en materia de protección de datos, así como la creación de un organismo de control que garantice su cumplimento, cabe recordar que en la actualidad, estas funciones son realizadas por la citada Superintendencia y la

Defensoría del Pueblo del Ecuador; ya que en esencia, los preceptos y derechos citados en el presente artículo, recogidos en la legislación ecuatoriana, son equivalentes a los recogidos en otras legislaciones internacionales, tal y como ocurre en la Ley Orgánica española.

1.3.2.- Lineamientos básicos para una propuesta regulatoria

Luego de revisar la evolución del sector financiero en productos y servicios financieros en el país, los riesgos inherentes y las propuestas y desarrollos en materia legal, podemos ver que los avances dados al respecto son satisfactorios, ya que se observa una toma de conciencia sobre los avances tecnológicos, sus ventajas e implicaciones para la relación entre proveedores y usuarios de los distintos servicios. Sin embargo, la identificación de riesgos evaluados en este documento deja entrever que hay algunos temas que aún no han sido tratados en la profundidad debida, los cuales deberán ser los que reciban mayor atención a la hora de iniciar un estudio más profundo en la materia. Lo primero que salta a la vista es la falta de definiciones y de acuerdos entre las partes, para ver la aplicabilidad de las normas existentes a los nuevos productos y servicios. Esto puede generar problemas conforme aumente la cantidad de usuarios de servicios de banca electrónica.

Por otra parte, dado que el alcance de Internet es mundial se plantea los siguientes cuestionamientos: *¿qué legislación se aplica en caso de una operación internacional?, ¿Debe decirlo eso la entidad, ser un acuerdo entre la entidad y el cliente, o debe someterse a la competencia de una "ley internacional"?, ¿Cuán expuesto y preparado está la entidad ante un problema legal, por incertidumbre del marco legal aplicable?, ¿De qué manera se mediría y cómo se sancionaría una exposición a este tipo de riesgo?.*

Los problemas más serios que presentan las nuevas tecnologías son, obviamente, problemas tecnológicos. Pero cuando éstos ocurren*, ¿quién es el responsable?.* Si, durante una transacción en la página web del banco, un tercero logra apoderarse de los datos de la tarjeta del cliente y comete una operación fraudulenta, *¿quién debe ser responsabilizado por el error?*, sea cual sea la respuesta, está explícitamente especificada en los términos de servicio. Y con respecto de la seguridad de los sistemas, *¿se deben exigir requisitos mínimos a los bancos?*, si es así, *¿de qué manera se exigirían y de qué manera se revisarían?, ¿Qué sanción debe serle aplicada a un banco cuyos sistemas no demuestren la seguridad suficiente?, ¿Debe haber un lineamiento de riesgos generales, una guía de procedimientos de examinación de sistemas?.*

Además, se ha visto que las entidades financieras, para realzar el servicio que brindan a sus clientes, puede dar servicios adicionales, no bancarios, que contratan con terceros. Si el banco brinda otros servicios, aparte de los propiamente bancarios, *¿quién regula la provisión de dichos servicios? ¿Hasta dónde debe ser responsable por daños causados a los clientes que usaron estos servicios?.*

Éstas son sólo algunas cuestiones que aún no han sido resueltas, y que deben ser estudiadas con más detalle para poder diseñar una regulación efectiva sobre el sector financiero. Es cierto que, al ser un entorno nuevo, incipiente y en desarrollo, requerimientos muy estrictos pueden desalentar el crecimiento de la oferta de productos en este sector. Sin embargo, dejar estos temas sin adecuado tratamiento puede causar, en el mediano plazo, una exposición considerable a los riesgos tratados en el presente documento, lo cual podría minar la confianza en los servicios, o hasta afectar el propio sistema financiero.

Además, respecto a lo citado y debido a la rapidez con que se han difundido los servicios en línea que brindan tanto bancos como otras instituciones a lo largo del mundo, y las nuevas implicancias que traen estos servicios en cuanto al claro establecimiento de los derechos, deberes y responsabilidades de las partes involucradas, en distintos organismos internacionales se están dando marcos legales para las diferentes operaciones que pueden existir en Internet.

Desde temas civiles y penales, hasta procedimientos y requerimientos específicos para el negocio bancario, estos documentos marcan la pauta en cuanto a normatividad aplicable para el tema en cuestión. Sobre tales documentos, el Ecuador ha puesto en vigencia algunas leyes que dan un marco legal general para el desarrollo de las transacciones electrónicas, quedando todavía bastantes temas por subsanar. A continuación, detallaremos los documentos más relevantes para la banca electrónica en materia de normatividad y recomendaciones desarrolladas a escala internacional, para comparar el nivel de desarrollo en el tema e identificar los puntos en los que aún no se ve un desarrollo normativo suficiente.

a. Ley Modelo de la CNUDMI sobre Comercio Electrónico.
b. Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito.
c. Ley de Transferencia Electrónica de Fondos y la Regulación - Electronic Funds Transfer Act EFTA).
d. Procedimientos de Revisión de la Solidez y Seguridad de la Banca Electrónica - *Electronic Banking – Safety and Soundness Examination Procedures.*

1.4.- ANÁLISIS DE VULNERABILIDADES A NIVEL DE IFIS

El sistema financiero ecuatoriano no ha sido ajeno a las pérdidas que genera la falta o la inadecuada administración del riesgo de operación tecnológico; esta situación se puede apreciar en los eventos de riesgo operativo que se presentaron en la crisis financiera que vivió el Ecuador hace años atrás y que fueron ocasionados por fallas e insuficiencias en los procesos, en las personas y en la tecnología de información.

La Superintendencia de Bancos y Seguros en el año 2011, revela cómo el fraude bancario ha migrado desde Colombia, a otros países, especialmente Ecuador y Venezuela, debido especialmente a la adopción de tecnologías de chip y PIN[6], así como al uso de sistemas de gestión de fraude basado en analítica, que utilizan los emisores de tarjetas en esos países.

En el Ecuador, los niveles de fraude crecieron un 31% entre el año 2009 y 2011, debido a las tecnologías utilizadas en los cajeros automáticos y debilidades identificadas a través de la banca virtual. Sin embargo, los delitos con tarjetas falsas emitidas en el extranjero han crecido un 33% desde el 2009, Las tecnologías de chip y PIN se empezaron a utilizar en Ecuador en el 2011 (frente a otros países que lo hicieron en el 2005), lo que muestra la importancia del uso de estas medidas de seguridad a la hora de reducir el fraude. En nuestro país, el fraude aún representa pérdidas para el sector cuantificadas en un valor de 3 millones de dólares anuales.

Utilizando los datos ofrecidos por Euromonitor Internacional, se puede comprobar cómo ha evolucionado el fraude en los últimos años en el Ecuador y

[6] El sistema de Chip y PIN es una iniciativa conjunta del sector de tarjetas de pago encaminada a reducir el fraude y a aumentar la seguridad de las transacciones. A diferencia de la antigua Tarjeta de firma, una Tarjeta Chip y PIN incluye un microchip, y requiere que el Cliente introduzca un PIN "*Personal Identification Number*" para autorizar la transacción.

cómo han crecido las áreas de riesgo, como la suplantación de identidades, las tarjetas falsas o el fraude online. De hecho, en toda la región destaca el incremento del fraude en las operaciones en las que no se precisa la tarjeta de forma física.

El incremento de la protección en las tarjetas, especialmente el uso de chip y PIN, ha provocado que los delincuentes dirijan sus acciones a Internet, donde hay mayores facilidades de cometer fraude que en sitios físicos. La respuesta a los fraudes con tarjeta en los que no se necesita de presencia ha sido más lenta, pero el creciente uso del protocolo 3D Secure, utilizado tanto por VISA como por MasterCard, y al que se está uniendo American Express, permite evidenciar una disminución de los riesgos identificados sobre este tema.

Desde octubre del año 2012 de acuerdo a los datos presentados por la Dirección Nacional de Estudios (SBS). Los pilares de la seguridad en Internet se han derrumbado y no volverán a parecerse a lo que hemos conocido hasta la fecha. No valen las posturas acomodaticias ni los arreglos a medias: los hackers han encontrado la manera de burlar radicalmente las hasta ahora bien construidas defensas de nuestros sistemas y de nada sirve –o de muy poco- armarnos hasta los dientes con los sistemas habituales (IPS[7], IDS[8] u otros) que resultaban eficaces.

Y es que desde octubre de 2010 los proveedores de seguridad de redes han caído en cuenta de que los hackers están violando los sistemas de los organismos más prestigiosos y mejor protegidos del mundo gracias a las denominadas Técnicas de Evasión Avanzadas (AETs), un conjunto de técnicas de

[7] Un **Sistema de Prevención de Intrusos (IPS)** es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

[8] Un **sistema de detección de intrusos** (o **IDS** de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

evasión que pueden ser fácilmente alteradas o combinadas con criterios diversos con el fin de evitar la detección por parte de los sistemas de seguridad.

Así, actúan como "llaves maestras" que dan acceso franco a lugares altamente protegidos y facilitan que cualquier carga útil –y peligrosa- pueda ser entregada en los objetivos. Es decir, las Técnicas de Evasión Avanzadas ponen en riesgo la funcionalidad de los datos capitales y los sistemas de las organizaciones.

Analicemos, para apuntalar la anterior afirmación, el período comprendido entre 2010 y comienzos de 2011. Cuatro fenómenos diferentes, Wikileaks, Stuxnet, las Técnicas de Evasión Avanzadas y la violación del código fuente SecurID han derribado los axiomas básicos del pensamiento de seguridad y actuado como despertadores también en el ámbito estratégico bancario.

En efecto, la banca es uno de los sectores más amenazados por los hackers, por motivos obvios. Por todos es conocido el gran ataque informático que sufrió uno de los más importantes bancos norteamericanos en mayo del 2013. El resultado fue nada menos que 2,7 millones de dólares sustraídos de 3.400 cuentas corrientes de sus clientes. Con todo, el asunto pudo haber sido peor, pues los hackers consiguieron entrar en otras 360.083 cuentas. El que no lograran sustraer más dinero fue una mera cuestión de suerte.

Lamentablemente, este asunto no fue un hecho aislado. Organismos como el FMI, Lockheed Martin *–proveedor de material tecnológico para el Departamento de Defensa de EE.UU-* o la archiconocida Sony han sufrido abordajes exitosos a lo largo de 2011.

Como vemos, las amenazas han cambiado, y lo peor es que no todos los proveedores lo están haciendo en consecuencia. A nuestro entender, está cada vez más claro que los hackers adoptan técnicas de mayor sofisticación para evitar ser cazados por los IPS e IDS. Pero lo que verdaderamente centra nuestra atención son básicamente dos aspectos; el primero de ellos es que estos nuevos ejemplos han logrado vencer todas las defensas conocidas y penetrado en diversos protocolos, incluyendo IPv4, IPv6, TCP y HTTP. Es decir, pueden acceder a sus víctimas a través de Internet.

En el Ecuador específicamente se tiene que las principales modalidades de fraude que han afectado al Sistema Financiero durante los últimos años ha sido la clonación de tarjetas de débito, crédito y las transferencias fraudulentas con el siguiente detalle para los años 2012 y 2013:

TABLA 1.1.- Estadísticas de Fraude Electrónico - FUENTE: SBS-DNR- 2012-2013[9].

FRAUDES POR	AÑO 2012	AÑO 2013
Impacto Económico	US$ 3'8 MM	US$ 1'3 MM
Clonación de Tarjetas de Débito	76.14%	43.50%
Tarjetas de Crédito	11.17%	22.43%
Canal Internet	6.51%	1.13 %
Otros (Retiros Cuentas Corrientes y de Ahorro)	6.18%	32.94%

En la TABLA 1.1 se puede apreciar que existe una reducción en las pérdidas económicas del año 2012 frente al 2013, así también se puede evidenciar que las pérdidas del 2012 por cada US$ 10M transadas equivalían a US$15.11 y las pérdidas del 2013 por cada US$ 10M transados equivalen al US$

[9] ***Superintendencia de Bancos y Seguros del Ecuador.-*** Datos evaluados por la Subdirección de Riesgo Operativo /Dirección Nacional de Riesgos para los años 2012 y 2013.

1.39. Sin embargo, se debe recalcar que los datos presentados no reflejan la realidad del país en manera integral por cuanto solo un 20 % de los fraudes son reportados por las entidades financieras, considerando lo expuesto se efectúo una encuesta considerando una muestra de 43 entidades financieras públicas y 7 privadas, arrojando los siguientes resultados:

TABLA 1.2.- Estadísticas de Fraude Electrónico - FUENTE: Investigación- Autoría Propia.

FRAUDES POR	**AÑO 2012**	**AÑO 2013**
Impacto Económico	US$ 11’2 MM	US$ 7’2 MM
Clonación de Tarjetas de Débito	60.35%	40.37%
Tarjetas de Crédito	12.15%	10.28%
Canal Internet	21.32%	45.20 %
Otros (Retiros Cuentas Corrientes y de Ahorro)	6.18%	4.15%

Del análisis a los datos expuestos en la TABLA 1.2, se tiene que los valores para el año 2013 disminuyen en relación al año 2012, no obstante para el canal de Internet se evidencia un incremento notable del riesgo de fraude identificado en el 2012, lo cual denota que las medidas de seguridad adoptadas no son efectivas.

Por otro lado, las principales medidas de mitigación implementadas por las entidades para reducir las pérdidas por fraude, corresponden a la implementación de un "*Centro de Monitoreo de Fraudes*" para las transacciones que los clientes realizan con tarjetas de débito en ATM´s y POS.

En relación a los fraudes por internet, se tiene que luego de la implementación del esquema de *One Time Password* (OTP) como complemento

al sistema biométrico (Resolución N° JB-2012-2148) se han eliminado los reclamos por fraudes en este canal.

No obstante de los resultados obtenidos, las entidades financieras se encuentran trabajando en temas como:

a. La ampliación del sistema de monitoreo para los canales de Banca de Personas, Cash Management, Corresponsales No Bancarios, Banca Móvil y Ventanillas.
b. Reemplazo y fortalecimiento de los cajeros automáticos incorporando medidas de seguridad de última generación.
c. Proceso de certificación EMV (**E**uropay-**M**asterCard-**V**isa) para la red de adquirencia (ATM´s, POS, CNB) para transacciones con chip.
d. Protección automática a nivel de usuario final.
e. Implementación de un modelo de comportamiento en la validación de las transacciones y montos habituales y listas "negras de cuantas beneficiarias.
f. Implementación de OTP para transacciones monetarias.
g. Identificación y "desmonte" de sitios falsos, detección de modificaciones de contenido y DNS.
h. Detección de ataques de Denegación de Servicio.
i. Detección de modificaciones de contenido y enlaces de los portales.
j. Campañas de comunicación, charlas y conferencias con expertos.

Del análisis planteado, no tenemos la menor duda de que algún día la industria en su conjunto será capaz de hacer frente a esta amenaza con la suficiente firmeza, pero hasta entonces nos queda un largo camino por recorrer, y el primer paso para emprenderlo es, sin lugar a dudas, llegar a un

reconocimiento unánime por parte de proveedores y clientes de la gravedad del problema y sus serias implicaciones.

La participación activa y la responsabilidad que asuman los máximos organismos de administración de las entidades son cruciales para el éxito del proceso, es por eso que la Resolución N° JB-2012-2148 planteada [1], adopta mecanismos que permitan brindar esquemas de seguridad básica como es el caso de la implementación de métodos de encriptación que motivan este proyecto de tesis.

CAPÍTULO II

MARCO TEÓRICO

En este capítulo se hace mención a la investigación realizada sobre los fundamentos criptográficos, cubriendo a manera general los fundamentos básicos de los principales métodos criptográficos existentes (Simétrica y Asimétrica). Además, se describen las diversas alternativas de implementación tales como firmas y certificados digitales.

2.1.- SEGURIDAD INFORMÁTICA APLICADA A IFIS [2]

Existe una amplia variedad de amenazas sobre los sistemas informáticos y de comunicaciones; estas debilidades poseen orígenes diversos. Por un lado el hardware puede ser físicamente dañado por la acción de agentes físicos: líquidos, fuego, herramientas mecánicas, golpes y caídas, entre otros. Si bien es cierto que estas acciones pueden ser fortuitas, producto de accidentes, también se encuentran con frecuencia los casos en que son producto de sabotaje. Por otro lado, el software también corre peligro; al actuar de forma mal intencionada, no sólo se pueden afectar la operatividad de los equipos, sino dañar incluso los medios magnéticos de almacenamiento de la información, utilizando por ejemplo dispositivos que emitan campos magnéticos intensos.

Sin embargo, en el mundo moderno, y particularmente dado el incremento de fraudes informáticos, es muy común que los factores de agresión intervengan la data informática de una forma que les resulte más provechosa.

Las líneas de comunicación pueden interferirse o "pincharse", la data puede ser sustraída de los computadores. Usuarios o empleados desleales pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos.

Amenazas más sutiles pero no por ello menos peligrosas provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente. Otra técnica fraudulenta consiste en transferir información de un programa a otro mediante canales ilícitos, no convencionales u ocultos.

Basta con que un intruso individual posea las destrezas, y por supuesto la oportunidad de realizar un acto ilícito, para que se convierta en un grave peligro para la seguridad de las instituciones financieras.

A nivel de redes, algunas de las principales amenazas para la protección de la información provienen de archivos adjuntos a mensajes enviados por correo electrónico, donde estos adjuntos están infectados con algún tipo de código malicioso, ataques a los recursos de la entidad, o la propia configuración incorrecta de los sistemas de protección de redes.

El factor humano ha sido siempre una parte importante en la seguridad informática; sin embargo, actualmente las entidades financieras menosprecian el papel de la conducta humana y se han inclinado a confiar en cajas (ATALLA) y algoritmos a nivel de hardware para resolver problemas de seguridad, y por ende sobreentienden que la información de la entidad está blindada.

Parte de los ataques de Hacker, Cracker , Phreaker y otros delincuentes informáticos se ha basado en ingeniería social; no es por nada que muchos responsables de sistemas apuntan a controlar más al "usuario" interno que al cliente externo. Si se consulta a cualquier artículo publicado o experto en la materia sobre el tema de seguridad, siempre dice casi lo mismo, un alto índice de hechos delictivos ocurre con complicidad interna, por lo que necesitan dedicar más tiempo a políticas, procesos y personal antes que a la tecnología si quieren asegurar con éxito las infraestructuras de TI.

Hoy día las entidades financieras al momento de establecer su seguridad informática se enfocan principalmente en los dos elementos más publicitados: "el Firewall" y los "Programas Antivirus". Aunque deben ser dos de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad. Un Firewall (o Muro Cortafuegos, en español) es un sistema ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet). Esencialmente:

Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él, y

Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

El Firewall sólo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa. Algunos Firewalls aprovechan esta propiedad de que toda la información entrante y saliente debe pasar a través de

ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red.

Por su parte, un antivirus es una gran base de datos con la huella digital de todos los programas maliciosos conocidos para identificarlos y descubrirlos a través de su comportamiento.

Actualmente existen técnicas capaces de analizar archivos, detectar y neutralizar posibles actividades sospechosas tales como:

Detección: se debe poder afirmar la presencia y/o accionar de un software malicioso virus en una computadora. Para realizar esta acción existen:

El Scanning: técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. [2]

La Heurística: o búsqueda de acciones potencialmente dañinas pertenecientes a un programa malicioso. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controladas por el usuario (MBR, Boot Sector, FAT, y otras). [2]

Neutralización: adicionalmente se deben brindar módulos de erradicación del segmento de código maligno y la cuarentena o eliminación completa de la entidad infectada.

De cualquier forma, ni los firewalls, ni los antivirus pueden defendernos contra las técnicas de ataque conocidas como "la Ingeniería Social" y el ataque de "Insiders".

La Ingeniería Social: abarca un conjunto de técnicas aplicadas a obtener información confidencial a través de la manipulación a los usuarios que poseen esta información. Un ingeniero social normalmente no utiliza programas sofisticados ni programas complejos de computación; simplemente realiza una llamada telefónica o se introduce en Internet para engañar a la gente, buscando información sensible. Para que sus ataques tengan éxito deben, por un lado, tener don de convencimiento y aprovechar la ignorancia, los temores o las costumbres del usuario. Por otro lado, debe existir un usuario mal capacitado en cuanto a las normas de seguridad de la organización, bien sea porque no ha desarrollado la conciencia para seguirlas, o incluso, porque la organización en sí misma no dispone de políticas expresadas claramente en procedimientos adecuados a sus usuarios. En consecuencia, el usuario se convierte en el eslabón débil de la seguridad informática, y sobre este principio se rige la ingeniería social.

Un Insider¬: es una persona a la que se le ha dado un grado de confianza y de acceso dentro de una organización, y que los usa en conjunto a sus conocimientos tecnológicos para hacer daño a esta misma organización.

Ante este panorama, las Instituciones Financieras deben hacerse algunas preguntas como: ¿Qué tan vulnerable es hoy la información de mi organización?,

¿Hay métodos y herramientas para rastrear detalladamente la actividad de los usuarios?, ¿Qué tan conscientes están los empleados dentro de esta organización del problema de la seguridad?. Son numerosas las amenazas y riesgos en los que ve inmersa la información en una estructura organizacional.

Generalmente los usuarios son administradores de sus propias máquinas e instalan programas que pueden poner en riesgo la información, violando la seguridad de la organización completa. A la par, hay otras prácticas comunes como el chat que afecta directamente la productividad de los funcionarios y por ende a las instituciones financieras. Una de las violaciones más comunes que sucede hoy día, es el uso indebido de un sistema de información por un usuario que no es el acreditado y que por alguna técnica pudo obtener el nombre de usuario autorizado y su clave para acceder a la información. La fuga de información generalmente sucede porque pese a las medidas que toman las Instituciones Financieras para asegurar su hardware y software, no toman las suficientes para evitar los usos indebidos de los sistemas y evitar que esta información sea enviada a destinos no autorizados.

Un ejemplo es que un usuario podría comenzar a instalar software de captura de datos, los denominados "snifers" que son capturadores de passwords, contraseñas y conversaciones. Entonces puede investigar cuáles son las cuentas electrónicas o passwords de sus compañeros, bajar sus e-mails e incluso suplantarlos. Estas son cosas que pueden estar sucediendo en una Institución Financiera y casi nadie podría darse cuenta de lo que está pasando.

2.1.1.- Seguridad Lógica y Seguridad Física

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Se suele hablar de la seguridad en términos de antivirus y de firewalls, es decir, en términos de la Seguridad Lógica, pero otros aspectos como la detección de un atacante interno a la organización que intenta acceder físicamente a una sala de servidores, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala de servidores, que intentar acceder vía lógica a la misma. La Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Luego de evidenciar cómo un sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con un efecto de falsa seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir métodos y técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica. Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".

Algunos de los objetivos que debe perseguir la Seguridad Lógica son: restringir el acceso a los programas y archivos, asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan, asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto,

que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro, que la información recibida sea la misma que ha sido transmitida, que existan sistemas alternativos secundarios de transmisión entre diferentes puntos, etc.

La labor del personal de Seguridad Lógica se divide en cinco grandes áreas:

Formulación de Políticas, Normas y Procedimientos.

Estudio, Instalación y Configuración del Software y el Hardware Adecuados.

Preparación de Jornadas Capacitación con Diseño a la Medida, Programación de Cursos, Talleres de Capacitación, y Foros en las Áreas de Seguridad Informática.

Monitoreo del Comportamiento de los Sistemas, particularmente del Tráfico de la Red, y de los Accesos a las Bases de Datos.

Aplicación y Análisis Forense Digital .

La Superintendencia de Bancos y Seguros suma esfuerzos para la realización y elaboración de Procedimientos, Normas y Políticas, cuya intención es dar a conocer la problemática de seguridad informática que existe en el campo financiero, que afecta a instituciones públicas y privadas, brindando asesoría sobre resguardo de la información y protección de los sistemas y redes, tanto privadas como públicas, de ataques internos y externos; con el fin de formular Políticas sobre Seguridad y Contingencia en las Redes Informáticas y de Telecomunicaciones a ser aplicadas en las Instituciones Financieras.

2.1.2.- Seguridad Criptográfica

Todas las aplicaciones y procesos bancarios, tanto en entidades financieras, en Pasarelas de Pago, Switches, etc. requieren de la criptografía basada en Hardware certificado (Soportada por dispositivos HSM, "Host Security Module") para realizar todos los procesos de generación de pines, claves de tarjetas, comunicaciones entre aplicaciones bancarias, etc. Las entidades financieras en el Ecuador en un 15% han invertido en infraestructura criptográfica, teniendo que pagar habitualmente por cada función criptográfica que necesite utilizar. Las entidades tienen que invertir en varias unidades de Hardware necesarias para soportar el rendimiento adecuado, y adicionalmente necesita un nivel de soporte que habitualmente no recibe, siendo éste un componente fundamental en todos los procesos de la entidad.

Tomando esto como antecedente es claro pensar que dados los costos no se ha invertido o realizado un estudio detallado que soporte la selección de criptosistemas a nivel de las instituciones financieras, por lo cual el trabajo de investigación complementa y acelera esta labor con la de las instituciones académicas de investigación y de otras instituciones de estándares del sector para garantizar que la Superintendencia de Bancos y seguros brinde soporte técnico sobre las soluciones de gestión de sistemas y seguridad más innovadores y que puedan satisfacer las necesidades a largo plazo de los usuarios, dedicados a la investigación avanzada de software de gestión de sistemas y seguridad para las Instituciones financieras.

2.2.- FIRMAS DIGITALES [2]

La firma digital hace referencia al método que asocia o adhiere una identidad digital (llave privada del iniciador) con un documento digital mediante la aplicación de un algoritmo. Este algoritmo consiste en la utilización de un procedimiento matemático, que verifica que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado en el proceso. Esta firma puede ser validada mediante la verificación del hash del documento con la llave pública del iniciador.

Es usada con el fin de validar la identidad de quien genera dicho objeto y la integridad del mismo, esto es garantizar su autenticidad, confidencialidad, integridad y no repudio (valores jurídicos asociados). Por esta razón la firma digital tiene la misma validez que la firma manuscrita.

Una firma digital de igual forma representa una secuencia de bits que se añade a una pieza de información cualquiera, y que permite garantizar su autenticidad de forma independiente del proceso de transmisión, tantas veces como se desee. Presenta una analogía directa con la firma manuscrita, y para que sea equiparable a esta última debe cumplir las siguientes propiedades:

Va ligada indisolublemente al mensaje. Una firma digital válida para un documento no puede ser válida para otro distinto.

Sólo puede ser generada por su legítimo titular. Al igual que cada persona tiene una forma diferente de escribir, y que la escritura de dos personas diferentes puede ser distinguida mediante análisis grafológicos, una firma digital sólo puede ser construida por la persona o personas a quienes legalmente corresponde.

Es públicamente verificable. Cualquiera puede comprobar su autenticidad en cualquier momento, de forma sencilla.

FIGURA 2.1.- Esquema de una firma digital base - A: generación de la firma; B: verificación. Tomado de Criptografía y Seguridad de Computadores. Fuente [2]

En la Figura 2.1 se presenta un esquema de una firma digital basada en funciones resumen y algoritmos de cifrado asimétricos.

La firma digital proporciona un amplio abanico de servicios de seguridad:

Autenticación: permite identificar unívocamente al signatario, al veri¬ficar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas o bien para garantizar el acceso a servicios distribuidos en red.

Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

Integridad: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante

alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.

No repudio: ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un time stamp, debido a la imposibilidad de ser falsificada.

Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados.

El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL (Secure Sockets Layer).

Existen diferentes tecnologías para realizar firmas digitales, la más usada en la actualidad es RSA (Rivest, Shamir y Adleman) la cual utiliza el problema de la factorización de un entero considerado computacionalmente infactible para tamaños del módulo mayores de 1024. Existen otros esquemas de firma digital que se apoyan sobre otros problemas como el problema del logaritmo discreto.

Las curvas elípticas se pueden utilizar para formular el problema del logaritmo discreto, una vez formulado este problema es posible construir un esquema de firma digital como el DSS (Digital Signature Standard) o el esquema Nyberg-Rueppel.

La aplicabilidad de las firmas digitales y certificados digitales se centra a en las siguientes situaciones: e-mail, contratos electrónicos, procesos de aplicaciones electrónicos, formas de procesamiento automatizado, transacciones realizadas desde financieras alejadas, en aplicaciones de negocios (Electronic Data Interchange) y en el intercambio electrónico de datos de computadora a computadora.

2.2.- CERTIFICADOS DIGITALES [2]

De la evaluación efectuada a los mecanismos de seguridad implementados por las entidades financieras en el país se deduce que muchas de las soluciones propuestas, tanto para aumentar la seguridad de los sistemas como la validez y no-repudiabilidad de las comunicaciones electrónicas, pasan por la instalación de certificados digitales o la autenticación de los documentos mediante firmas electrónicas. En este punto se abordará brevemente qué son y cómo funcionan los certificados digitales, las Autoridades Certificadoras y otros términos conexos, para su posterior análisis dentro del contexto de criptografía.

Un certificado digital es un documento de identidad digital que contiene toda la información del suscriptor o poseedor del certificado [2], más una serie de condiciones que la Autoridad de Certificación (CA) ha certificado, así como el conjunto de llaves pública y privada y el hash de firma de la Entidad de Certificación de confianza que verificó estos datos, con el fin de identificar al dueño del certificado ante la Red (sea una red interna o Internet). La Autoridad Certificadora es un agente que, debido a la confianza que se ha ganado dentro

de la red de usuarios que comparten o aceptan sus certificados, tiene validez para expedir éstos a quienes los soliciten, luego de haber pasado por un estricto proceso de verificación de datos e identidad.

El certificado digital contiene tres partes básicas: los datos del certificado (quién lo expidió, a nombre de quién está expedido, cuándo fue expedido y cuándo vence), la llave pública del dueño del certificado y la firma electrónica de la Autoridad Certificadora.

Una llave pública y su correspondiente llave privada son un par de cadenas numéricas bastante largas, y relacionadas entre sí a través de complicadas operaciones matemáticas, de tal forma que es casi imposible obtener la llave privada a partir de la llave pública. Cuando se instala el certificado en la máquina del dueño, su llave privada se guarda en un sitio seguro del disco duro. Sin embargo, la llave pública, junto con los demás elementos del certificado, se publican en una base de datos en la Web, accesible a todos los usuarios.

El certificado funciona de la siguiente manera:

Si alguien quiere enviarle datos cifrados (codificados) al dueño del certificado, busca en la base pública de certificados la llave pública del receptor, y con un algoritmo matemático muy complejo convierte los datos en un código incomprensible. Estos datos, una vez llegados al poder del receptor, y en caso de no haber sido modificados durante el tránsito (aunque sólo haya cambiado un caracter), pueden ser decodificados usando otro algoritmo matemático y la llave privada del receptor; ningún otro código puede abrir los datos cifrados. Por otra parte, si los datos fueron alterados durante el tránsito de los mismos, el receptor recibirá un mensaje de error cuando intente abrirlos. Por ende, si no recibe

mensaje de error alguno, puede estar seguro de que recibió exactamente los datos que le fueran enviados.

Si alguien quiere "firmar" los datos que envía (firma digital), genera un mensaje adicional a los datos, el cual se codifica mediante el uso de su propia llave privada.

Cuando el receptor recibe los datos, busca en la base de certificados la llave pública del emisor y trata de abrir la "firma". Si puede abrir la firma, entonces efectivamente queda comprobado que ese mensaje se firmó mediante el uso del certificado del emisor.

Esto es lo que se conoce como criptografía de llave pública o criptografía asimétrica, porque usa dos llaves para abrir y cerrar los mensajes, una de las cuales es de acceso público. Hay otro tipo de criptografía, llamada criptografía secreta o criptografía simétrica, la cual usa sólo una llave para abrir y cerrar los mensajes, la cual debe mantenerse en reserva absoluta.

2.3.- CRIPTOGRAFÍA [2]

Etimológicamente hablando, es una palabra que proviene de las palabras griegas criptos y graphos y significa literalmente "escritura oculta", es decir, la criptografía es el estudio de los métodos de envío y recepción de mensajes que solamente la persona a la cual va dirigido puede descifrar y consecuentemente, entender.

El objetivo de la criptografía es el desarrollar formas seguras de comunicación privadas usando medios de difusión públicos. Para lograrlo es necesario transformar el mensaje original en un conjunto de caracteres, señales o bits en el caso de los computadores, que no sean de ninguna utilidad para cualquier interceptor del mensaje, pero que posea algún procedimiento preciso de descifrado, de forma que la información sólo pueda verla aquel receptor que el emisor deseó en principio.

Hoy en día la criptografía es fundamental para el desarrollo de las tecnologías de la información y las comunicaciones, principalmente por dos motivos:

Las Redes Públicas (entiéndase Internet e Internet 2) se han convertido en el principal medio de envío/recepción de información, y al ser públicas, están expuestas a todo tipo de ataques y violaciones de la privacidad tecnológicamente posibles.

La data que guardan las instituciones, aunque no viaje, siempre corre el peligro de accesos no autorizados. Pero si estos accesos se producen sobre data encriptada (protegida por la criptografía) su valor informativo es nulo.

La criptografía se fundamenta en dos ramas de las matemáticas: las matemáticas discretas y la teoría de la información. Varios autores (matemáticos profesionales) han publicado diversas teorías sentando los fundamentos de ambas. Algunos famosos fueron Claude Shannon con sus artículos A Mathematical Theory of Communication y Communication Theory of Secrecy Systems. Por su parte, Whitfi Eld Diffi y Martin Hellman publicaron posteriormente New Directions in cryptography en el que introducían la criptografía asimétrica.

Un punto importante es la distinción (muchas veces se presenta esta confusión) entre "criptografía" y "código". Un código simplemente convierte palabras en otras palabras o caracteres en otros caracteres. El resultado de esta conversión es un conjunto de símbolos difíciles de entender, pero con las herramientas apropiadas, y muy importante sin necesidad de una clave o secuencia cifrante es posible obtener las palabras o caracteres originales. La criptografía en cambio, convierte palabras y caracteres en algo indiscernible, a tal punto que no es posible ni siquiera saber el tamaño del mensaje original. Al tomar este conjunto de datos confusos y aplicarle herramientas de descifrado no es posible obtener las palabras originales sin la clave o secuencia cifrante.

Aquí se aclara otro concepto, el de clave. Clave es aquel conjunto de caracteres que dan acceso a una información o a un sistema. Pero no debe confundirse la clave que se introduce para tener acceso, llamada en inglés password o passphrase con la clave utilizada para alimentar un algoritmo

criptográfico, denominada secuencia diferencia. Muchos sistemas usan ambos tipos de clave, el password para acceder, y la secuencia cifrante para realizar las operaciones dentro del mismo, por lo que el concepto tiende a volverse más oscuro.

El criptoanálisis, por su parte, es la contrapartida de la criptografía. Consiste en analizar los algoritmos criptográficos, buscándoles patrones y debilidades. Por supuesto, si el algoritmo de encriptación es bueno no las tendrá, pero eso lo determina el criptoanalista, no el criptógrafo. Ambos han tenido un gran peso en la historia, llegando incluso a influir el rumbo de las guerras. Juntos, criptografía y criptoanálisis, constituyen la criptología.

2.4.- CRIPTOSISTEMAS [6]

Un Criptosistema, o sistema criptográfico, se puede definir como los fundamentos y procedimientos de operación o algoritmo que participan en el cifrado y descifrado de un mensaje. Todo sistema criptográfico consta de cinco componentes:

El conjunto de todos los mensajes a transmitir.

El conjunto de todos los mensajes cifrados.

El conjunto de claves a utilizar.

El conjunto de todos los métodos de cifrado.

El conjunto de todos los métodos de descifrado.

Para encriptar un mensaje, básicamente se ejecutan dos operaciones, la sustitución y la transposición.

Sustitución: Consiste en que a un caracter se le asigne otro. En el caso de los computadores, se toma un conjunto de bits, y se sustituye por otro. Como ejemplo se tiene al sistema de César, el cual utiliza una sustitución muy simple, en el que cada letra del alfabeto se corresponde con la que tiene un número k de puestos más adelante. El número utilizado es la secuencia cifrante del sistema.

Transposición: Transponer es desordenar los elementos del mensaje. El mensaje original se divide en subconjuntos, de tamaño fijo (el mismo tamaño para ambos extremos) y después se aplica al subconjunto una permutación, es decir "un desorden ordenado" de sus elementos.

La cantidad de veces que se realizan estas dos operaciones, su orden, la sucesión de los elementos de entrada al algoritmo, el tamaño de los bloques, la ubicación de la salida y las características de la secuencia cifrante y el uso de la clave, no se escogen al azar, sino de acuerdo a las propiedades matemáticas. El aprovechamiento de estas propiedades corresponde a un buen algoritmo criptográfico que las utilice.

A lo largo de la historia, se han utilizado cientos de criptosistemas diferentes, pero, a grandes rasgos se pueden dividir solamente en dos:

Criptosistemas simétricos o de clave privada.

Criptosistemas asimétricos o de clave pública.

Ambos sistemas en la práctica se suelen usar conjuntamente para alcanzar niveles de rápida ejecución, pues los simétricos podemos adelantar que

son bastante más rápidos en ejecución y los asimétricos son mas seguros, consiguiendo con su uso conjunto el nivel adecuado de seguridad.

a.- Sistemas Simétricos [6]

Los sistemas simétricos, son aquellos en los cuales se necesita una única clave para cifrar y descifrar mensajes entre el emisor y el receptor del mensaje, dicha clave debe ser acordada con anterioridad a la emisión del mismo para un correcto funcionamiento del sistema.

Los sistemas simétricos basan su seguridad en el tamaño de la clave a aplicar, es decir, a mayor tamaño de la clave usada, mayor seguridad se otorga.

FIGURA 2.2.- Sistemas de encriptación simétrica - Fuente: Propia Autoría.

En la Figura 2.2 se puede ver un diagrama esquemático del funcionamiento del sistema criptográfico simétrico:

El emisor (E) envía un mensaje, el cual entra al proceso de cifrado usando la clave simétrica previamente distribuida. Al final del proceso de cifrado se obtine el mensaje codificado conocido como criptograma, el cual para conocer su contenido se debe pasar por el proceso de descifrado aplicando la misma clave usada para el cifrado, al finalizar el descifrado, el receptor recuperará el mensaje inicial.

En la tabla 2.1 se presentan reseñas para los algoritmos más usados de cifrado simétrico:

TABLA 2.1.- Algoritmos más usados de cifrado simétrico - Fuente: Propia Autoría.

ALGORITMO	CLAVE (#BITS)	CARACTERÍSTICA BÁSICA
FEISTEL	Por lo general 64	Padre de los cifradores simétricos en bloques.
LUCIFER	128	Es un algoritmo del tipo Feistel y posteriormente dará paso a DES.
DES	56	Algoritmo tipo Feistel que se convirtió en estándar, actualmente no se usa debido a su vulnerabilidad.
LOKI	64	Algoritmo similar a DES.
RC5	Variable	Algoritmo muy rápido debido a su arquitectura simple, sus bajos requisitos de memoria y alta seguridad.
CAST	64	Inmune a ataques por criptoanálisis diferencial y lineal.
BLOWFISH	Variable	Algoritmo de tipo Feistel propuesto por Bruce Schneier.
IDEA	128	Algoritmo que es inmune ante un criptoanálisis diferencial.

SKIPJACK 80 Algoritmo usado para comunicaciones oficiales en USA, es inseguro ya que posee Backdoor .

Rijndael o AES 128 o más Algoritmo más usado y es actualmente un estándar mundial.

Los sistemas simétricos son más rápidos en la operación de cifrado y descifrado de mensajes en comparación con los sistemas asimétricos, esto es debido a la simplicidad de sus operaciones, las cuales pueden ser por sustitución de caracteres o algunas operaciones básicas de matemáticas como por ejemplo el operador lógico XOR.

Los sistemas simétricos fueron los más usados en la antigüedad, sin embargo, presentan las siguientes debilidades:

Inadecuada gestión de claves: para un número de usuarios n son necesarias ∑_(i_0)^(n-1)▒i claves distintas, es decir, para seis usuarios distintos el sistema debería manejar quince claves distintas, lo que implica cinco claves para cada usuario y cada clave distinta una de la otra, esto se puede apreciar de mejor manera en la Figura 2.3.

La inexistencia de una manera fácil y sencilla de firmar mensajes, aunque éstos se pueden llegar a autentificar mediante marcas.

FIGURA 2.3.- Distribución de claves simétricas – Fuente: CERTICOM [9].

Inadecuada forma de distribuir la clave a ocupar para cifrar y descifrar mensajes, esto es debido a que para la transmisión de claves se ocupa un método de transmisión inseguro ya sea Internet, teléfono, correo u otro método similar, la manera más segura de transmitir una clave que se ocupará para cifrar y descifrar mensajes es entregarla personalmente, pero en ese caso es preferible entregar inmediatamente el mensaje y no realizar el método de cifrado y descifrado.

b.- Sistemas Asimétricos [6]

Los sistemas asimétricos, son aquellos en los cuales se necesitan dos claves para cifrar y descifrar mensajes entre el emisor y el receptor del mensaje, tanto el emisor como el receptor poseen un par de claves, de éstas una será de tipo público donde da lo mismo que todo el mundo la conozca, y la otra será de tipo privado (la cual se tiene que proteger); y, para enviar mensajes el emisor tiene que cifrar el mensaje con la clave pública del receptor, para que así el receptor sea el único que pueda descifrar el mensaje usando su clave privada, cabe destacar que tanto la clave pública como la privada son inversas entre si dentro de un cuerpo multiplicativo, en la Figura 2.4 se muestra cómo funciona el intercambio de claves en los sistemas asimétricos.

FIGURA 2.4.- Distribución de claves asimétricas – Fuente: CERTICOM [9].

Los sistemas asimétricos basan su seguridad en las funciones matemáticas del tipo unidireccional, es decir que son fáciles de calcular en un sentido pero en el otro sentido complica mucho el cálculo.

En la Figura 2.5 se puede ver un diagrama esquemático de funcionamiento del sistema criptográfico asimétrico:

FIGURA 2.5.- Sistemas de encriptación asimétricos – Fuente: Propia Autoría.

El receptor publica su clave pública mediante cualquier medio, ya sea por Internet o publicado en algún diario u otro medio similar y es tomado por el emisor del mensaje y cifra el mensaje con esta clave, luego envía el criptograma mediante cualquier canal de transmisión, el receptor toma el criptograma lo descifra con su clave privada y obtiene así el mensaje.

En la tabla 2.2 se presentan reseñas para los algoritmos más usados de cifrado asimétrico:

TABLA 2.2.- Algoritmos más usados de cifrado asimétrico – Fuente: Propia Autoría

ALGORITMO CLAVE (#BITS) CARACTERÍSTICA BÁSICA

DSA Cualquier factor de 64 entre 512 y 1024. Algoritmo con el cual firmaba documentos el gobierno federal de USA.

EL GAMAL No trabaja con tamaños de bits, sino que trabaja bajo el cuerpo de un número primo grande. Algoritmo basado en Diffie-Hellman, también basado en el problema del logaritmo discreto.

POHLIG Y HELLMAN No trabaja con tamaños de bits- Esquemas Numéricos Logarítmicos. Algoritmo de cifra de clave secreta y que basa su seguridad en el problema del logaritmo discreto.

DIFFIE-HELLMAN No trabaja con tamaños de bits, sino que se selecciona un grupo multiplicativo (con inverso) p y un generador α de dicho primo, ambos valores públicos. Algoritmo de intercambio de claves de sesión.

RSA Superior a 1024 bits y se basa en la distribución de la elección de los primos p y q. Algoritmo de cifrado de bloque más usado en la actualidad.

ECC Se recomienda un tamaño de clave superior a los 80 bits. Algoritmo que es una variante de los sistemas asimétricos ya que ocupan las curvas elípticas para cifrar.

Los sistemas asimétricos son los más usados en la actualidad, sin embargo, se le pueden asociar las siguientes debilidades:

Para una misma longitud de clave y mensaje se necesita mayor tiempo de procesado de información, en comparación con un algoritmo de cifrado simétrico.

Las claves asimétricas deben ser de mayor tamaño que las claves simétricas, para así garantizar la autenticidad e integridad del mensaje.

El mensaje cifrado ocupa más espacio que el original.

Se cifran números, no se cifran mensajes, por lo mismo los mensajes hay que pasarlos por alguna función HASH como SHA-1 o MD5 antes de cifrar el mensaje.

c.- Comparación entre Criptosistemas Simétricos y Asimétricos

Diversos sistemas criptográficos han sido desarrollados a lo largo de la historia. Sólo un grupo reducido de esos sistemas son considerados realmente seguros en la actualidad. No obstante, el auge de las redes y la proliferación de servicios a través de éstas han ejercido presión en el área de la criptografía, en demanda de tecnologías que garanticen altos niveles de seguridad.

Al analizar las actuales técnicas criptográficas, es posible determinar aspectos que evidencian ciertas de sus debilidades frente a los nuevos retos de la criptografía. No se trata de demostrar la inseguridad de los sistema actuales, sino de poner en relieve su grado de adaptación a los nuevos desafíos criptográficos.

Los problemas fundamentales de los criptosistemas simétricos en relación a los criptosistemas asimétricos son [2]:

El problema de la seguridad (Shanonn 1949, Bell System Journal). Shanonn dio una definición de lo que es la seguridad de un criptosistema; definió la seguridad incondicional, ésta se establece cuando un criptosistema es seguro con independencia de los medios disponibles (infinita potencia de cálculo). Si un criptosistema es incondicionalmente seguro no se puede romper. Se demostró la existencia de criptosistemas de seguridad incondicional (cifrar de Vernann) aunque para el caso práctico no tienen utilidad. Los criptosistemas más modernos se basan en la seguridad computacional. La idea es considerar un criptosistema computacionalmente seguro cuando aunque haya un algoritmo que rompa el sistema éste requiera un tiempo de computación tan grande que sea inviable llevarlo a la práctica. Dentro de este punto, se debe mencionar que los criptosistemas clásicos o simétricos a la fecha han sido vulnerados o rotos lo que no permiten garantizar su efectividad.

El problema del manejo y distribución de claves. Los criptosistemas simétricos son de clave secreta, cualquiera que conozca la clave puede descifrar la información. Estos criptosistemas son vulnerables aunque no se sepa como criptoanalizarlos si se intercepta la clave secreta.

El problema de la autentificación. Los criptosistemas simétricos no proporcionan ningún método para que el receptor del mensaje pueda tener la seguridad de que quien envió el mensaje es quien debería haberlo enviado y no una tercera parte. El mensaje podría ser alterado y no se podría saber si esta situación se ha producido.

Lo expuesto, denota que los algoritmos simétricos a la fecha no permiten garantizar eficiencia y seguridad sobre el campo en estudio "Canales Electrónicos", razón por lo cual, el trabajo de tesis se limita al análisis de los criptosistemas asimétricos RSA y ECC que la fecha son considerados como invulnerables y de seguridad comprobada.

2.5.- CRIPTOSISTEMA RSA [2]

RSA es un Sistema Criptográfico de Claves Públicas y Autenticación que usa un algoritmo desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, el algoritmo RSA es el más usado en Internet, es parte de los navegadores como Netscape e Internet Explorer, así como de muchos otros más. Es un algoritmo utilizado tanto para encriptar información como para firmas digitales. En los sistemas de firma digital se utilizan para garantizar que el autor de la información es el firmante y no ha sido modificada por un tercero. La clave puede tener una longitud variable y puede ser tan grande como se desee y se pueda generar.

En lugar de emplear una sola clave para encriptar y desencriptar datos, el sistema RSA emplea un par combinado de claves que desarrolla una transformación en un solo sentido. Cada clave es la función inversa de la otra, es decir, lo que una hace, sólo la otra puede deshacerlo. La Clave Pública en el sistema RSA es publicada por su propietario, en tanto que la Clave Privada es mantenida en secreto. Para enviar un mensaje privado, el emisor lo encripta con la Clave Pública del receptor deseado. Una vez que ha sido encriptado, el mensaje sólo puede ser descifrado con la Clave Privada del receptor. Inversamente, el usuario puede encriptar datos utilizando su Clave Privada; es decir, las claves del sistema RSA pueden ser empleadas en cualquier dirección. Esto sienta las bases para la firma digital. Si un usuario puede desencriptar un mensaje con la Clave Pública de otro usuario, éste debe, necesariamente, haber utilizado su Clave Privada para encriptarlo originariamente. Desde el momento que solamente el propietario puede utilizar su propia Clave Privada, el mensaje encriptado se transforma en una especie de firma digital, un documento que nadie más ha podido crear. Bajo RSA se desarrolló el algoritmo estándar de firmas digitales para correos S/MIME (Extensiones de Correo de Internet de Propósitos Múltiples / Seguro).

RSA emplea las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo.

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta , el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga

computacional lo suficientemente grande para que este tipo de ataque sea viable. Sin embargo, se ha de notar que, el hecho de aumentar la longitud de las claves RSA no supone ninguna dificultad tecnológica.

TABLA 2.3.- Resumen de longitudes de claves del criptosistema RSA.

Fuente: CCN – 2012.

N·	CARACTERÍSTICAS	NIVEL BAJO	NIVEL MEDIO	NIVEL ALTO
01	Protección de la Confidencialidad.	No se aplica.	Permitido Claves ≥ 2048 bits	Permitido Claves ≥ 2048 bits
02	Protección de la autenticidad y de la integridad	No se aplica.	Permitido Claves ≥ 2048 bits	Permitido Claves ≥ 2048 bits
03	Cifrado de la			

Información No se aplica. No se aplica Permitido

Claves ≥ 2048 bits

04 Protección de

las claves

criptográficas Permitido

Claves ≥ 2048 bits Permitido

Claves ≥ 2048 bits Permitido

Claves ≥ 2048 bits

N· FIRMA ELECTRÓNICA NIVEL BAJO NIVEL MEDIO NIVEL ALTO

01 RSA Permitido

Claves ≥ 1024 bits Permitido a corto plazo

Claves ≥ 1024 bits Permitido

Claves ≥ 2048 bits

Considerando las longitudes de claves, la Tabla 2.3 contempla un cuadro resumen de longitudes de claves de criptosistemas basados en algoritmos RSA y resumen de longitudes de claves de criptosistemas RSA en esquemas de firma electrónica.

2.5.1.- Funcionamiento – Criptosistema RSA [4]

Como todo criptosistema de clave pública, el protocolo del criptosistema RSA tiene tres partes:

(a) Generación de claves

(b) Cifrado del mensaje

(c) Descifrado del mensaje

2.5.1.1.- Generación de claves

Se eligen dos números primos p y q suficientemente grandes.

Se calcula n como producto n = pq y se considera como conjunto de mensajes a utilizar el grupo multiplicativo Z_n^* cuyo orden es Φ (n), donde Φ (n), es la función indicador de Euler,

$$\Phi(n) = \Phi(pq) = (p-1)(q-1).$$

Se elige e Є Z, tal que $1 < e < \Phi(n)$ de modo que sea primo con el orden del grupo, es decir

$$mcd(e, \Phi(n)) = 1.$$

Donde mcd, se denota al mayor de sus divisores comunes

Mediante el algoritmo de Euclides extendido se calcula el inverso de e en Z_(Φ (n)))^* , es decir, se calcula d ∈ Z tal que

ed = 1 (mod Φ (n)),

con 1 < d < Φ (n).

La clave pública está constituida por la pareja (n, e) y la clave privada es el número d. Los números p, q, Φ (n) también deben permanecer secretos.

Definición 2.1: Los valores e y d se denominan exponente de cifrado y exponente de descifrado, respectivamente.

Definición 2.2: El entero n se denomina módulo del criptosistema RSA.

En ocasiones, en lugar de utilizar el valor Φ (n) = Φ (pq) = (p−1)(q−1), se utiliza el valor λ = mcm(p−1, q−1), que es conocido como exponente universal de n, donde mcm es el mínimo común múltiplo bajo matemática modular.

En cualquier caso, si p y q se eligen de forma aleatoria, se espera que mcd(p−1, q−1) sea pequeño y, por tanto, Φ (n) y λ sean aproximadamente del mismo tamaño.

2.5.1.2.- Cifrado de mensajes

Si un usuario U desea enviar un mensaje m a otro usuario V , debe realizar las operaciones siguientes:

Obtiene la clave pública de V , (nV , eV).

Representa el mensaje m como un elemento de Z_nV^*, , es decir, como un entero de rango {0, 1, 2, . . . , nV − 1}.

Envía a V el valor del criptograma c = meV (mod nV).

En RSA los mensajes que se transmiten son elementos de Z_n^* y si se desea transmitir un mensaje más largo, se debe dividir en bloques de tal manera que cada bloque sea un elemento de Z_n^*.

2.5.1.3.- Descifrado de mensajes

Para recuperar el mensaje original m, el usuario V utiliza su clave privada dV y calcula:

CdV (mod nV) = (meV)dV (mod nV) = meV dV (mod nV) = m.

EJEMPLO [4]

Se utilizan primos pequeños para ejemplificar el método RSA.

Determinación de la clave

El usuario V elige dos número primos de forma secreta, los multiplica para obtener n, y determina el indicador de Euler

$p = 383, q = 521,$

$n = pq = 383 \cdot 521 = 199543,$

$\Phi(n) = (p - 1)(q - 1) = 382 \cdot 520 = 198640$

Elige el exponente de cifrado, $2 < e < 198640$, por ejemplo $e = 3$ y comprueba que

$mcd(3, 198640) = 1.$

Utiliza el algoritmo de Euclides extendido para obtener el inverso

$198640 = 66213 \cdot 3 + 1,$

de donde

$-66213 \cdot 3 \pmod{198640} = 132427 \cdot 3 \pmod{198640} = 1,$

es decir, $d = 132427$.

Finalmente, el usuario V da a conocer su clave pública,

$(n, e) = (199543, 3)$

manteniendo oculta su clave privada $d = 132427$, así como los restantes valores, $p = 383$, $q = 521$ y $\Phi(n) = 198640$.

Cifrado del mensaje en claro

Si el usuario U desea enviar el mensaje “RSA” a V, realiza los siguientes pasos:

Obtiene la clave pública de V, (199543, 3).

Codifica el mensaje a enviar como un número menor que n = 199543. Para ello se considera la tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Se emplea base 26 para representar cualquier palabra. De este modo:

$263 = 17576 < n = 199543 < 456976 = 264$,

es decir, cada mensaje parcial puede contener como máximo 3 caracteres.

En el ejemplo R → 17, S → 18, A → 0, con lo que el mensaje es

RSA → $m = 17 \cdot 262 + 18 \cdot 26 + 0 = 911$

A continuación el usuario U cifra m calculando:

$$c = m^e \pmod{n}$$

$$= m^3 \pmod{n}$$

$$= m^2 m \pmod{n}$$

$$= 9112 \cdot 911 \pmod{199543}$$

$$= 31749 \cdot 911 \pmod{199543}$$

$$= 189147$$

Transforma este número a base 26 para convertirlo en caracteres,

$189147 = 26 \cdot 7274 + 23,$

$7274 = 26 \cdot 279 + 20,$

$279 = 26 \cdot 10 + 19,$

de donde

$c = 189147 = 10 \cdot 263 + 19 \cdot 262 + 20 \cdot 26 + 23\ 7 \rightarrow$ KTUX

Descifrado del mensaje

Una vez que el usuario V recibe el criptograma enviado por U: "KTUX", lo representa como un número en base 26, obteniendo c = 189147 y procede del siguiente modo:

Utiliza su clave privada d = 132427 y calcula:

m = cd (mod n) = 189147132427 (mod 199543)

Como

d = 132427

= 10000010101001011(2)

= 217 + 210 + 28 + 26 + 23 + 2 + 1,

el usuario V realiza las siguientes potencias (módulo n)

1891472 (mod 199543) = 189147 · 189147 (mod 199543) = 124053,

1891472^2 (mod 199543) = 1240532 (mod 199543) = 191106,

1891472^3 (mod 199543) = 1911062 (mod 199543) = 145661,

1891472^4 (mod 199543) = 1456612 (mod 199543) = 118817,

. . . . . .

1891472^17 (mod 199543) = 1730012 (mod 199543) = 90974

A continuación se multiplica las potencias que aparecen reduciendo módulo n después de cada producto, es decir:

189147 · 124053 (mod 199543) = 190964,

190964 · 145661 (mod 199543) = 112090,

112090 · 133139 (mod 199543) = 128626,

$128626 \cdot 188504 \pmod{199543} = 45574,$

$45574 \cdot 18 \pmod{199543} = 22160,$

$22160 \cdot 90974 \pmod{199543} = 911$

Finalmente recupera el mensaje original sin más que escribir el valor obtenido

$m = 911$ en base 26, es decir:

$m = 911 = 17 \cdot 262 + 18 \cdot 26 + 0 \rightarrow$ RSA

2.5.2.- Firma digital en RSA [4]

Para firmar digitalmente un mensaje, el remitente debe llevar a cabo determinados cálculos con el mensaje que desea enviar y con su clave privada. De este modo, cada mensaje lleva su propia firma y se puede comprobar que el remitente es el único que lo ha podido firmar, dado que es el único que posee su clave privada.

La firma digital del esquema RSA es explícita (añadida como una marca inseparable al mensaje), pública (permite identificar al remitente ante cualquier persona) e irrevocable porque el receptor puede probar que el remitente escribió el mensaje.

El protocolo de firma digital consta de dos partes: la firma del mensaje y el proceso de verificación.

Sean (nU, eU) y dU las claves pública y privada, respectivamente, de un usuario U, y sean (nV , eV) y dV , las claves del usuario V .

Si el usuario U desea enviar, junto con el criptograma c del mensaje m, su firma digital para ese mensaje, procede a ejecutar el siguiente protocolo:

Calcula mediante el exponente de descifrado, dU, el valor de

$$r = m^{dU} \pmod{nU},$$

que es la rúbrica para el mensaje m.

Luego cifra el valor anterior con la clave pública de V ,

$$s = r^{eV} \pmod{nV}.$$

El mensaje cifrado que el usuario U envía a V es la pareja (c, s) y es claro que solo U puede firmar el mensaje, dado que es el único que conoce su clave privada dU.

Para que V pueda verificar que la firma corresponde a U solo tiene que ejecutar los siguientes pasos:

Recupera la rúbrica del usuario U para el mensaje m calculando:

$$s^{dV} \pmod{nV} = (r^{eV})^{dV} \pmod{nV} = r^{eV\,dV} \pmod{nV} = r.$$

Posteriormente V comprueba si la rúbrica cifrada coincide con el mensaje

$$r^{eU} \pmod{nU} = m^{dUeU} \pmod{nU} = m.$$

En el caso de que el resultado anterior no coincida con el valor de m obtenido en el proceso de descifrado, el mensaje original es rechazado.

El ataque contra el protocolo de la firma digital de un mensaje con el criptosistema RSA es el mismo que el utilizado para romper el propio criptosistema, dado que en ambos se realizan las mismas operaciones.

2.5.3.- Seguridad – Criptosistema RSA

La seguridad del criptosistema RSA está basado en dos problemas matemáticos: el problema de factorizar números grandes y el problema RSA. El descifrado completo de un texto cifrado con RSA es computacionalmente intratable, no se ha encontrado un algoritmo eficiente todavía para ambos problemas. Proveyendo la seguridad contra el descifrado parcial podría requerir la adición de una seguridad padding scheme .

La factorización de números grandes por lo general proponen métodos teniendo 663 bits de longitud usando para ello métodos distribuidos avanzados. Las claves RSA son normalmente entre 1024-2048 bits de longitud. Algunos expertos creen que las claves de 1024 bits podrían comenzar a ser débiles en poco tiempo, considerando que con claves de 4096 bits ya se tiene registros a la fecha de que han sido vulneradas. Un dispositivo hardware teórico llamado TWIRL descrito por Shamir y Tromer en el 2003, cuestionó a la seguridad de claves de 1024 bits. Es actualmente recomendado que n sea como mínimo de 2048 bits de longitud.

En 1993, Peter Shor publicó su algoritmo, mostrando que una computadora cuántica podría en principio mejorar la factorización en tiempo polinomial, mostrando RSA como un algoritmo obsoleto. Sin embargo, las

computadoras cuánticas no se esperan que acaben su desarrollo hasta dentro de muchos años.

2.6.- CRIPTOGRAFÍA DE CURVAS ELÍPTICAS [5]

La Criptografía de Curva Elíptica es una de las disciplinas más prometedoras en el campo de los cifrados asimétricos. Las curvas elípticas constituyen un formalismo matemático conocido y estudiado desde hace más de 150 años, y presentan una serie de propiedades que da lugar a problemas difíciles, análogos a los que presentaba la aritmética modular, lo cual las hace válidas para aplicar algunos de los algoritmos asimétricos más conocidos. Si bien su estructura algebraica es algo compleja, su implementación suele resultar tanto o más eficiente que la aritmética modular, y además con claves mucho más cortas se puede alcanzar el mismo nivel de seguridad que con otras técnicas.

Las primeras propuestas de uso de las curvas elípticas en Criptografía fueron hechaspor Neal Koblitz y Victor Miller en 1985. Precisamente el principal argumento que esgrimen los detractores de estas técnicas es que, si bien las curvas elípticas han sido objeto de estudio y análisis durante más de un siglo, las propiedades que pueden estar directamente relacionadas con su calidad como base para un sistema criptográfico, apenas llevan quince años siendo consideradas.

La criptografía de curvas elípticas (CCE) fundamenta su seguridad en el alto grado de dificultad que supone resolver el problema del logaritmo discreto en el grupo abeliano formado por curvas elípticas definidas sobre campos finitos.

De forma general, una curva elíptica E(Fq) se define como el conjunto de puntos que satisface la ecuación:

E : y2 = x3 + ax + b;

donde a y b están en un campo finito apropiado Fq de orden q, el cual puede ser el grupo de los números racionales, números complejos, enteros módulo n, campos de Galois, etc. Los coeficientes a y b caracterizan de manera unívoca cada curva.

Se define también un punto en el infinito, denotado como ϑ, a un punto imaginario situado por encima del eje de las abcisas a una distancia infinita, y que por lo tanto no tiene un valor concreto. Existe en el grupo la suma y una operación conocida como multiplicación escalar: si k es un entero y P ∈ E(Fq) es un punto, entonces kP es el punto obtenido al sumar k copias de P. El elemento neutro es ϑ .

(a)

(b)

FIGURA 2.6.- Graficas de curvas elípticas: a) y2 = x3 - 10x+7 sobre R; b) y2+xy = x3+g4x2+1 sobre F(24)

Las curvas elípticas definidas en un Campo de Galois GF(P), siendo P un número primo, forman un grupo donde todos los elementos, con excepción del cero, tienen inversa, por lo que se puede sumar, restar, multiplicar y dividir. Los puntos de estas curvas cumplen la ecuación:

$$y2 = x3 + ax + b \pmod{P}$$

definiendo de esta forma el grupo E(GF(P)).

En la figura 2.6 se muestran curvas elípticas definidas en el conjunto R, y en el campo F(24).

Tómese un punto G cualquiera de una curva elíptica E. Se denominará G al conjunto { ϑ, G, 2G, 3G,…, }. En E(GF(P)) y E(GF(2m)) los conjuntos de esta naturaleza deberán necesariamente ser finitos, ya que el número de puntos de la curva es finito. Por lo tanto, si se dispone de un punto Q ∈ G, debe existir un número entero k tal que kG = Q.

El problema de logaritmo discreto para las curvas elípticas consiste en hallar el número k a partir de G y Q.

Debido a la enorme complejidad computacional que dicho problema matemático representa, es posible obtener con CCE niveles de seguridad similares a los proporcionados por sistemas de cifrado de campos finitos. Las operaciones sobre campos finitos menores conducen al uso de llaves publicas y secretas también menores lo que a su vez tiene como resultado una mayor velocidad, y menores requerimientos de memoria y de poder de cómputo en las implementaciones de los algoritmos que conforman al esquema.

La principal característica que tienen los sistemas sobre curvas elípticas es que el PLDE es totalmente exponencial, es decir no existe un algoritmo eficiente que calcule logaritmos discretos. Esto permite usar claves de longitud reducida en los sistemas criptográficos que los usan. Vale entonces realizar la siguiente comparación:

Claves CCE de 163bits = claves RSA de 1024b

Claves CCE de 224bits = claves RSA de 2048b

La Tabla 2.4 contempla un cuadro resumen de longitudes de claves de criptosistemas basados en curvas elípticas y resumen de claves en esquemas de firma electrónica.

TABLA 2.4.- Resumen de longitudes de claves - Curvas Elípticas. Fuente: CCN

N·	CARACTERÍSTICAS	NIVEL BAJO	NIVEL MEDIO	NIVEL ALTO
01	Protección de la Confidencialidad.	No se aplica.	Permitido Claves: 224-255 bits.	Permitido Claves ≥ 256 bits.
02	Protección de la autenticidad y de la integridad	No se aplica.	Permitido	

Claves: 224-255 bits. Permitido

Claves ≥ 256 bits.

03 Cifrado de la

Información No se aplica. No se aplica Permitido

Claves ≥ 256 bits.

04 Protección de

las claves

criptográficas Permitido

Claves: 224-255 bits. Permitido

Claves: 224-255 bits. Permitido

Claves ≥ 256 bits.

N· FIRMA ELECTRÓNICA NIVEL BAJO NIVEL MEDIO NIVEL ALTO

01 ECC Permitido

Claves: 224-255 bits Permitido) a corto plazo

Claves: 224-255 bits Permitido

Claves: 256-283 bits.

Para el caso de la implementación hay que contar con buenos programas que realicen la aritmética del campo finito, además de buenos algoritmos que sumen puntos racionales, tanto en el caso de Zp como F2n, en este último se toma una base polinomial que tenga el mínimo de términos por ejemplo un trinomio para generar los elementos del campo finito esto si la implementación es en software, y se toma una base normal si es en hardware. Además de contemplar que las operaciones de puntos racionales pueden hacerse en el espacio proyectivo, esto elimina el hacer divisiones, ahorrando tiempo.

Lo anterior se ve reflejado en las ventajas que ofrecen los CCE en comparación con RSA, la principal es la longitud de la clave secreta. Se puede mostrar que mientras en RSA se tiene que usar una clave de 1024 para ofrecer una considerable seguridad, los CCE solo usan 163 bits para ofrecer la misma seguridad, así también las claves RSA de 2048 son equivalentes en seguridad a 210 de CCE. Esto se debe a que para resolver el PLDE el único algoritmo conocido toma tiempo de ejecución totalmente exponencial.

Lo anterior permite que los Criptosistemas de Curva Elíptica sean idóneos para ser implementados en donde el poder de cómputo y el espacio del circuito sea reducido, donde sea requerida una alta velocidad de procesamiento o grandes volúmenes de transacciones, donde el espacio de almacenamiento, la memoria o el ancho de banda sea limitado. Lo que permite su uso en Smart Cards, Teléfonos celulares, Fax, Organizadores de Palma, PCs, etcétera.

En la actualidad existen varios estándares que permiten el uso adecuado y óptimo de los CCE, entre los cuales se encuentran: IEEE P1363 (Institute of Electrical and Electronics Engineers), el ANSI X9.62, ANSI X9.63, ANSI TG-17,

ANSI X12 (American National Standards Institute), UN/EDIFACT, ISO/IEC 14888, ISO/IEC 9796-4, ISO/IEC 14946 (International Standards Organization), ATM Forum (Asynchronous Transport Mode), WAP (Wireless Application Protocol). En comercio electrónico: FSTC (Financial Services Technology Consortion), OTP 0.9 (Open Trading Protocol), SET (Secure Electronic Transactions). En internet IETF (The Internet Engineering Task Force), IPSec (Internet Protocol Security Protocol).

FIGURA 2.7.- Modelo por capas de un Criptosistema de Curvas Elípticas. FUENTE: [5]

Los CCE son el mejor candidato para la implementación de esquemas de firma digital, intercambio de claves simétricas y otros. La figura 2.7, permite observar cómo se encuentra compuesta una aplicación que utiliza criptografía de llave pública con curvas elípticas. La capa superior representa la aplicación que se desarrolla, los dos siguientes niveles representan los protocolos de seguridad que se emplean dentro de la aplicación y las primitivas de la firma/verificación. Los siguientes niveles representan las primitivas de curvas elípticas y las primitivas de la aritmética de campos finitos. Estas últimas capas representan la base para realizar un criptosistema de curvas elípticas. Es en las dos primeras capas y parte de la tercera, en lo que se enfoca el presente trabajo de tesis.

2.6.1.- Funcionamiento - ECC [2]

De forma análoga a otros criptosistemas de clave pública, los ECC constan de tres fases:

(a) Generación de claves

(b) Cifrado del mensaje

(c) Descifrado del mensaje

2.6.1.1.- Generación de Claves

Si el usuario A desea generar sus claves para un criptosistema de curvas elípticas, debe seguir los siguientes pasos:

A genera una curva elíptica, E, sobre el cuerpo finito Fq de modo que la representación binaria de q tenga, al menos, 160 bits.

A elige un generador de la curva, G, cuyo orden sea primo, p, con $p \approx q$.

A genera un número aleatorio a, con $1 < a < p-2$, y calcula el valor del punto de la curva $a \cdot G$.

La clave pública de A es el conjunto (Fp, E, G, $a \cdot G$) y su clave privada es el número a.

2.6.1.2.- Cifrado de Mensajes

Si el usuario B desea cifrar un mensaje m para A, seguirá el siguiente protocolo:

B obtiene la clave pública de A: (Fp, E, G, a·G).

B representa el mensaje m como un punto de la curva E, es decir, transforma m en M = (m1, m2)∈E, con m1, m2∈Fp.

B genera un número aleatorio x, 1 < x < p−2, calcula los puntos de la curva dados por P = x·G,

Q = M+x·(a·G),

y envía a A el criptograma, que está formado por c = (P, Q).

En este caso, el factor de expansión del criptosistema de curvas elípticas es 2, dado que cada criptograma está formado por dos puntos de la curva, mientras que lo que se cifra es sólo un punto. Sin embargo, su tamaño en bits es menor que en el caso de ElGamal, dado que p es sólo de 160 bits.

En general, para ahorrar tiempo en las comunicaciones, se suele recomendar el uso de una representación comprimida de los puntos de la curva. En efecto, como la ecuación de la curva es conocida, para definir un punto Z = (z1, z2), es suficiente con dar su coordenada z1 y un bit de la coordenada z2, no todo el valor de z2. De hecho, si la representación de un punto de la curva es Z = (z1, 0), la representación de su punto opuesto, –Z, es – Z = (z1, 1). De esta manera para representar un punto de la curva sólo son necesarios p+1 bits.

2.6.1.3.- Descifrado de Mensajes

Una vez que el destinatario A recibe el criptograma c = (P, Q), para recuperar el mensaje original, m, realiza los siguientes pasos:

A utiliza su clave privada, a, para calcular

$R = a \cdot P = a(x \cdot G) = a \cdot x \cdot G.$

A obtiene el punto de la curva original sumando al segundo punto del criptograma, el punto opuesto del obtenido anteriormente:

$Q+(-R) = M+x \cdot (a \cdot G)+(-a \cdot x \cdot G) = M+x \cdot a \cdot G-a \cdot x \cdot G = M$

2.6.2.- Algoritmo de firma digital con curvas elípticas [5]

El algoritmo de firma digital con curvas elípticas, ECDSA por sus siglas en inglés "Elliptic Curve Digital Signature Algorithm", es el análogo para la criptografía de llave pública de curvas elípticas y DSA. Fue aceptado en 1999 como un estándar ANSI, y fue adoptado en 2000 por la IEEE y la NIST como estándar.

A diferencia de los problemas ordinarios de logaritmo discreto y problemas de factorización, no se conoce algún algoritmo de tiempo subexponencial para el problema de logaritmo discreto con curvas elípticas. Por esta razón, la fortaleza por cada bit de la llave es substancialmente mayor en un algoritmo que utiliza curvas elípticas.

Para firmar un mensaje m con ECDSA, una entidad A con parámetros de dominio D = (q, FR, a, b, G, n, h) y un par de llaves asociado (d;Q) hace lo siguiente:

Selecciona un entero aleatorio k, $1 \leq k \leq -1$

Calcular kG = (x1; y1) y convertir x1 a un entero x 1

Calcular r = x1 mod n. Si r = 0 entonces ir al paso 1.

Calcular k -1 mod n.

Calcular SHA - 1(m) y convertir esta cadena de bits a un entero e.

Calcular s = k-1(e + dr) mod n. Si s = 0 entonces ir a paso 1.

La firma de A para el mensaje m es (r, s).

Para verificar la firma con ECDSA de A de (r; s) sobre m, B obtiene una copia de los parámetros de dominio de A D = (q, FR, a, b, G, n, h) y la llave pública asociada Q. B entonces realiza lo siguiente:

Verificar que r y s sean enteros dentro del intervalo [1, n - 1].

Calcular SHA - 1(m) y convierte esta cadena de bits en un entero e.

Calcular w = s -1 mod n.

Calcular u1 = ew mod n y u2 = rw mod n.

Calcular X = u1G + u2Q.

Si X = 0, entonces rechazar la firma. De otro modo, convertir la x - coordenada x1 de X a un entero x¯1, y calcular v = x¯1 mod n.

Aceptar la firma si y sólo si v = r.

2.6.3.- Seguridad - ECC

Dado que el problema matemático sobre el que se fundamentan los ECC es el logaritmo discreto sobre curvas elípticas, existen ataques que son específicos de las curvas elípticas, dado que estas pueden elegirse sin las suficientes condiciones de seguridad.

A continuación se presentan los principales ataques contra los ECC.

Ataque por Fuerza Bruta. Este ataque contra el ECDLP consiste en probar todos los posibles valores de un entero k hasta que se obtenga la solución buscada k = a, es decir, hasta obtener el valor conocido de a·G, lo que permitiría conocer la clave privada del usuario al que se ataca. Este ataque puede evitarse si los parámetros del criptosistema se eligen con los tamaños recomendados para las claves, según los diferentes niveles de seguridad requeridos, de modo que el tiempo de computación necesario sea lo suficientemente elevado.

Ataque de POHLIG-HELLMAN [10]. El ataque trata de resolver el ECDLP en subgrupos de orden primo pequeño del grupo original, de modo que las soluciones parciales pueden ser luego complementadas mediante el Teorema

Chino del Resto para obtener la solución global. Con el fin de evitar este ataque, se recomienda que el orden de la curva elíptica definida sobre el cuerpo finito, #E, tenga un divisor primo grande, por ejemplo p, de modo que éste sea mayor que el máximo entre 2160 y 22·s–1, donde s es el nivel de seguridad deseado, en bits, es decir, uno de los siguientes valores: 80, 112, 128, 192, 256, etc. Dicho de otro modo, si se cumple que:

$$p > \max\{2160, 22 \cdot s - 1\}, \text{ donde } s \in \{80, 112, 128, 192, 256, \ldots\}.$$

Ataque de FREY y RÜCK [11]. Este ataque generaliza el ataque de Menezes, Okamoto y Vanstone [12] generalmente conocido como ATAQUE MOV. El ataque reduce el ECDLP definido sobre una curva elíptica a un DLP sobre conjuntos donde este problema es algo más sencillo de resolver. Ambos ataques pueden ser evitados si la curva elíptica se define sobre el cuerpo Fq, de modo que se verifique la siguiente condición: $q^i \neq 1 \pmod{n}$, para todo i, con $1 \leq i \leq 100$.

Ataques a Curvas Anómalas. Se dice que una curva elíptica definida sobre un cuerpo finito Fq es «anómala» si se cumple que el orden de la curva verifica #E = q. Semaev [13], Smart [14] y Satoh y Araki [15] mostraron que el ECDLP en curvas anómalas se puede resolver de modo eficiente. Por tal motivo, dichas curvas deben ser evitadas. Los ataques a curvas anómalas se puede prevenir si se verifica lo siguiente: $\#E \neq q$.

CAPÍTULO III

APLICACIONES CRIPTOGRÁFICAS

El presente capitulo cubre el estado del arte de la criptografía asimétrica enfocada a las aplicaciones de los algoritmos de curva elíptica. Cuando se lanzó el Criptosistema de Curvas Elíptica "ECC" en 1985 había mucho escepticismo sobre sus elementos de seguridad; actualmente, después de múltiples pruebas y técnicas criptoanalíticas, se ha logrado demostrar su eficiencia, al punto que diferentes proveedores han incorporado esta técnica en sus productos. En los últimos años RSA Security ha perfeccionado técnicas más eficientes de implementación de ECC, e incluso adquirió una patente con tiempos de rendimiento y transmisión optimizados. Este estándar se ha posicionado en comunicaciones móviles, PDA's y dispositivos inalámbricos. En la presente investigación se puede dilucidar ampliamente el uso de ECC en 4 categorías, así: Seguridad de Canales Electrónicos, smart cards, Redes Inalámbricos – Dispositivos Móviles y VPN's.

3.1.- SEGURIDAD DE CANALES TRANSACCIONALES [2]

Quizás la aplicación más antigua de la Criptografía sea precisamente la de establecer canales de comunicaciones seguros, considerando para ello protocolos de seguridad de comunicaciones de red y esquemas de autenticación como elementos relevantes.

Dentro de este marco se tiene que un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan o son interoperables con esquemas de seguridad criptográfica.

El ejemplo más común es el protocolo SSL (Secure Socket Layer) que fue creado desde el principio de la década de los noventa inicialmente por la compañía Netscape. Al finalizar esta década fue estandarizado por la IETF (Internet Engineering TaskForce) como TLS (Transpor tLayer Security); otro ejemplo es PGP (Pretty Good Privacy) que es un protocolo libre ampliamente usado de intercambio de correo electrónico seguro; uno más es el conocido y muy publicitado SET (Secure Electronic Transaction) que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito e IPsec que proporciona seguridad en la conexión de Internet a un nivel más bajo.

Éstos y cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad en canales de comunicación como la integridad, la confidencialidad, la autenticación y el no rechazo. Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Por otro lado, dentro del campo de estudio de autenticación, los servidores de las entidades financieras y de las administraciones públicas, tienen la opción de utilizar criptografía de clave simétrica junto con la criptografía de clave asimétrica. Al instalar un certificado relacionado con su clave, el computador del usuario, donde está un navegador, se conecta con el servidor. Si la dirección empieza con https, sabemos que la conexión es segura. Cuando se hace este tipo de conexión, el navegador del usuario le pregunta al servidor si es capaz de mantener conexiones seguras y el servidor le contesta que sí y le entrega su certificado al navegador. Con la información del certificado, el

navegador extrae la clave pública, y cifra con la clave pública una clave de sesión, se lo envía al servidor, que es el único que lo puede descifrar con su clave privada, a partir de ese momento, mantienen una sesión cifrada.

Los servidores web seguros tienen interés para el sector ABC, Administración electrónica, Banca electrónica y Comercio electrónico, porque en estos contextos es muy importante que la información que pasa por los canales transaccionales vaya cifrada, siendo éstos: números de tarjetas de crédito, datos confidenciales y datos personales protegidos por la Legislación Ecuatoriana. Dentro de este campo la tecnología de curvas elípticas permite que con tamaños de clave menores se tenga una robustez criptográfica superior deseada.

Entre las entidades proveedoras de los certificados de servidor necesarios para utilizar esta tecnología ECC se ha de destacar la norteamericana VeriSign y Thawte en Sudáfrica. En Ecuador EADTrust ha empezado a emitir certificados para servidores web. Además, debemos considerar que el Instituto Nacional de Normas y Tecnología de EE.UU. (NIST - National Institute of Standards and Technology) y la Unión Europea recomiendan el uso de curvas elípticas para proteger a los servidores de una manera más robusta.

3.1.1.- Protocolos de Comunicación Segura

3.1.1.1.- Protocolo SSL (Secure Sockets Layer) [2]

El protocolo SSL (Secure Sockets Layer), permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente. Se sitúa en la capa de aplicación, directamente sobre el protocolo TCP, y aunque puede

proporcionar seguridad a cualquier aplicación que corra sobre TCP, se usa principalmente para proporcionar seguridad a los protocolos HTTP (web), SMTP (email) y NNTP (news), dando lugar en el primero de los casos a los servidores web seguros, cuya URL comienza por el prefijo https://. Su fundamento consiste en interponer una fase de codificación de los mensajes antes de enviarlos a través de la red. Una vez que se ha establecido la comunicación, cuando una aplicación quiere enviar información a otra computadora, la capa SSL la recoge y la codifica, para luego enviarla a su destino a través de la red. Análogamente, el módulo SSL del otro ordenador se encarga de decodificar los mensajes y se los pasa como texto claro a la aplicación destinataria.

SSL también incorpora un mecanismo de autentificación que permite garantizar la identidad de los interlocutores. Típicamente, ya que este protocolo se diseñó originalmente para establecer comunicaciones web, el único que suele autentificarse es el servidor, aunque también puede realizarse una autentificación mutua.

Una comunicación a través de SSL implica tres fases fundamentalmente:

i. Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación, a partir del conjunto de algoritmos soportados por cada uno de los interlocutores.

ii. Intercambio de claves, empleando algún mecanismo de clave pública y autentificación de los interlocutores a partir de sus certificados digitales.

iii. Cifrado simétrico o asimétrico del tráfico.

Una de las ventajas de emplear un protocolo de comunicaciones en lugar de un algoritmo o algoritmos concretos, es que ninguna de las fases del protocolo queda atada a ningún algoritmo, por lo que si en el futuro aparecen algoritmos mejores, o alguno de los que se emplean en un momento dado quedara comprometido, el cambio se puede hacer sin modificar el protocolo.

En la actualidad, las implementaciones típicas de SSL soportan algoritmos como RSA, Diffie-Hellman o DSA y ECC para la parte asimétrica; RC2, RC4, IDEA, DES, TripleDES o AES para la simétrica, y como funciones SHA-1 o MD5.

Las ventajas de SSL son evidentes, ya que liberan a las aplicaciones de llevar a cabo las operaciones criptográficas antes de enviar la información, y su transparencia permite usarlo de manera inmediata sin modificar apenas los programas ya existentes.

Desde hace tiempo los principales navegadores de Internet incorporan un módulo SSL, que se activa de forma automática cuando es necesario. Hasta diciembre de 1999, debido a las restricciones de exportación de material criptográfico existentes en los EE.UU., la mayoría de los navegadores incorporaban un nivel de seguridad bastante pobre (claves simétricas de 40 bits), por lo que conviene comprobar qué nivel de seguridad se está empleando cada vez que hagamos una conexión. En respuesta de ello existen implementaciones de SSL que permiten construir los denominados túneles SSL basados en ECC, que permiten dirigir cualquier conexión a un puerto TCP a través de una conexión SSL previa, de forma transparente para las aplicaciones que se conectan.

3.1.1.2.- Protocolo TLS (Transport Layer Security) [2]

TLS (descrito en el documento RFC 2246) es un protocolo basado en la versión 3.0 de SSL, si bien con una serie de mejoras que lo hacen incompatible con este último. Una de las ventajas que proporciona sobre SSL es que puede ser iniciado a partir de una conexión TCP ya existente, lo cual permite seguir trabajando con los mismos puertos que los protocolos no cifrados. Mientras que SSL es un protocolo incompatible con TCP, lo cual significa que no podemos establecer una conexión de un cliente TCP a un servidor SSL ni al revés, y por tanto es necesario diferenciarlos utilizando distintos números de puerto (80 para un servidor web normal y 443 para un servidor web sobre SSL), con TLS puede establecerse la conexión normalmente a través de TCP y el puerto 80, y luego activar sobre el mismo el protocolo TLS.

En este protocolo se emplea una serie de medidas de seguridad adicionales, encaminadas a protegerlo de distintos tipos de ataque, en especial de los de intermediario:

- Uso de funciones MAC en lugar de funciones MDC únicamente.

- Numeración secuencial de todos los campos que componen la comunicación, e incorporación de esta información al cálculo de los MAC.

- Protección frente a ataques que intentan forzar el empleo de versiones antiguas —menos seguras— del protocolo o cifrados más débiles.

- El mensaje que finaliza la fase de establecimiento de la conexión incorpora una signatura (hash) de todos los datos intercambiados por ambos interlocutores.

Si bien el método usado con más frecuencia para establecer conexiones seguras a través de Internet sigue siendo SSL, cabe esperar que con el tiempo sea paulatinamente reemplazado por TLS, y que este último se convierta en el estándar de seguridad para las comunicaciones cifradas en Internet.

3.1.1.3.- Protocolos IPsec (Internet Protocol Security) [6]

IPsec es un estándar que proporciona cifrado y autentificación a los paquetes IP, trabajando en la capa de red. En lugar de tratarse de un único protocolo, IPsec es en realidad un conjunto de protocolos, definidos en diversos RFCs (principalmente en el 2401), encaminados a proporcionar autentificación, confidencialidad e integridad a las comunicaciones IP. Su carácter obligatorio dentro del estándar IPv6n—recordemos que en IPv4, la versión más empleada en la actualidad de este protocolo, es opcional— hará con seguridad que la popularidad de IPsec crezca al mismo ritmo que la implantación de la nueva versión del protocolo IP.

IPsec puede ser utilizado para proteger una o más rutas entre un par de ordenadores, un par de pasarelas de seguridad —ordenadores que hacen de intermediarios entre otros, y que implementan los protocolos IPsec— o una pasarela y un ordenador. En función del tipo de ruta que se proteja, se distinguen dos modos de operación:

- Modo túnel: Se realiza entre dos pasarelas de seguridad, de forma que éstas se encargan de crear una ruta segura entre dos ordenadores

conectados a ellas, a través de la cual viajan los paquetes. De este modo se puede disponer dentro de una red local de un ordenador que desempeñe las labores de pasarela, al que las computadoras de la propia red envíen los paquetes, para que éste les aplique los protocolos IPsec antes de remitirlos al destinatario —o a su pasarela de seguridad asociada—. Este modo permite interconectar de forma segura ordenadores que no incorporen IPsec, con la única condición de que existan pasarelas de seguridad en las redes locales de cada uno de ellos.

- Modo transporte: En este caso los cálculos criptográficos relativos a los protocolos IPsec se realizan en cada extremo de la comunicación.

Básicamente, IPsec se compone a su vez de dos protocolos, cada uno de los cuales añade una serie de campos, o modifica los ya existentes, a los paquetes IP:

- Cabecera de autentificación IP, abreviado como AH (IP Authenticacion Header), diseñado para proporcionar integridad, autentificación del origen de los paquetes, y un mecanismo opcional para evitar ataques por repetición de paquetes.

- Protocolo de encapsulamiento de carga de seguridad, o ESP (Encapsulating Security Payload) que, además de proveer integridad, autentificación y protección contra repeticiones, permite cifrar el contenido de los paquetes.

Debido a que algunos de los servicios que IPsec proporciona necesitan de la distribución e intercambio de las claves necesarias para cifrar, autentificar y verificar la integridad de los paquetes, es necesario que éste trabaje en consonancia con un conjunto externo de mecanismos que permita llevar a cabo esta tarea, tales como IKE, SKIP o Kerberos.

3.1.1.4.- Análisis de Aplicación Criptográfica – Protocolos De Comunicación

En la práctica, podemos encontrar protocolos encaminados a obtener comunicaciones seguras en prácticamente todos los niveles de los canales transaccionales, sin embargo de la evaluación efectuada se tiene que el protocolo TLS (Transport Layer Security) permite mayor eficiencia criptográfica empleando ECC.

El protocolo TLS se implanta o se divide en dos etapas fundamentales: inicio de sesión e intercambio de datos. El propósito del inicio de sesión es lograr que los nodos que desean establecer una comunicación segura acuerden las claves secretas necesarias para enviar y recibir datos durante la segunda etapa del protocolo. Para llevar a cabo esta tarea se utilizan algoritmos criptográficos de intercambio de claves y de firma digital, ambos basados en criptografía asimétrica (clave de cifrado difiere de la clave de descifrado). La segunda etapa utiliza las claves generadas durante el inicio de sesión para proteger los datos intercambiados entre los dos nodos. Durante esta etapa se utilizan algoritmos de cifrado simétrico y de chequeo de integridad.

Para este análisis se seleccionaron los algoritmos criptográficos utilizados en el protocolo TLS a implementar en hardware. Para realizar esta selección se tuvieron en cuenta los siguientes parámetros:

a. Cantidad de tiempo consumido por la ejecución del algoritmo.

b. Frecuencia de utilización de los algoritmos.

c. Selección realizada por otros fabricantes y desarrolladores.

La criptografía asimétrica consume mayor tiempo de procesamiento con respecto a los algoritmos simétricos comúnmente utilizados por el protocolo TLS. Una comparación de la misma con respecto a otros algoritmos se presenta en la tabla 3.1, donde los algoritmos RSA y ECDSA (Elliptic Curve Digital SignatureAlgorithm), consumen mucho más tiempo de procesamiento que el AES-256-CBC (cifrado simétrico) y la función hash SHA-512. Por otra parte se debe clarificar que los algoritmos RSA y ECDSA (basados en criptografía asimétrica) en la práctica solamente son utilizados durante el inicio de una sesión TLS.

TABLA 3.1.- Consumo de tiempo de distintos algoritmos presentes en el protocolo TLS – Fuente: CITI

RSA - 4096 ECDSA-571 AES-256 SHA-512

20 s

(firma)8.3 s (Verificación) 6 ms

(1500 bytes) 18 ms

(1500 bytes)

Otro de los aspectos que se han tenido en cuenta durante la selección de los algoritmos a implementar está relacionado con decisiones que han tomado algunos fabricantes e investigadores en relación a este tema. Es muy común encontrar reportes de implementaciones muy rápidas de los algoritmos que utilizan criptografía asimétrica para aquellos sistemas de cómputo que necesiten manejar varias conexiones TLS al mismo tiempo, como es el caso de servidores de redes privadas virtuales, servidores de transferencias bancarias, etc. Por otra parte, los algoritmos de cifrado simétrico y las funciones hash (los utilizados durante la etapa de intercambio de datos en TLS) se encuentran implementados en sistemas de cómputo que tienden a manejar menor cantidad de conexiones con relación a la cantidad de información que intercambian con el otro extremo de la conexión.

3.1.2.- Autenticación - Firmas y Certificados Digitales

Cuando se establece una comunicación de cualquier tipo, es necesario poder asegurar que los mensajes no han sufrido alteraciones, es decir, que la información recibida coincide exactamente con la enviada. En muchos casos, existe el requerimiento adicional de conocer la identidad de nuestro interlocutor para evitar que sea suplantado por un impostor. Denominaremos en general autentificación (o autenticación) a las operaciones consistentes en verificar tanto la identidad de nuestro interlocutor como la integridad de los mensajes que de él recibimos.

Independientemente de que la operación de autentificación se lleve a cabo sobre el contenido de una comunicación o sobre los propios interlocutores, ésta puede realizarse en el mismo momento, de forma interactiva, como cuando se introduce una contraseña para acceder a un sistema, o dejarse pospuesta para ser realizada posteriormente fuera de línea, como cuando se firma digitalmente un mensaje, en cuyo caso la firma puede ser verificada tantas veces como se desee, una vez finalizada la comunicación.

Una primitiva criptográfica que es fundamental en la autentificación, autorización y no repudio, es la firma digital. El propósito de una firma digital es proveer a una entidad un medio para enlazar su identidad a un elemento de información. El proceso de firma dentro de los esquemas de llave pública se puede ver como el proceso de cifrado con la llave privada y el proceso de verificación se puede ver como el proceso de descifrado con la llave pública. El esquema general de firma digital se muestra en la Figura 3.1. Como se observa, al mensaje se le aplica una función hash cuyo resultado será firmado con la llave privada del signatario y anexado al mensaje para ser enviados al destinatario. El destinatario separa los dos componentes: el mensaje y la firma. Le aplica la misma función hash al mensaje obteniendo el valor v1 y a la firma la verifica con la llave pública del signatario obteniendo el valor v2, si v1 = v2 se dirá que el mensaje no ha sido alterado en la transmisión y que la autenticidad del origen ha sido confirmada.

FIGURA 3.1.- Esquema de Firma Digital. Fuente: Entrust 2001

3.1.2.1.- Firmas Digitales [22]

Las firma digital es la herramienta criptográfica que ha resuelto varios aspectos de la autentificación e integridad de datos. Dentro de este campo, el algoritmo ECDSA (Elliptic Curve Digital Siganture Algorithm) es considerado como un esquema de alto rendimiento y eficiencia computacional por cuanto su principal ventaja es que requiere claves de menor tamaño para brindar la misma seguridad que DSA o RSA.

Por otro lado, el tamaño en bits de la clave pública ECDSA es aproximadamente dos veces el tamaño del nivel de seguridad, en bits. En comparación, en un nivel de seguridad de 80 bits (lo que significa que un atacante necesita el equivalente de unos 280 operaciones para encontrar la clave privada) el tamaño de una clave pública DSA es de al menos 1024 bits, mientras que el tamaño de una clave pública ECDSA sería de 160 bits. Por otro lado, el tamaño de la firma para DSA y ECDSA está dado por una relación 4 t , donde t es el nivel de seguridad en bits, es decir, alrededor de 320 bits para un nivel de seguridad de 80 bits. Estas ventajas del tamaño de la firma, ancho de banda, y la eficiencia computacional, pueden hacer a ECDSA una atractiva opción para muchas implementaciones de IKE y IKEv2 .

A diferencia de los problemas ordinarios de logaritmo discreto y problemas de factorización, no se conoce algún algoritmo de tiempo subexponencial para el problema de logaritmo discreto con curvas elípticas. Por esta razón, la fortaleza por cada bit de la llave es substancialmente mayor en un algoritmo que utiliza curvas elípticas.

Por otro lado, la Norma FIPS-186 y el estándar ANSI X9.62 [23] cubren el esquema ECDSA y describen distintas curvas que pueden ser utilizadas en los

procedimientos de firma. Aunque dichos documentos sólo poseen un ámbito de aplicación interna en los E.E.UU., al ser información de dominio público, en la práctica se utilizan fuera de este ámbito.

3.1.2.2.- Certificados Digitales [6]

Un certificado digital es un documento electrónico en donde se unen la llave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la llave pública pertenece a la entidad identificada y que la entidad posee la correspondiente llave privada. Los certificados digitales deben ser expedidos por una Autoridad Certificadora, AC, ya que si una entidad se certifica a sí misma no hay ninguna garantía de que su identidad sea la que presume, y por lo tanto, no va a ser aceptada por una tercera entidad que no la conozca.

Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si éste es válido. Para evitar la falsificación de certificados, la entidad certificadora los firma digitalmente después de autentificar la identidad de un sujeto.

Si el certificado es auténtico y se confía en la AC, entonces, también se confía en que el sujeto identificado en el certificado digital posee la llave pública que se señala en dicho certificado. Así, si un sujeto firma un documento y anexa

su certificado digital, cualquiera que conozca la llave pública de la AC podrá autenticar el documento.

Como se puede observar, los certificados digitales son una herramienta muy eficiente para lograr la autenticación entre dos o más entidades, con la premisa de que esas entidades deben de confiar en una tercera entidad, es decir, la AC. El formato de certificado digital X.509 es el más difundido y ampliamente conocido basado en ECC.

El formato de los certificados X.509 es un estándar del International Telecommunication Union Telecommunication Standarization Sector (ITU-T) y el International Standards Organization / International Electrotechnical Commission (ISO/IEC) que se publicó en 1988. Actualmente la versión que está en uso es la v3. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996. En Figura 3.2 se muestra el esquema de un certificado digital X.509.v3.

FIGURA 3.2.- Certificado Digital X.509. Fuente: B. Schneier, 1996 [24].

Los elementos principales de un certificado X.509 v3 son:

a. Versión. Contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.

b. Número de serie del certificado. Es un entero asignado por la autoridad certificadora. Cada certificado emitido por una AC debe tener un número de serie único.

c. Identificador del algoritmo de firmado. Identifica el algoritmo empleado para firmar el certificado (ECC, RSA o DSA).

d. Nombre del emisor. Identifica a la AC que ha firmado y emitido el certificado.

e. Período de validez. Indica el período de tiempo durante el cual el certificado es válido y la AC está obligada a mantener información sobre el estado del mismo. El campo incluye la fecha en la que el certificado fue expedido y la fecha de revocación.

f. Nombre del sujeto. Este campo identifica la identidad cuya llave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una AC dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.

g. Información de llave pública del sujeto. Contiene la llave pública, sus parámetros y el identificador del algoritmo con el que se emplea la llave.

h. Identificador único del emisor. Este es un campo opcional que permite reutilizar nombres de emisor.

i. Identificador único del sujeto. Este es un campo opcional que permite reutilizar nombres de sujeto.

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, llaves públicas, por mencionar algunos. Un campo de extensión tiene tres partes:

- Tipo de extensión. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.

- Valor de la extensión. Este subcampo contiene el valor actual del campo.

- Indicador de importancia. Es una bandera que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

f. Firma digital. El certificado es firmado por la AC.

El formato de los certificados X.509 se especifica en un sistema de notación llamada Abstract Sintax One (ASN-1). La Notación de Sintaxis Abstracta v1, es un lenguaje para describir los mensajes que se intercambian las aplicaciones en internet, ejemplos de aplicaciones que usan ASN.1 son: redes inteligentes, teléfonos celulares, comercio electrónico, servicios electrónicos seguros, etc.

3.1.2.3.- Análisis de Aplicación Criptográfica – Firmas y Certificados digitales.

En el ámbito práctico desafortunadamente el esquema de firma digital en canales transaccionales no está exento de ataques, por lo que es necesario que una tercera entidad avale la identidad de los participantes en una comunicación. Para ello existen los certificados digitales, en los cuales una entidad de confianza (Autoridad Certificadora) certifica la identidad de una entidad.

Considerando la existencia de ataques de autenticación (Pasivos y Activos) y a pesar de las ventajas del esquema de firma digital, desafortunadamente, existe una ataque conocido como "intruso de en medio o "man in the middle", que puede burlar el esquema de llave pública sin necesidad de romperlo, por lo cual es importante autentificar tanto la identidad de la entidad con la cual se establece el contacto y, a su vez, certificar de alguna manera que la llave pública sí pertenece a dicha entidad. También existe un ataque denominado "replay" el cual consiste en reenvíae paquetes de información cifrados, cabe señalar que el oponente no necesita conocer la llave que se utilizó para cifrar.

Para evitar los ataques mencionados anteriormente, uno de los mecanismos que protege de mejor manera la autenticación son los certificados digitales sustentados en ECC, ya que con ellos se certifica a una entidad junto con su llave pública y así evitar que un oponente se haga pasar por otro y perpetrar algún ataque.

Lo expuesto es ratificado en los estudios efectuados por la Universidad Mayor de San Andrés sobre la Seguridad en la autenticación de usuarios mediante firmas y certificados digitales [16], cuyos resultados son plasmados en la Tabla 3.2.

TABLA 3.2.- Comparación de Nivel de Seguridad entre Curvas Elípticas y RSA, en firmas digitales. Fuente: UMA [16].

Nivel de Seguridad (en Bits)	Tamaño del n orden de la Curva Elíptica E (FP), (en bits)	RSA tamaño el módulo n (en bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Del análisis a los datos presentados se tiene que para realizar una comparación, entre dos criptosistemas por un lado debemos notar que un método criptográfico basa su seguridad en el tamaño de sus llaves, para esto necesita primos relativamente grandes para que su factorización sea difícil o impráctico de calcular. Puesto que si se logra la factorización es posible romper su seguridad Además, las diferencias se expresan por cuanto RSA utiliza el problema de la factorización de un entero considerado computacionalmente infactible para tamaños del modulo mayores de 1024.

Por otro lado, en el Capítulo IV del presente Proyecto de Tesis se plantea pruebas sobre modelo criptográfico RSA y ECC en la generación de llaves y análisis del tamaño de sus llaves con el fin de validar lo expuesto.

3.2.- SEGURIDAD EN TARJETAS (SMART CARDS) [2]

Las Smart Cards son tarjetas de bolsillo con circuitos integrados, utilizadas en diversos ámbitos en organizaciones como bancos, operadoras de teléfono y corporaciones de seguros, entre otras. La gran ventaja de utilizarlas, respecto a las tarjetas magnéticas comunes, es que permiten ejecutar algoritmos criptográficos en su circuitería interna.

En este tipo de dispositivos se evidencia el mayor uso de ECC. Muchas empresas de manufactura electrónica están produciendo smart cards que hacen uso de algoritmos de firmas digitales de curvas elípticas. Compañías como Phillips, Fujitsu, MIPSTechnologies and DataKey, Funge Wireless y Entrust Technologies. Actualmente este tipo de tecnologías son usadas como tarjetas de banco (crédito, débito) y sistemas de tickets electrónicos para identificación

personal a fin de disminuir los riesgos generados por la clonación de dispositivos smart cards.

En el mercado existe una amplia gama de tarjetas JCOP (desarrolladas inicialmente por IBM, y en la actualidad por NXP) compatibles con distintas versiones de Java Card [17], que se han introducido eficazmente debido principalmente a su disponibilidad. De entre las tarjetas JCOP que implementan funcionalidades de la ECC, se tiene modelos tales como JCOP 41 y JCOP 3A que se caracterizan porque su tiempo de procesamiento superiormente inferior a las tecnologías tradicionales en función de la interfaz empleada (con contactos y sin contactos). Además de las diferencias respecto al tiempo de cifrado y descifrado, la utilización de distintas interfaces produce comportamientos marcadamente distintos en la misma tarjeta. Si se observan los tiempos de cifrado para las tarjetas JCOP 41 en ambos casos (Figura 3.3 y Figura 3.4), se puede comprobar que en la interfaz con contactos el comportamiento es prácticamente lineal, mientras que en la interfaz sin contactos el aumento del tiempo de cifrado se produce por escalones.

FIGURA 3.3.- Tiempo de Cifrado con curvas sobre F2m en JCOB 41 e interfaz sin contactos. Fuente: [17]

FIGURA 3.4.- Tiempo de Cifrado con curvas sobre F2m en JCOB 41 e interfaz con contactos. Fuente: [17]

El tiempo de descifrado en las tarjetas Java Card es sensiblemente inferior al tiempo de cifrado. Esto podría deberse a la falta de más datos sobre el funcionamiento de las tarjetas y sus coprocesadores, a que en la operación de cifrado se ejecuta un paso adicional relacionado con la aritmética de puntos de la curva y elementos finitos (la generación pseudoaleatoria del par de claves temporal) que no es necesario durante el descifrado.

3.2.1.- Análisis de Aplicación Criptográfica – Tarjetas Inteligentes.

Un ejemplo donde la criptografía de curvas elípticas ofrece beneficios claros es en la utilización de las smart cards. Son generalmente usadas para accesos seguros, transacciones financieras, identificación y todas aquellas actividades donde se requiera de seguridad. Además se tiene que la Industria de tarjetas de pago (PCI) ha definido un conjunto de requisitos de las normas de seguridad de datos "PCI DSS V2", cuyo cumplimiento se encuentra en la utilización de algoritmos asimétricos fuertes, en respuesta a esto las Tarjetas Java Card podrían ser la solución en el mercado ecuatoriano, considerando que su rendimiento y seguridad en tarjetas con coprocesador PKI, dado que el tiempo de respuesta en encriptación de 128 bit para un algoritmo clásico es de 670 ms y para un ECDSA es de 7 ms. [35]

3.3.- SEGURIDADES INALÁMBRICAS - DISPOSITIVOS MÓVILES [2]

La globalización de las comunicaciones inalámbricas ha permitido el desarrollo de nuevos estándares y productos que están produciendo cambios en la vida diaria. La movilidad se ha vuelto un requerimiento cada vez mayor dentro de los ambientes de trabajo y gracias a las redes inalámbricas se ha obtenido una movilidad real en los dispositivos móviles.

En las redes inalámbricas el canal de comunicación es peculiarmente inseguro y en aplicaciones de comercio móvil o electrónico la inseguridad es una característica no deseada, siendo imprescindible la efectividad en los mecanismos de seguridad para que el desarrollo e implementación de las redes inalámbricas sean explotados de una manera eficaz y confiable; desafortunadamente, las características inherentes de las redes inalámbricas pueden ser un punto en contra de tal seguridad.

Las redes inalámbricas, toleran un ancho de banda restringido y una latencia relativamente alta por lo que el tiempo de procesamiento, el tamaño de los mensajes a transmitir son puntos clave para desarrollar una implementación eficiente del protocolo de negociación. Dentro de este campo, para las redes inalámbricas la respuesta se plantea en el estudio e implementación del protocolo donde se lleva al cabo la autenticación, el protocolo WTLS (Wireless Transport Layer Security).

Con el propósito de establecer una sesión segura el protocolo de Negociación del WTLS admite el uso de únicamente dos criptosistemas de llave pública: RSA y Criptosistemas de Curvas Elípticas (CCE). Tradicionalmente CCE ha sido la opción criptográfica más utilizada en las implementaciones de WTLS reportadas hasta la fecha, considerando los niveles de seguridad similares a los proporcionados por RSA con tamaños de llaves hasta 10 veces menores, lo que

lo hace la mejor opción en implementaciones de este tipo. Por otro lado, dependiendo de las opciones elegidas en el protocolo de negociación se tienen tres clases de implementaciones de WTLS definidas en la especificación de WAP-261-WTLS-20010406-a Versión 6-Abril-2001 [19] , éstas son:

a. WTLS Clase 1: Sólo brinda privacidad e integridad de datos mediante un intercambio de llaves anónimo sin autenticación.

b. WTLS Clase 2: Se provee privacidad e integridad de datos además de autenticación WAP a nivel del servidor. Aquí, la autenticación del servidor se basa en certificados digitales. La llave del servidor puede ser anónima o autenticada, la llave del cliente es anónima.

c. WTLS Clase 3: Se provee privacidad e integridad de datos además de autenticación tanto del servidor como del cliente. La autenticación del servidor y del cliente se basa en certificados digitales. La llave del servidor y del cliente puede ser anónima o autenticada.

3.3.1.- Seguridades en Dispositivos Móviles

Los dispositivos móviles son aquellos equipos diseñados específicamente para realizar funciones específicas y de forma portable, como por ejemplo, teléfonos celulares, PDAs, palms, entre otros. El uso de este tipo de tecnologías va creciendo día a día convirtiéndose en herramientas fundamentales para las personas y su relación con empresas u organizaciones de diferentes tamaños. Hoy en día se puede revisar el correo electrónico y calendario personal fuera de la oficina en un pequeño teléfono inteligente o salir de viaje de negocios con un

dispositivo pocket PC inalámbrico con capacidad GPS que ayude a orientarse en ubicaciones poco conocidas.

Los PDAs son considerados los más populares para la implementación de criptosistemas de llave pública ya que poseen más capacidad de cómputo comparados con la mayoría de dispositivos móviles, como los teléfonos celulares. Es evidente que aún existen restricciones en ancho de banda, y por supuesto se convierte en un factor importante para escoger ECC como opción criptográfica. Compañías como 3COM y CertiCOM implementaron versiones de ECC para la plataforma móvil de PalmPilot y PalmOne.

El acceso a Internet vía WAP por ejemplo, es algo que pueden realizar celulares, PDA, Blackberrys y otros equipos similares. A través de WAP uno puede realizar transacciones comerciales que necesitan ser seguras, es decir, también necesitan una gran infraestructura en donde la criptografía es uno de sus principales componentes.

El riesgo de pérdida o hurto de los dispositivos móviles está siempre presente, por lo que proteger la información sensible para una organización es de vital importancia. Esta información que vendedores, distribuidores de productos, encuestadores pueden almacenar en sus aparatos móviles es posible cifrarla, utilizando por ejemplo, en el caso de las PDA, la aplicación PDA Defense.

Los aparatos mencionados por lo general, no tienen un rendimiento como el de un computador de escritorio, por lo que necesitan algoritmos que se puedan ejecutar lo más rápidamente posible.

Sea cual sea la utilización que se le otorgue a estos dispositivos, cada uno de ellos posee características en relación a la cantidad de memoria que usan o la

capacidad de procesamiento de información que aplican para su funcionamiento. Si hablamos de la implementación de procesos de cifrado para potenciar la seguridad que brindan, se puede entrar en un conflicto de valoración de un producto móvil, debido a que aplicar un proceso de cifrado implica una mayor carga de transacciones y por ende se requiere mayor poder de procesamiento por parte del equipo móvil, esto traducido a términos económicos significa dispositivos móviles con memorias y procesadores evidentemente más caros.

Para muchos dispositivos móviles que requieren de algún nivel de seguridad, la implementación de un proceso de cifrado usando RSA se hace casi impracticable, la cantidad de memoria adicional que se requiere y los tiempos de CPU que se deben dedicar al proceso son altísimos. Si se implementa un sistema como éste, el valor del dispositivo subiría considerablemente simplemente por el hecho de poseer un procesador más potente y memoria dedicada para este proceso, para no interferir con la que memoria que usa para desarrollar su propio desempeño funcional. Cabe recordar que la aplicación de un proceso de cifrado de información dentro de un dispositivo móvil es una función de soporte, la cual no debe interferir con las funciones principales de cada dispositivo, no se puede pensar que el proceso de cifrado use una mayor porción de procesamiento de datos que la función primaria de un dispositivo.

3.3.2.- Análisis de Aplicación Criptográfica – Dispositivos Móviles

Uno de los aspectos que se deben de tomar en cuenta cuando se trabaja en un medio con restricciones tales como una latencia alta y ancho de banda relativamente bajo, siendo estas características propias de la seguridad inalámbrica y dispositivos móviles, es la cantidad y tamaño de los mensajes

intercambiados, siendo el uso de protocolos de negociación WTLS (Wireless Transport Layer Security) una alternativa de implementación.

WTLS recomienda utilizar, en la etapa de negociación, dos sistemas criptográficos de llave publica: RSA y CCE. CCE ofrece el mismo nivel de seguridad que RSA pero con tamaños de llave aproximadamente diez veces menores, lo que implica un proceso de negociación más "económico". La evidencia experimental encontrada hasta el momento muestra resultados favorables para el protocolo WTLS cuando utiliza el sistema de criptografía de curvas elípticas. Es así que los resultados experimentales [25] permiten confirmar que efectivamente CCE es la opción criptográfica más eficiente para la implementación de WTLS, con tiempos de ejecución 2 y 5 veces más rápidos que los correspondientes para RSA de 1024 y 2048 bits. Esta diferencia de complejidad de ejecución entre criptosistemas de curvas elípticas y RSA tiene repercusiones en el desempeño del protocolo de seguridad lo que a su vez implica un detrimento en la calidad final de los servicios ofrecidos al usuario.

3.4.- SEGURIDAD EN REDES VIRTUALES PRIVADAS (VPN) [6]

Las VPN (Virtual Private Network) es una red privada que se extiende, mediante un proceso de encapsulamiento de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. En otras palabras, las VPN's son sistemas que permiten a un computador en una red pública, conectarse a una red local.

Existe tres conceptos que hacen que una conexión VPN sea segura:

- Tunneling: El servicio VPN crea un túnel seguro a través de las redes no fiables que haya entre el punto de destino y origen. Los usuarios de Internet no podrán ver o reconocer este túnel. El servicio VPN crea un mecanismo de seguridad con la ayuda de tecnologías de red especiales que se llaman protocolos criptográficos de tunneling. Estos protocolos establecen y mantienen una conexión VPN, cifran la información que se envía por el túnel y mantienen la integridad del mensaje.

- Cifrado del tráfico: Toda la información enviada por el túnel está cifrada. Mediante una aplicación de seguridad complementaria se cifra, no sólo los datos, sino también las direcciones de red de origen y destino. No se podrá usar la información privada sin autorización. Hoy en día el método ECC proporciona un cifrado efectivo, tan seguro que se necesitarían miles de ordenadores y años para descifrarse.

- Mecanismo de autentificación: Una conexión VPN fiable tiene un mecanismo de autentificación muy avanzado. Significa que el punto final del túnel debe ser autentificado antes de poder establecer túneles VPN seguros. Para la autentificación puede usarse lo siguiente: contraseñas, certificados digitales, biométricos, autentificación de dos factores y otros métodos criptográficos.

Para entenderlo mejor, veamos cómo funciona:

Por ejemplo, se tiene que una entidad financiera necesita intercambiar e-mails con regularidad, información absolutamente confidencial, con sus

asociados en el extranjero; considerando, que los archivos son bastante grandes, y que se necesita enviarlos por Internet. En este caso, la conexión VPN es la solución más segura, conveniente y barata. Usando Internet como base, el servicio VPN establece un túnel entre los asociados y la entidad, y la información cifrada, está protegida de otros usuarios de Internet.

Las VPN´s son implementadas bajo condiciones y diferentes tipos de tecnología. Sin embargo, éstas alcanzan su evolución en el empleo del protocolo de cifrado denominado «Esquema de Cifrado Integrado con Curvas Elípticas» (Elliptic Curve Integrated Encryption Scheme, ECIES), para el intercambio de información cifrada ([19], [20], [21]).

Finalmente, en Conferencia RSA 2005, la Agencia de Seguridad Nacional de Estados unidos anunció el uso de VPN únicamente bajo un modelo ECC, así como para la generación de la firma digital y el intercambio de claves. Considerando su efectividad y alta seguridad. Además, se debe considerar que el diseño propuesto permite proteger tanto a los sistemas de seguridad norteamericanos clasificados y no clasificados y el tratamiento de la información en general.

3.4.1.- Análisis de Aplicación Criptográfica - VPN

Uno de los aspectos que se deben de tomar dentro de la implementación de VPN´s es el ancho de banda consumido por los sistemas ECC, el cual es menor que los sistemas tradicionales. Los bits de payload reservados en las cabeceras IP son de 326 para RSA mientras que para ECC son de 41. Además, según los estudios especializados de NITS se tiene que son 3.5 veces más

seguros utilizando algoritmos ECC que algoritmos como RSA, El Gamal, DSA, entre otros. El tiempo de respuesta entre cliente y servidor es mucho menor tal y como se muestra en el Figura 3.5.

FIGURA 3.5.- Rendimiento VPN – RSA vs ECC. Fuente: [26]

3.5.- LÍNEAS FUTURAS ECC [32]

Los Estados Unidos, el Reino Unido, Canadá y algunos otros países de la OTAN han adoptado alguna forma de criptografía de curva elíptica para proteger información sensible. La Iniciativa de Modernización de cifrado en el Departamento de Defensa de EE.UU. pretende sustituir casi 1,3 millones de equipos existentes en los próximos 10 años. Además, la Red de Información Global del Departamento requerirá una vasta expansión del número de dispositivos de seguridad en uso en todo el Ejército de los EE.UU.; para ello será necesario el cambio y la renovación de los equipos con los principales aliados de Estados Unidos. La mayoría de estas necesidades se satisfacen con una nueva generación de equipos de cifrado que utiliza la criptografía de curva elíptica para la gestión de claves y firmas digitales.

De lo expuesto en párrafos anteriores se han estudiado diversos tipos de investigaciones realizadas por organizaciones de prestigio y cuyas metodologías de trabajo son consideradas de alto nivel, de acuerdo a esto se han sacado conclusiones respecto al futuro de los algoritmos de cifrado RSA y de Curva Elíptica.

Una gran interrogante que existe es: ¿Los métodos basados en curvas elípticas reemplazarán o coexistirán con RSA?. Si bien, existen muchos estudios y estándares que respaldan el uso de algoritmos basados en curvas elípticas, no podemos obviar la influencia que tiene RSA en el mercado de la seguridad de la información. Si se compara el poder de RSA respecto a su competidor Certicom en cuanto a su influencia en el mercado, se podría decir que es similar a la competencia que tiene Microsoft y Linux. Como se sabe, las distribuciones Linux tienen muchas ventajas sobre el sistema operativo Windows de Microsoft, sin embargo, existe una amplia diferencia en cuanto al uso de estos sistemas operativos en el mundo, y podemos atribuir esa diferencia a la solidez y prestigio que ha generado Microsoft en los años que lleva en el mercado.

Como se ha visto, la criptografía de curva elíptica lleva varios años dando vuelta en la mente de investigadores y desarrolladores, pero gran parte de la diferencia respecto a RSA, es que no se ha promovido de manera masiva la idea de cambiar a una mejor tecnología, esto se debe esencialmente a la traba de pensar que cambiar de tecnología es sinónimo de costos muy elevados para las organizaciones. Otra traba existente es, que al no usarse regularmente en productos, existen pocos intentos de ataque que busquen romper la seguridad de los algoritmos basados en curva elíptica, por lo que es difícil confiar en algo que no ha pasado la prueba de la sociedad por decirlo así, ya que los hackers suelen atacar sistemas con el fin de obtener algún provecho, pero al no ocuparse ECC en sistemas de organizaciones, los intentos para investigar sobre ataques a ECC son escasos.

Volviendo a la interrogante, va a ser un proceso similar al vivido por Windows y Linux pero con algunas diferencias. Todos los estudios revelan que en algunos años más, los sistemas de las organizaciones estarán sobrecargados

al usar RSA. Se cree que a finales del 2014 algunas empresas innovadoras en el ámbito de la tecnología, empezarán a estudiar la factibilidad de migrar de tecnología, por lo que habrá coexistencia de los algoritmos durante varios años, hasta que se consolide el uso de algoritmos basados en curva elíptica.

Otra interrogante de gran importancia es la siguiente: ¿Cuándo es conveniente migrar de tecnología? Se han analizado algunos aspectos económicos sobre las ventajas que posee la utilización de ECC sobre RSA, sin embargo, pueden existir casos en que la inversión no genere las expectativas de las entidades financieras, o bien, que no convenga en ese momento.

Las entidades necesitan que sus decisiones estén respaldadas por estudios de alto nivel, por lo que atreverse a cambiar de tecnología tempranamente es difícil, aún cuando se han logrando excelentes resultados empleando ECC.

Se piensa que esta tecnología podría ser aprovechada por las PYMES, ya que el riesgo que estas empresas corren es menor que el riesgo que corren las grandes empresas y a su vez pueden ofrecer un servicio de comercio electrónico con un nivel de seguridad más alto.

Otro aspecto importante al decidir la migración es hacer una evaluación de proyecto al momento de adquirir una máquina que utilice tecnología de cifrado, ya que dependiendo de la cantidad de años que se utilice en el proyecto sería necesario migrar de una tecnología a otra. Por ejemplo, si se compra un servidor que utiliza cifrado RSA, hay que tener en consideración que a medida que pasen los años, el nivel de seguridad tendrá necesariamente que aumentar, lo que significaría mayor carga para el servidor. Si el servidor que se adquiere,

se ocupará durante gran cantidad de años, la necesidad de migrar de tecnología se hará evidente.

Otro aspecto a considerar para decidir de migrar de tecnología es la clasificación que le damos a la información, es decir, pública, secreta, top-secret, etc. Esto se debe a que, dependiendo de la clasificación de la información, es el nivel de seguridad mínimo que deben tener los sistemas que manejan esa información. Por lo general todo esto está ligado a seguridad de tipo gubernamental o militar, pero es considerado por grandes empresas también. Comúnmente se utiliza el nivel de seguridad mínimo para los sistemas, para no disminuir la eficiencia de los procesos, pero cuando hablamos de información militar, se necesitan muchos niveles de seguridad, por lo que al utilizar el algoritmo RSA para proteger información clasificada como top-secret significa una sobrecarga al sistema que reduce la eficiencia de todos los procesos en un porcentaje elevado.

Las Instituciones que quieren seguir ocupando RSA se preguntarán: ¿Existe alguna manera para que no disminuya tanto la capacidad de procesamiento? . Constantemente se ha estado trabajando en dispositivos que aceleren algunas operaciones básicas de cifrado, mediante la implementación de algunos algoritmos específicos, pero la diferencia no es tan significativa. Otra manera es balancear la carga de cifrado y descifrado, es decir, usar claves públicas más grandes, lo que significaría claves privadas mas pequeñas. El problema de esto es que estarían transfiriendo la carga de procesamiento a los usuarios del sistema, que en muchas ocasiones poseen computadores de bajo nivel de procesamiento. Si bien, el sistema en sí tendría menos carga de trabajo, las transacciones al final serían más lentas, debido a lo que se demoraría el computador del usuario en cifrar la información, por lo que la calidad de servicio

disminuiría notablemente, y esto puede que cause pérdidas mayores al gasto de máquinas que soporten más procesamiento o bien al proceso de migración de tecnología.

Lo cierto es que la nueva tendencia es la utilización de dispositivos cada vez más pequeños para realizar tareas que faciliten la vida laboral y cotidiana. Esto quiere decir que el acceso a Internet está aumentando de manera exponencial, por lo que garantizar un servicio de calidad y seguro se convirtió en una necesidad clara, y las empresas fabricantes de los dispositivos móviles se encuentra hoy en día constantemente estudiando cómo mejorar el servicio debido a la gran competencia que existe. Nos referimos a empresas como IBM, Sun Microsystems, Microsoft, Hewlett-Packard o Motorola, entre otras.

El cambio de sistema criptográfico es inminente, y si bien tomará algunos años en incorporarse de lleno en el mercado, Ecuador tendrá que esperar a que las sedes primarias de las instituciones en países extranjeros adopten el uso de la criptografía de curva elíptica, y luego exijan su uso en las sedes secundarias en el resto del mundo.

CAPÍTULO IV

ESTUDIO Y EVALUACIÓN

Este capítulo plantea el análisis de dos métodos criptográficos asimétricos, la criptografía RSA y la criptografía de curvas elípticas. Tanto RSA como curvas elípticas se encuentran respaldados por muchos estudios de alto nivel que acreditan ser métodos criptográficos eficientes; poseen además normativas que regulan su utilización en aplicaciones tanto a nivel gubernamental como comercial, como por las normativas aplicadas por los estándares fijados por la IEEE, NIST, ANSI, entre otros. Además se ha efectuado pruebas sobre la eficiencia de los métodos de cifrado RSA y ECC, considerando tres factores: sobrecarga en cálculos, tamaño de clave y ancho de banda.

4.1.- ESTUDIOS ACTUALES

Debido a la problemática actual comentada anteriormente, es necesario buscar algoritmos que permitan proteger eficientemente información anticipando los avances tecnológicos. Existen un sin número de productos y servicios que de una u otra forma dependen de la tecnología.

Tanto organismos gubernamentales como organismos comerciales están preocupados por la rapidez con la que crece la tecnología en contraste a la seguridad actual de los sistemas de información. Entre éstos se pueden mencionar a NIST, Certicom, Sun Microsystems, IEEE, entre otros.

4.1.1.- NIST (National Institute of Standards and Technology) [6]

NIST constituye uno de los organismos que trabaja constantemente buscando estándares que permiten resguardar activos de información. Es un organismo federal que forma parte del departamento de comercio de EEUU, cuyo fin es elaborar y promover patrones de medición, normas y tecnologías para aumentar la productividad, facilitar el comercio y mejorar la calidad de vida. Las áreas que dependen netamente del NIST en EEUU son biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada.

Como los algoritmos asimétricos son utilizados generalmente para el intercambio de claves entre dos entes, para luego cifrar la información mediante un algoritmo simétrico, NIST ha realizado estudios sobre el tamaño de las claves que deben usar algunos algoritmos asimétricos en contraste a los tamaños de claves del algoritmo simétrico AES (Advanced Encryption Standard).

Como se puede observar en la tabla 4.1, para proteger la información utilizando una clave de 128 bits para el algoritmo AES , se emplea un algoritmo basado en curvas elípticas con clave de 256 bits, o bien se utiliza el algoritmo RSA con clave de 3072 bits.

A medida que se requiere mayor seguridad, el ratio entre el tamaño de clave de un algoritmo basado en curvas elípticas y el algoritmo RSA se va haciendo más evidente.

TABLA 4.1.- Tamaños para claves públicas para usar con AES – Fuente: NIST to ANSI X944. [27]

ECC KEY SIZE (Bits) RSA KEY SIZE (Bits) KEY SIZE RATIO AES KEY SIZE (Bits)

163 1024 1:6 -

256 3072 1:12 128

384 7680 1:20 192

512 15380 1:30 256

NIST GUIDELINES FOR PUBLIC KEY SIZES FOR AES

NIST define o estandariza los tamaños de claves, las que están descritas en el documento FIPS186-3 [26]. La Tabla 4.2 presenta la diferencia de los tamaños de claves para el algoritmo RSA para diversos usos en contraste a algún algoritmo basado en curvas elípticas.

TABLA 4.2.- Tamaño de claves y algoritmos para cada tipo de uso. Fuente: NIST FIPS186-3 . [26]

PIV KEY TYPE PERÍODO PARA USO ALGORITMOS Y TAMAÑOS DE CLAVES

PIV authentication key 31/12/2010 RSA (1024, 2048 ó 3072 bits)

ECDSA(Curvas recomendadas de 224-283 bits)

Después del 31/12/2010 RSA (2048 o 3072 bits)

ECDSA(Curvas recomendadas de 224-283 bits)

Card authentication key 31/12/2010 2TDEA

3TDEA

AES-128, AES-192, AES-256

RSA(1024, 2048 ó 3072 bits)

ECDSA(Curvas recomendadas de 224-283 bits)

Después del 31/12/2010 3TDEA

AES-128, AES-192, AES-256

RSA(2048 ó 3072 bits)

ECDSA(Curvas recomendadas de 224-283 bits)

Digital signature key 31/12/2008 RSA(1024, 2048 ó 3072 bits)

ECDSA(Curvas recomendadas de 244-283 bits)

Después del 31/12/2008 RSA(2048 ó 3072 bits)

ECDSA(Curvas recomendadas de 224-283 bits)

Key management key 31/12/2008 RSA key transport (1024, 2048 ó 3072 bits)

ECDH ó ECC MQV (curvas recomendadas 224-283 bits)

Después del 31/12/2008 RSA key transport (2048 ó 3072 bits)

ECDH ó ECC MQV (curvas recomendadas 224-283 bits)

Por lo expuesto y considerando este esquema, NIST recomienda usar algunas curvas específicas para el gobierno federal, las que están descritas en el mencionado documento. Las curvas estandarizadas por dicho organismo son las siguientes: [26]

CAMPO BINARIO DE GRADO 163

p(t) = t163 + t7 + t6 + t3 + 1

n = 5846006549323611672814742442876390689256843201587

a = 1

b = 2 0a601907 b8c953ca 1481eb10 512f7874 4a3205fd

Px = 3 f0eba162 86a2d57e a0991168 d4994637 e8343e36

Py = 0 d51fbc6c 71a0094f a2cdd545 b11c5c0c 797324f1

CAMPO BINARIO DE GRADO 263

p(t) = t233 + t74 + 1

n = 690174634679056378743475586227702555583981273734501355\

5379383634485463

a = 1

b = 066 647ede6c 332c7f8c 0923bb58 213b333b 20e9ce42 81fe115f 7d8f90ad

Px = 0fa c9dfcbac 8313bb21 39f1bb75 5fef65bc 391f8b36 f8f8eb73 71fd558b

Py = 100 6a08a419 03350678 e58528be bf8a0bef f867a7ca 36716f7e 01f81052

CAMPO BINARIO DE GRADO 283

p(t) = t283 + t12 + t7 + t5 + 1

n = 7770675568902916283677847627294075626569625924376904889

109196526770044277787378692871

a = 1

b = 27b680a c8b8596d a5a4af8a 19a0303f ca97fd76 45309fa2

a581485a f6263e31 3b79a2f5

Px = 5f93925 8db7dd90 e1934f8c 70b0dfec 2eed25b8 557eac9c

80e2e198 f8cdbecd 86b12053

Py = 3676854 fe24141c b98fe6d4 b20d02b4 516ff702 350eddb0

826779c8 13f0df45 be8112f4

CAMPO BINARIO DE GRADO 409

p(t) = t409 + t87 + 1

n = 66105596879024859895191530803277103982840468296428121928464879830415777482737480520814372376217911096597986728836656752677

a = 1

b = 021a5c2 c8ee9feb 5c4b9a75 3b7b476b 7fd6422e f1f3dd67

4761fa99 d6ac27c8 a9a197b2 72822f6c d57a55aa 4f50ae31

7b13545f

Px = 15d4860 d088ddb3 496b0c60 64756260 441cde4a f1771d4d

b01ffe5b 34e59703 dc255a86 8a118051 5603aeab 60794e54

bb7996a7

Py = 061b1cf ab6be5f3 2bbfa783 24ed106a 7636b9c5 a7bd198d

0158aa4f 5488d08f 38514f1f df4b4f40 d2181b36 81c364ba

0273c706

CAMPO BINARIO DE GRADO 571

p(t) = t571 + t10 + t5 + t2 + 1

n = 3864537523017258344695351890931987344298927329706434998

6572352514515191422895604245361439993894157730831338811 2

1926944486246872462816813070234528288303332411393191105 2

85703

a = 1

b = 2f40e7e 2221f295 de297117 b7f3d62f 5c6a97ff cb8ceff1

cd6ba8ce 4a9a18ad 84ffabbd 8efa5933 2be7ad67 56a66e29

4afd185a 78ff12aa 520e4de7 39baca0c 7ffeff7f 2955727

Px = 303001d 34b85629 6c16c0d4 0d3cd775 0a93d1d2 955fa80a

a5f40fc8 db7b2abd bde53950 f4c0d293 cdd711a3 5b67fb14

99ae6003 8614f139 4abfa3b4 c850d927 e1e7769c 8eec2d19

Py = 37bf273 42da639b 6dccfffe b73d69d7 8c6c27a6 009cbbca

1980f853 3921e8a6 84423e43 bab08a57 6291af8f 461bb2a8

b3531d2f 0485c19b 16e2f151 6e23dd3c 1a4827af 1b8ac15b

Podemos notar que en todas estas curvas, el coeficiente de a es 1, lo que NIST describe como una ecuación seudo aleatoria de una curva elíptica, en donde el cofactor es 2, es decir, el número de puntos pertenecientes a este cuerpo es, 2n.

Existen curvas que usan otros coeficientes para el parámetro a y b, las cuales son llamados curvas de Koblitz, pero mantienen el tamaño de la clave sugeridas por el NIST.

Éstas son las curvas recomendadas para trabajar en cuerpos binarios, sin embargo existen otras curvas recomendadas para trabajar en cuerpos con números primos que son equivalentes a un nivel de seguridad a las recomendadas por el NIST, las cuales tienen tamaño de clave de 192, 224, 256, 384 y 521 bits.

Para representar las curvas como objetos, NIST creó la siguiente tabla:

TABLA 4.3.- Identificador ANSI para las curvas aprobadas por NIST. Fuente: NIST FIPS186-3. [26]

Se puede ver que el nombre de representación de los objetos, provienen del "American National Standards Institute" (ANSI), organismo sin fines de lucro que supervisa el desarrollo de estándares para producto, servicios y sistemas en EEUU.

En relación a las Previsiones del NIST en su documento titulado "SP800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification", el NIST considera que, en el año 2011, los cifrados con seguridades equi¬valentes a 80 bits de cifrado simétrico están fuera de uso, al menos para la identi¬ficación personal, y los sistemas deberán haber migrado a una seguridad equivalente a 112 bits o hacia cotas más elevadas. Para los sistemas asimétricos basados en criptografía de curvas elípticas se especifica un mínimo de 112 bits, lo que supone utilizar claves de 224 bits de longitud.

Así pues, dado que el cre¬cimiento de la clave en ECC es menor y que las capacidades computacionales en la facto¬rización de números enteros semiprimos, como lo son los del RSA, va creciendo a buen ritmo, quizás sea el momento de pensar en abandonar la criptografía de clave pública de primera generación, y pasar a usar curvas elípticas.

El que esto no se haya hecho antes quizás se deba a que la Criptografía de Curvas Elípticas está fuertemente "patentada" y sus propietarios no parecen estar por entregarla al libre uso y del público.

4.1.2.- IEEE (Institute of Electrical and Electronics Engineers) [6]

IEEE es una organización mundial, sin fines de lucro, que se dedica al desarrollo de estándares. Se creó en el año 1884, por grandes personalidades como Thomas Alva Edison, Alexander Gram. Bell y Franklin Leonard Pope. Cuando se fusionaron el AIEE (American Institute of Electrical Engineers) y el IRE (Institute of Radio Engineers) en el año 1963, se cambió el nombre por el actual. Sus estándares representan prestigio y calidad en las áreas derivadas de la eléctrica, tales como la ingeniería computacional, tecnologías biomédicas, telecomunicaciones, etc.

La criptografía es una rama considerada fundamental en los procesos de las organizaciones, es por esto que la IEEE se preocupa por el desarrollo de estándares en esta materia. Una de los estándares más estudiados por las grandes organizaciones, precisamente es el llamado "Standard Specifications For Public-Key Cryptography" creado por IEEE en su proyecto P1363.

Los jefes del proyecto han ido cambiado desde su inicio en 1994. Primero estuvo Buró Kaliski perteneciente a RSA Security, luego Ari Singer de NTRU, y actualmente es William Whyte, de NTRU Cryptosystems Inc.

El alcance del proyecto abarca los siguientes temas:

- Criptografía asimétrica tradicional.

- Criptografía asimétrica basada en problemas fuertes en Lattices.

- Criptografía asimétrica basada en passwords.

- Criptografía asimétrica basada en identidad usando pares.

a. Criptografía asimétrica tradicional [22].- La criptografía asimétrica (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. Esta especificación trabaja con 3 tipos de esquemas:

□ Esquemas de Intercambio de claves: Se especifican los algoritmos para el intercambio de claves de los sistemas. Éstos son:

DL/ECKAS-DH1 - DL/ECKAS-DH2: Algoritmos basados en el problema de logaritmo discreto, o bien logaritmo discreto de curvas elípticas, es decir los algoritmos de Diffie-Hellman y su similar para curvas elípticas.

DL/ECKAS-MQV: También basado en el problema de logaritmo discreto y logaritmo discreto de curvas elípticas, utilizando el algoritmo de Menezes-Qu-Vanstone. [28]

☐ Esquema de Firmas: Especifica los algoritmos para utilizar en firmas digitales. Éstos son:

- DL/ECSSA: Utiliza los algoritmos DSA, ECDSA, Nyberg-Rueppel y Nyberg-Rueppel para curvas elípticas.

- IFSSA: Basado en factorización de enteros. Utiliza variantes de RSA como Rabin Williams y ESIGN con varios métodos de codificación de mensajes (RSA1 con EMSA3).

- DL/ECSSR: Similar a DL/ECSSA pero con recuperación.

- DL/ECSSR-PV: Similar a DL/ECSSR ocupando la versión de Pintsov-Vanstone.

- IFSSR: Esquema de firma de factorización de enteros con recuperación.

☐ Esquema de Cifrado: Especifica varios esquemas de cifrado, siendo éstos:

- IFES: Basados en factorización de enteros. Principalmente cifrado RSA con relleno óptimo de cifrado asimétrico (OAEP).

- DL/ECIES: Basado en el problema de logaritmo discreto de curva elíptica. Elliptic Curve Integrated Encryption Écheme (ECIES). Variante de ElGamal.

- IFES/EPOC: Similar a IFES, ocupando la versión EPOC.

b. Criptografía asimétrica basada en problemas fuertes en Lattices .- Especifica técnicas criptográficas basadas en problemas fuertes en Lattices , cuyo propósito es incluir primitivas matemáticas para derivación de claves secretas, cifrado asimétrico, identificación, firmas digitales y esquemas criptográficos basados en lattices. Ejemplo de ello es el Criptosistema de Clave pública NTRUEncrypt que constituye un sistema de cifrado relativamente nuevo. La primera versión del sistema, que se llama simplemente NTRU, se desarrolló alrededor de 1996 por tres matemáticos (J. Hoffstein, J.Pipher y JH Silverman). En 1996 estos matemáticos junto con D. Lieman fundaron la NTRU Criptosistemas, Inc. y se les facilitó una patente sobre el sistema de cifrado. [29]

Durante los últimos diez años se ha estado trabajando en la mejora del sistema de cifrado. Desde la primera presentación del criptosistema, se realizaron algunos cambios para mejorar tanto el rendimiento del sistema y su seguridad. La mayoría de las mejoras en el rendimiento se centraron en la aceleración del proceso, en lugar de arreglar el problema de descifrado incorrecto, resultado de lo cual se puede encontrar literatura que describe los fracasos sobre el descifrado de NTRUEncrypt. En cuanto a la seguridad se han introducido nuevos parámetros frente a ataques conocidos y al aumento razonable de la potencia de cálculo. Ahora el sistema está plenamente aceptado en los estándares IEEE P1363. Debido a la velocidad del criptosistema de clave pública NTRUEncrypt y su uso bajo de memoria que puede ser utilizado en aplicaciones tales como dispositivos móviles y tarjetas inteligentes. En abril de 2011, NTRUEncrypt fue aceptado como estándar X9.98, para su uso en la industria de servicios financieros.

c. Criptografía asimétrica basada en contraseñas [30].- El objetivo de este documento es incluir esquemas para intercambio de claves con autenticación vía password. Ésto incluye:

- BPKAS-PAK: Corresponde a un esquema balanceado, versión PAK.

- BPKAS-PPK: Similar a la anterior pero utiliza versión PPK.

- BPKAS-SPEKE: Similar a los anteriores, utilizando intercambio de claves simple exponencial.

- APKAS-AMP: Corresponde a un esquema para el intercambio de claves, versión AMP.

- APKAS-BSPEKE2: Similar al anterior pero versión BSPEKE2.

- APKAS-PAKZ: Similar al anterior pero versión PAKZ.

- APKAS-SRP3 - APKAS-SRP6: Similar al anterior pero utiliza password seguro remoto.

- APKAS-WSPEKE: Similar al anterior pero versión WSPEKE.

- PKRS-11: Corresponde a un esquema de recuperación de la llave de autenticación para el password.

En criptografía, un método de acuerdo de claves con contraseña autenticado, es un método interactivo para dos o más partes para establecer las claves de cifrado basadas en el conocimiento de una o varias partes de una contraseña. Una propiedad importante es que un hacker no podría obtener

suficiente información para ser capaz a través de mecanismos de fuerza bruta adivinar una contraseña por la singularidad de su contraseña, lo que permite mitigar razonablemente los riesgos generados.

d. Criptografía asimétrica basada en identidad usando pares [31].- Este marco de referencia específica esquemas basados en mapas bilineares sobre curvas elípticas, es decir, puntos de curva elíptica. Define algoritmos para el cómputo de los puntos, parámetros adecuados de curva, etc.

4.2.- ESTÁNDARES COMERCIALES (ISO, IEEE, ANSI X9F, IETF)

Las políticas de certificación y prácticas establecen un marco de estandarización de las actividades que permite la operación efectiva desde el punto de vista técnico. A continuación se mencionan algunos documentos de referencia que están siendo utilizados como estándares de la industria de certificación digital y PKI. En la tabla 4.4 podemos ver varios de éstos:

TABLA 4.4.- Algunos estándares de ECC – Fuente: [2]

GRUPO	ESTÁNDAR
IEEE	P1363-2000 · P1363a · P1363.2
CEN	TC331 WG3 (DPM)
NESSIE	ECDSA · PSEC

SECG SEC1 · SEC2

ANSI X9F X9.24 Key management · X9.37 Check Image Exchange · X9.57 Cert management · X9.59 Payment · X9.62 ECDSA · X9.63 Key establishment · X9.68 Compressed certificates · X9.73 CMS · X9.84 Biometrics · X9.90 IRD · X9.92 ECPVS · X9.95 Time stamps · X9.96 XML CMS

FIPS FIPS 186-2 Signatures (ECDSA) · SP 800-56 Key establishment · SP 800-57 Key management

FAA Security Next Generation ATN · Secure ACARS

ISO 14888 · 15946 · 9796 · 18033 …

IETF PKIX · SMIME · IPSec (IKE) · TLS

CE 1394 Consumer Electronics DTCP

OMA WTLS · WPKI · WMLScript …

4.3.- ANÁLISIS COSTO – BENEFICIO CRIPTOSISTEMA DE CURVAS ELÍPTICAS

Si hablamos de la implementación de procesos de cifrado para potenciar la seguridad que brindan, se puede entrar en un conflicto de valoración, debido a que aplicar un proceso de cifrado implica una mayor carga de transacciones y por ende se requiere mayor poder de procesamiento por parte de los equipos, esto traducido a términos económicos significa dispositivos con memorias y procesadores evidentemente más caros.

Para muchos dispositivos que requieren de algún nivel de seguridad, la implementación de un proceso de cifrado usando RSA se hace casi impracticable, la cantidad de memoria adicional que se requiere y los tiempos de CPU que se deben dedicar al proceso son altos. Si se implementa un sistema como éste, el valor del dispositivo subiría considerablemente simplemente por el hecho de poseer un procesador más potente y memoria dedicada para este proceso para no interferir con la que memoria que usa para desarrollar su propio desempeño funcional. Cabe recordar que la aplicación de un proceso de cifrado de información dentro de un dispositivo móvil por ejemplo es una función de soporte, la cual no debe interferir con las funciones principales de cada dispositivo, no se puede pensar que el proceso de cifrado use una mayor porción de procesamiento de datos que la función primaria de un dispositivo. Usando curvas elípticas significa que un dispositivo embebido puede:

- Usar un procesador más barato y pequeño o aplicar mayor procesamiento a las funciones primarias del dispositivo; en casos donde las operaciones de seguridad son integradas a un chipset, usando curvas elípticas se reducirán los costos.

- Aplicar menos ciclos de procesador porque el dispositivo está generando menos calor, por ende menos consumo energético, dando como resultado alargar la vida útil de sus baterías.

- Requerir menos ancho de banda para sus transacciones debido a que los protocolos son más eficientes.

A continuación se examinan los factores asociados a los costos que los desarrolladores, fabricantes y vendedores deberían considerar cuando implementan seguridad embebido en sus diseños.

a.- Poder de Procesamiento

En la determinación de las operaciones potenciales de cualquier dispositivo, la selección de chips es una de las consideraciones más importantes: un procesador más caro permite a un dispositivo hacer más, además al usar métodos eficientes se le permite a un procesador más barato realizar las mismas funciones que uno más caro. Es aquí donde las características de la criptografía de curvas elípticas se presentan como un método de eficiente que permite el ahorro de dinero ante el uso de RSA.

Por ejemplo, una tarjeta inteligente para una transacción financiera se debe autenticar a través de un lector, al emplear curvas elípticas requerirá menos procesamiento, lo que permite procesar mayor cantidad de transacciones y generar mayores ingresos. Otros dispositivos móviles como PDAs o smartphones muestran resultados similares. Un procesador típico para esta clase de dispositivos es el ARM SA1110, 206MHZ que posee un similar nivel de

seguridad de 128 bits de AES. Por otro lado, ECC-256 provee de excelentes tiempos de respuesta, mientras RSA-3072 ofrece una buena respuesta solamente en verificaciones de firmas; mientras que los tiempos para generar claves y firmas son considerados ineficientes.

Como conclusión se puede afirmar que para obtener un buen resultado usando RSA se requiere del uso de un procesador más caro que el usado por curvas elípticas para obtener resultados similares.

b.- Número de Compuertas Lógicas [6]

La criptografía de curvas elípticas ofrece mejoras en software, sin embargo, también puede ser muy eficiente en hardware. Los beneficios de curvas elípticas pueden incrementar dramáticamente su eficiencia en comparación a RSA en ambientes basados en hardware. Los diseños optimizados basados en chips han demostrado que pueden ser hasta treinta y siete veces más rápidos que el mismo diseño implementado en software.

Esta ventaja se ve reflejada en la cantidad de compuertas lógicas usadas en un diseño electrónico (lo que indica el espacio usado en un chip) y en performance en relación a RSA. Como todo diseñador electrónico sabe, más compuertas lógicas dentro del diseño electrónico significan más dinero.

Como se puede apreciar en la tabla 4.5, la criptografía de curvas elípticas sobresale en el espacio utilizado y en velocidad dentro de un diseño electrónico. Siguiendo las tendencias tecnológicas, cuando se optimiza por espacio se tiene que es diez veces menor (3260 compuertas lógicas vs 34000) y aún así presenta

mejores tiempos de respuesta que su competencia RSA. Cuando se optimiza por velocidad, la criptografía de curvas elípticas es siete veces más rápida usando los mismos tamaños de claves y más de ochenta veces más rápido cuando se usan claves que se requerirán a futuro para garantizar la seguridad. [32]

TABLA 4.5.- Tiempo de procesamiento y cantidad de compuertas lógicas usadas en hardware para la implementación de los algoritmos RSA y Curvas Elípticas – Fuente: Certicom [3].

ALGORITMO OPTIMIZACIÓN TIEMPO CANT. DE COMPUERTAS LÓGICAS

RSA – 1024

ECC – 163 Optimización de espacio 4.90 ms

0.66 ms 34.000

3.260

RSA – 1024

ECC – 163 Optimización de velocidad 2.60 ms

0.35 ms 150.000

48.400

RSA – 3072

ECC – 283 Optimización de espacio 184 ms

29 ms 50.000

6.660

RSA – 3072

ECC – 283 Optimización de velocidad 110 ms

1.3 ms189.200

80.100

Por estas razones, la criptografía de curvas elípticas es una opción efectiva al momento de implementar este tipo de seguridad en hardware. Cualquier dispositivo que use RSA requerirá de mayor poder de procesamiento para un microprocesador estándar.

Como consecuencia de una implementación eficiente de seguridad en hardware según lo planteado en el uso de compuertas lógicas, se requiere de menos ciclos de procesamiento y menos trabajo por parte de los microprocesadores, lo que finalmente se traduce en el uso de menos energía y en una disipación de calor menor. Esto es un punto crítico dentro de los dispositivos móviles, donde el factor limitante para el uso en muchos casos es la duración de la batería.

Como el uso de ECC reduce los factores mencionados, se dice que ECC es parte de la solución para aumentar la vida de los dispositivos móviles.

c.- Eficiencia Computacional

La seguridad no es la única característica atractiva de la criptografía de curva elíptica. Los criptosistemas de curvas elípticas también son más eficientes computacionalmente que los sistemas de primera generación de clave pública, RSA y Diffie-Hellman. En la tabla 4.6 se muestra la relación de RSA frente a cálculo computacional de ECC, para cada uno de los tamaños de clave estandarizados por NIST.

TABLA 4.6.- Costos Relativos de Cómputo de RSA y las curvas elípticas. Fuente: Certicom [3].

NIVEL DE SEGURIDAD (BITS)	RELACIÓN DE COSTO RSA VS COSTO ECC
80	03:01
112	06:01

128

10:01

192

32:1

256

64:1

Estrechamente relacionado con el tamaño de la clave de los diferentes sistemas de clave pública está la sobrecarga de los canales necesarios para realizar intercambios de claves y firmas digitales en un enlace de comunicaciones. Los tamaños para la clave pública de la Tabla 4.6 es aproximadamente igual a la cantidad de bits que necesitan ser transmitidos en un canal de comunicación para un intercambio de claves. En limitaciones de canal, las curvas elípticas ofrecen una solución mucho mejor que la primera generación de sistemas de clave pública como RSA y Diffie-Hellman, considerando su rendimiento.

d.- Requerimientos de Ancho de Banda

La criptografía de curva elíptica usa menos ancho de banda que los algoritmos comúnmente usados para protocolos de SSL/TLS, significando que

puede se puede transferir más datos en el mismo tiempo. Lo citado será verificado a través de la realización de pruebas técnicas- operativas en el presente capitulo.

e.- Reducción de Gastos

Existen costos que se pueden reducir en diferentes etapas del desarrollo de un proyecto de seguridad, la aplicación de hardware específico optimizado para utilizar la menor cantidad de compuertas lógicas o la implementación de los algoritmos de cifrado por medio de software, entre otras opciones. En ambas se ha demostrado que el uso de la criptografía de curvas elípticas presenta los mejores resultados.

Un ejemplo donde la criptografía de curvas elípticas ofrece beneficios claros es en la utilización de las tarjetas inteligentes, en este campo los criptosistemas RSA para claves mayores a 1024 bits requieren un coprocesador matemático para lograr un performance aceptable, lo que trae consigo una mayor complejidad y por ende un valor comercial más elevado, mientras que para curvas elípticas no se requiere de un coprocesador, a lo más de un pequeño set de hardware reducido.

4.4.- EVALUACIÓN TÉCNICO – OPERATIVA

Las curvas elípticas pueden ser implementadas con gran eficiencia en hardware y software, y son capaces de competir en velocidad con sistemas como RSA y DSS. En general se cree que son seguros, pero esto no ha sido

demostrado. La seguridad de los sistemas de criptografía con curvas elípticas es buena a priori y, pese al esfuerzo realizado para intentar atacarlos, hasta el momento no ha habido ninguna sorpresa. Sin embargo, las curvas elípticas parecen funcionar eficientemente en la práctica y presentan una ventaja definitiva en cuanto al tamaño de la clave.

Existen varios intentos de estandarización para los criptosistemas de curvas elípticas (como por ejemplo ECDSA por ANSI). Actualmente las curvas elípticas son sobradamente conocidas, pero su uso en la práctica no está muy extendido.

Considerando temas de evaluación, la elección de una curva elíptica como la base de un sistema de clave pública plantea el análisis de una gran variedad de opciones diferentes. En nuestro caso de estudio se emplea curvas elípticas sobre cuerpos finitos con grandes módulos primos (256, 384, y 521) publicado por el NIST con el fin de establecer comparativas con criptosistemas de tipo RSA.

El análisis se sustenta en la generación de dos certificados. El primer certificado, RSA, con clave de 2048 bits y el segundo es un certificado ECC con clave de 224 bits (robustez equivalente a 2048 bits en claves RSA) empleado en un servidor SSL, considerando requerimientos de memoria, el tiempo de ejecución y la razón cifrado □descifrado obtenida a nivel de hardware. El estudio muestra una comparación del tiempo de respuesta de cifrado y descifrado de un Web Server UltraSparc III de 900 MHz corriendo Apache 2.0.45, usando RSA y curvas elípticas con distintos tamaños de claves.

Los certificados se entregan en formato PKCS#12 y la generación de claves es llevada a cabo por la entidad certificadora EADTrust. Dado que los

certificados ECC no los soportan todos los navegadores, es necesario configurar los servidores de forma que se usen los algoritmos más potentes que soporte cada navegador, combinando ambos certificados para lo cual es necesario instalar los certificados raíz de las dos jerarquías de certificación:

- RSA root CA (sha1RSA). RSA 2048-bit.

- ECC root CA (sha1ECDSA). ECC 224 bits.

Tanto Internet Explorer, como Chrome y Mozilla Firefox soportan el cifrado ECC. De momento, Opera y Safari no lo soportan, aunque esto puede cambiar en breve. La forma de implementar una solución que sea compatible en el 100% de los casos es instalar el certificado RSA en el modo seguro de un servidor convencional (puerto 443), y si al establecer el protocolo SSL se detecta que el browser soporta la robustez criptográfica extra, se le desvía automáticamente a otro puerto (o a otro servidor) en el que se instala el certificado ECC.

NOTA: Las pruebas técnico operativo se sustentan en certificados de Prestador de Servicios de Certificación de EADTrust (European Agency of Digital Trust) que dispone de CAs root vinculadas que combinan criptografía RSA y criptografía ECC (Elliptic Curve cryptography).

De la evaluación efectuada y considerando el entorno de implementación citado en el [APÉNDICE A] se tiene que en la figura 4.1 se muestra un comparativo de los tiempos de respuesta del servidor entre usar un algoritmo basado en curva elíptica y RSA. Como se ve claramente, usar el algoritmo RSA es menos eficiente, en cambio al usar curvas elípticas, el impacto es mucho menor, y por lo tanto, el tiempo de respuesta es más rápido. La respuesta a

dicha diferencia que se encuentra en el orden de diez a uno, es debido a la sobrecarga de cálculos que presenta RSA, que no es más que los requerimientos de computación que necesarios para ejecutar las transformaciones de clave privada y clave pública.

FIGURA 4.1.- Gráfico comparativo entre el tiempo de respuesta de un servidor al usar algoritmos criptográficos RSA y curvas elípticas según peticiones de transacciones por segundo. Fuente: Evaluación Técnico – Operativo [APÉNDICE A].

En la tabla 4.7, se muestra una comparativa que respalda lo indicado en el gráfico anterior.

TABLA 4.7.- Comparación de performance de RSA y curvas elípticas. Fuente: Evaluación Técnico – Operativo [APENDICE A].

PARÁMETRO	ECC-160	RSA-1024	ECC-224	RSA-2048
TIEMPO (ms)	3.69	8.75	5.12	56.18
OPERACIONES/SEG	271.3	114.3	195.5	17.8
RATIO DE PERFORMANCE	2.4 : 1		11:1	
RATIO DE TAMAÑO DE CLAVE		1:6.4		1:9.1

Aquí se exponen los sistemas con sus tamaños de claves equivalentes, mostrando los tiempos de respuesta (ms), operaciones por segundos, el ratio de rendimiento entre ellos y el ratio entre los tamaños de claves. Claramente se nota la superioridad en todos estos aspectos de la criptografía de curva elíptica respecto a RSA, incluso se observa que si se utiliza una curva con clave de 224 bits (equivalente a RSA de 2048 bits), sigue siendo más rápido que usar RSA de 1024 bits, con lo que aumentaríamos la seguridad y la velocidad actual de muchos sistemas basados en RSA.

Por otro lado, en relación al tamaño de clave. En la tabla 4.8 se muestran los tamaños de clave pública y privada, y de parámetros del Sistema. Es claro que los ECC son más cortos que los de RSA.

TABLA 4.8.- Tamaño de los parámetros del sistema y par de claves (en bits). Fuente:Evaluación Técnico – Operativo [APENDICE A].

ALGORIMO PARAMETROS DEL SISTEMACLAVE PÚBLICA CLAVE PRIVADA

RSA N/A 1088 20148

ECC 481 161 160

Un factor elemental para evaluar la eficiencia de los criptosistemas es el ancho de banda. En este tema se considera mensajes cortos, ya que los criptosistemas de clave pública son a menudo empleados para transmitir mensajes cortos, como claves de sesión para algoritmos de encriptación de clave simétrica. Para hacer una comparación concreta, supongamos que cada sistema está siendo usado para firmar un mensaje de 2000 bits, o para encriptar un mensaje de 100 bits.

En las Tablas 4.9 y 4.10 se comparan las longitudes de las firmas y mensajes encriptados respectivamente. Denotando que ECC ofrece un ahorro de ancho de banda considerable sobre los otros tipos de sistemas de clave pública. Por lo tanto, todos estos ahorros redundan en velocidades más altas, menor consumo de energía, y reducciones en el tamaño del código.

TABLA 4.9.- Tamaño de firma (en bits). Fuente: Evaluación Técnico – Operativo [APENDICE A].

ALGORIMO TAMAÑO DE FIRMA

RSA 1024

ECC 320

TABLA 4.10.- Tamaño de mensaje encriptado (en bits). Fuente: Evaluación Técnico – Operativo [APENDICE A].

ALGORIMO TAMAÑO DE MENSAJE ENCRIPTADO

RSA 1024

ECC 321

Además, del análisis a los tres factores obtenidos: sobrecarga en cálculos, tamaño de clave y ancho de banda, se observa que el tiempo de procesamiento al usar curvas elípticas se reduce desde un 29% hasta un 85% respecto a RSA. Otro estudio importante es el tiempo que se demora un equipo en romper el nivel de seguridad de los algoritmos. Para que quede comprobado el potencial (en cuanto a eficiencia y seguridad) de este sistema lo compararemos con el RSA mediante la tabla 4.8.

TABLA 4.11.- Eficiencia y Seguridad (RSA vs Curvas Elípticas). Fuente: [32]

Nº DÍGITOS	SISTEMA CRIPTOGRÁFICO	Nº OPERACIONES (CIFRADO/DESCIFRADO)	Nº OPERACIONES (RUPTURA CLAVE)	TIEMPO (RUPTURA CLAVE CON ORDENA . DE 109 FLOPS)
30	RSA	9.0 E 02	2.7 E 07	0.3 SEGUNDOS
	CURVAS ELÍPTICAS	2.7 E 04	1.0 E 15	11 DIAS
35	RSA	1.2 E 03	1.4 E 08	1.2 SEGUNDOS
	CURVAS ELÍPTICAS	4.2 E 04	3.0 E 17	9.1 DIAS
40	RSA	1.6 E 03	7.3 E 08	6.0 SEGUNDOS
	CURVAS ELÍPTICAS	6.4 E 04	1.0 E 20	3.0 E 03 AÑOS
50	RSA	2.5 E 03	1.4 E 10	2.0 MINUTOS
	CURVAS ELÍPTICAS	1.2 E 05	1.0 E 25	3.0 E 06 AÑOS
85	RSA	7.2 E 03	9.0 E 13	1 DIA
	CURVAS ELÍPTICAS	6.1 E 05	3.0 E 42	….
100 (*)	RSA	1.0 E 04	2.3 E 15	28 DIAS
	CURVAS ELÍPTICAS	1.0 E 05	1.0 E 50	….

200 (*)	RSA	4.0 E 04	1.2 E 23	3.8 E 6 AÑOS
	CURVAS ELÍPTICAS	8.0 E 05	1.0 E 100	….

(*) Considerando el tiempo de validación requerido para la implementación de las pruebas de seguridad y siendo que estas se encuentran fuera del alcance del trabajo de tesis se ha tomado la referencia de la fuente Taher ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory a fin de validar nuestro estudio.

Finalmente, podemos observar que las diferencias son significativas, siempre muy a favor de las curvas elípticas. Esto es así porque el logaritmo elíptico puede ser una función mucho más segura que el logaritmo discreto o la factorización cuando se trabaja con números enteros de una determinada dimensión, concluyendo que la criptografía de curva elíptica usa menos ancho de banda que los algoritmos comúnmente usados para protocolos de SSL/TLS, considerando el esquema de pruebas evaluado.

4.5.- PROPUESTA DE ARQUITECTURA FUNCIONAL [1]

Considerando los requerimientos normativos establecidos en la resolución de Junta Bancaria N° JB-2012-2148, publicada en el Registro Oficial de 19 de junio de 2012, se tiene que la Superintendencia de Bancos y Seguros a la fecha no ha definido los lineamientos e instrumentado controles para el cumplimiento

normativo en relación del numeral 4.3.8.6 de la mencionada norma que dispone lo siguiente:

"4.3.8.6 Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;"

En referencia a lo planteado, uno de los objetivos del trabajo de tesis es diseñar una arquitectura hardware de un sistema de cifrado/descifrado de datos mediante criptografía de curva elíptica que opere en tiempo real y que permita guiar a las instituciones financieras en el cumplimiento de las disposiciones normativas.

El modelo se sustenta en el uso de procesadores de seguridad (NSP – Network Security Processor) considerando la normativa vigente "hardware de propósito específico" [1] para la transmisión y almacenamiento de información restringida y confidencial en la red, base de datos, etc., como el caso de la información de tarjetahabientes y cuando esta información sea parte de los procesos internos de los sistemas.

El uso de equipos hardware de encriptación permite el almacenamiento seguro de claves, que son los datos sensibles de esta tecnología y permitan mitigar los riesgos reforzando los controles. Por otro lado, dentro del mercado existe una variedad de productos hardware y software (HSM – IBM, Atalla – HP,

entre otros); sin embargo, el estudio planteado se orienta en la adopción de un criptosistema de curva elíptica con compresión de datos permitiendo de esta manera que los datos a cifrarse se comprimen primero de manera transparente mediante un algoritmo de compresión sin pérdida implementado en hardware. Una de las ventajas de este enfoque es el poder mejorar el rendimiento del sistema al reducir la cantidad de información a cifrarse, además de posibilitar más información con el mismo ancho de banda disponible.

a.- Modelo Funcional Propuesto

El Modelo propuesto se basa en relacionar la criptografía y la compresión entendiéndose que la criptografía convierte información inteligible en algo totalmente ininteligible permitiendo la confidencialidad de los datos, mientras que la compresión reduce la cantidad de información y con ello, los costos de espacio de almacenamiento y tiempo de transferencia. La combinación de estas dos tecnologías importantes en las aplicaciones en red no ha sido explotada ampliamente. Compresión y criptografía han sido consideradas como tecnologías opuestas: mientras que los algoritmos de criptografía esconden patrones de información predecible, los algoritmos de compresión buscan esos patrones de información para sustituirlos por tokens de longitud menor. La compresión y la criptografía deben realizarse en el orden correcto, se aplica primero compresión a los datos y después se realiza el proceso de cifrado. Si primero se realizara el cifrado de los datos y a continuación la compresión, no se tendrían buenos

resultados debido a que los datos cifrados presentan muy poca redundancia con lo que la compresión sería pobre.

La Criptografía de Curva Elíptica (ECC) para este caso ofrece la principal ventaja sobre el criptosistema ampliamente usado y aceptado RSA de operar con llaves de longitud de hasta 6 veces más cortas, ofreciendo los mismos niveles de seguridad que RSA con longitud de llave de 1024 bits.

Tomando como referencia implementaciones efectuadas, se ha medido el tiempo de ejecución de forma modular por el INAOP (Instituto Nacional de Astrofísica, Óptica y Electrónica) de la ciudad de México, como una base para comenzar a realizar el diseño de la arquitectura hardware que implemente el algoritmo ECES. En la Tabla 4.9 se muestran los tiempos de ejecución para el cifrado de dos archivos con y sin compresión previa.

TABLA 4.9.- Tiempo de ejecución de ECES. Fuente: Estudio Base. [35]

TAMAÑO (Bytes)	Tc (s)	TAMAÑO COMPRIMIDO (Bytes)	Tg(s)	Tcf(s)	Tsc(s)
152,089	0.05	72.322	2.22	0.04	0.1
8,673,375	3.18	4.204.995	2.57	2.37	4.65

En la tabla 4.9, Tc representa el tiempo en realizar la compresión, Tg es el tiempo en generar la curva elíptica y las llaves pública y privada, Tcf es el tiempo en realizar el cifrado de los datos con compresión y Tsc es el tiempo en realizar el cifrado sin compresión. Los tamaños de los archivos están dados en bytes y los tiempos de ejecución están expresados en segundos. Al reducir la cantidad de información, el tiempo para realizar el cifrado se reduce también cerca del 50%. Igualmente se observa que los tiempos para comprimir y cifrar son elevados. La generación de la curva, el cálculo de K*P y la compresión de la información son las partes que más tiempo consumen y donde se hace evidente una optimización mediante soluciones en hardware.

ECC ofrece los más altos niveles de seguridad dentro de los criptosistemas de llave pública ya que el mejor algoritmo que se conoce para resolver el problema matemático, en el que ECC basa su seguridad, es de complejidad exponencial.

Tanto los algoritmos de compresión como los algoritmos criptográficos realizan operaciones computacionales intensivas y sus implementaciones en software no satisfacen los requerimientos para sistemas donde el procesamiento de los datos debe realizarse eficientemente.

FIGURA 4.2.- Modelo Base de Arquitectura Propuesta (Hardware) – Fuente: Propia Autoría.

Considerando lo expuesto, el modelo define en hardware de manera eficaz una arquitectura que realice el cifrado/descifrado de datos en tiempo real aplicando criptografía de curva elíptica. Una de las principales razones para realizar una implementación en hardware es la velocidad de operación, ya que los algoritmos criptográficos son caros computacionalmente y se ejecutan ineficientemente en procesadores de propósito general. Un diagrama general de la arquitectura propuesta se muestra en la Figura 4.2.

Para mejorar el rendimiento del sistema, la información a cifrarse se comprime primero mediante un algoritmo de compresión sin pérdida. Además de reducirse la información a procesarse, la compresión desaparecerá patrones en los datos de entrada que pudieran ser empleados por criptoanalistas para recuperar la información original. En base a lo definido, el diseño debe plantearse con un lenguaje de descripción de hardware (RPG/400,RPGLE) y la implementación de la arquitectura hardware se realizará en un dispositivo lógico programable (FPGA), por cuanto permite conexiones tipo TCP/IP, asegurando un control en estado de conexión o cierre del enlace.

Por otro lado, la compresión de datos reduce la cantidad de información disminuyendo los costos de almacenamiento y transmisión. Existen varias técnicas para realizar compresión de datos obteniendo una razón de compresión promedio de alrededor del 50%. Los métodos de compresión sin pérdida permiten recuperar íntegramente la información original a partir de la información comprimida arrojando una baja tasa de comprensión.

Existen dos enfoques para realizar compresión sin pérdida: mediante métodos estadísticos y mediante métodos basados en diccionarios. Entre los

métodos estadísticos destacan Codificación de Huffman, Codificación Aritmética, entre otros . Los métodos estadísticos consiguen las mejores razones de compresión asignando códigos de longitud variable a los símbolos de entrada de acuerdo a su frecuencia [35]. Debido a que se requieren las estadísticas de los símbolos antes de realizar la codificación, los requerimientos de espacio y tiempo son elevados. Por otra parte, los métodos basados en diccionario realizan la compresión sustituyendo ocurrencias de subcadenas en la entrada por índices de un diccionario donde se almacenan las subcadenas que ya han aparecido previamente. Los métodos basados en diccionarios no logran las razones de compresión de los métodos estadísticos, pero sus implementaciones son menos costosas en cuanto tiempo y espacio. Una característica importante de los métodos basados en diccionario es la rapidez para descomprimir los datos.

Las arquitecturas propuestas para compresión de datos sin pérdida pueden dividirse en dos enfoques principales: mediante CAM'S (Content Addressable Memory) y mediante arreglos sistólicos. En estudios realizados por la IEEE [33], se implementa el método estadístico de codificación de Huffman dinámico, el cual, realiza la compresión asignando códigos de longitud variable a los símbolos de entrada. Los códigos se asignan recorriendo un árbol binario que se construye conforme los datos se leen. Los símbolos menos frecuentes serán hojas de las ramas más profundas del árbol y tendrán los códigos de longitud más grande. Los símbolos más frecuentes se situarán en las hojas de las ramas menos profundas y tendrán códigos más cortos. La arquitectura propuesta se basa en CAM's, contiene alrededor de 17,700 compuertas, opera a 40 MHz, tiene un rendimiento de 40 Mbps y logra una razón de compresión del 50%. En estudios realizados por Jung [34], se implementa el algoritmo LZ77 (Modelo de compresión Lempel y Jacob Ziv), el cual es un método basado en diccionario. Se

tiene un arreglo de elementos de procesamiento que buscan la subcadena de mayor longitud en el diccionario. La arquitectura ocupa alrededor de 11000 transistores con un rendimiento de 90 Mbps.

En lo que se refiere a la conjunción de compresión con criptografía, solo se conocen algunos trabajos realizados por empresas como HiFn, PKWare y CISCO. En PKWare, al programa de compresión PKZip v6 se le agregan capacidades de cifrado. El algoritmo utilizado para realizar las operaciones criptográficas es RSA. En HiFn, se aborda el problema que se tiene al aplicar cifrado a la carga útil de los paquetes que se transmiten en red. El algoritmo empleado para compresión es LZS, un método basado en diccionario y los algoritmos para el cifrado de la información son el DES y el 3DES, ambos, algoritmos de criptografía de llave privada. En CISCO se incorporan módulos para compresión y cifrado junto con enrutadores para redes de comunicación para mejorar el rendimiento en la transmisión de datos. La carga útil de los paquetes se comprime según el protocolo de compresión IPPCP o mediante el algoritmo LZS. La información comprimida se cifra con el algoritmo AES (llave privada) con longitudes de llave de 128, 192 y 256 bits.

La arquitectura que se propone en esta investigación constituye una línea de estudio innovadora ya que no existe una implementación en hardware reportada de un algoritmo de cifrado mediante ECC en el Ecuador. De igual forma, no se han reportado arquitecturas para cifrado que integren compresión en el mismo chip.

b.- Proceso de Autorización de tarjetas de Crédito

El diseño que se muestra a continuación pretende ejemplarizar el módulo funcional propuesto, cubriendo el proceso de autorización de tarjetas de crédito integrando el Procesamiento del Emisor de tarjetas que no es más que resolver las peticiones de autorización y el Procesamiento de Adquirencia que resuelve las peticiones de autorizaciones de clientes externos a los adquirentes. El diagrama de flujo implementado se muestra en la figura 4.3, donde el equipo Atalla realiza la validación del PIN y los códigos de seguridad de la tarjeta (CVV1), fecha de caducidad y PVV que vienen en el track 1 y/o track II. Se añade validación de ICVV y ARQC. La validación de estos datos es realizada utilizando el hardware criptográfico (ATALLA). Además, debe recalcar que no se almacena y no se desencripta datos sensibles previo a la comprensión y validación en la caja.

Por otro lado, el sistema de autorizaciones propuesto en cumplimiento con las normas PCI no graba los datos de seguridad de las tarjetas como son PIN, CVV1, CVV2, entre otros.

FIGURA 4.3.- Arquitectura Propuesta. Esquema de Autorización de Tarjetas de Crédito.

Fuente: Propia Autoría.

c.- Resultados

El estudio de la conjunción de compresión con criptografía no ha sido explotado ampliamente. La compresión ofrece ventajas a la criptografía al reducir la cantidad de información que el cifrador procesará y al desaparecer

patrones predecibles en los datos que pudieran emplearse para descifrar la información. Los avances logrados indican que realizando compresión en tiempo real y realizando las operaciones de ECC en hardware especializado, es posible tener un sistema de cifrado con la más alta seguridad que realice el procesamiento de los datos en periodos de tiempo mínimos, lo que permite recomendar ampliamente su uso en la implementación de proyectos criptográficos.

CAPÍTULO V

BENCHMARK DE EVALUACIÓN

La evaluación dentro de este capítulo se plantea mediante el uso de una herramienta de Cifrado a nivel de software de propia autoría como parte de los objetivos propuestos del trabajo de tesis, cuya implementación se basa en un Modelo de criptografía de .NET Framework bajo lenguaje de programación c# [APÉNDICE B]. De esta implementación, se ha medido el tiempo de ejecución considerando cinco pruebas de cifrado y descifrado con el fin de comprobar la eficacia del algoritmo de curva elíptica en comparación al algoritmo de RSA.

NOTA: Por motivos de validación se consideraron los valores de prueba de estudios efectuados por la Universidad Central de Chile por cuanto están sustentados en estándares NIST [6].

5.1.- CIFRADO Y DESCIFRADO DEL ALGORITMO DE CURVAS ELÍPTICAS

Para la prueba de Cifrado y Descifrado del Algoritmo de Curva Elíptica se plantea el uso de la palabra "PUCEPRUEBA" y se usaron los siguientes valores NIST:

TABLA 5.1.- Valores de Prueba 01 para validación.

163 Bits Privada de A.

584600654932361167281474244287639068925684320158 4

Privada de B.

584600654932361167281474244287639068925684320158 3

233 Bits Privada de A.

690174634679056378743475586227702555583981273734501355537938363448546 0

Privada de B.

690174634679056378743475586227702555583981273734501355537938363448545 9

283 Bits Privada de A.

777067556890291628367784762729407562656962592437690488910919652677004427787378692868

Privada de B.

777067556890291628367784762729407562656962592437690488910919652677004427787378692867

409 Bits Privada de A.

661055968790248598951915308032771039828404682964281219284648798304157774827374805208143723762179110965979867288366567526768

Privada de B.

661055968790248598951915308032771039828404682964281219284648798304157774827374805208143723762179110965979867288366567526767

571 Bits Privada de A.

386453752301725834469535189093198734429892732970643499865723525145151914228956042453614399938941577308313388112192694448624687228168130702345282883033241139319110528570 0

Con los valores ya mencionados se obtuvieron los siguientes resultados arrojados por la herramienta RSA-ECC CryptoService Versión 1.0:

TABLA 5.2.- Valores Resultado de Prueba 01 para validación / RSA-ECC CryptoService Versión 1.0

TAMAÑO DE CLAVE	TIEMPO EN PRUEBAS DE CIFRADO	TIEMPO PROMEDIO DE CIFRADO	TIEMPO EN PRUEBAS DE DESCIFRADO	TIEMPO PROMEDIO DE DESCIFRADO
163 Bits	00:00:00,20	00:00:00,19	00:00:00,19	00:00:00,19
	00:00:00,19		00:00:00,19	
	00:00:00,17		00:00:00,19	
	00:00:00,19		00:00:00,19	
	00:00:00,19		00:00:00,19	
233 Bits	00:00:00,44	00:00:00,44	00:00:00,45	00:00:00,49
	00:00:00,42		00:00:00,58	
	00:00:00,42		00:00:00,45	
	00:00:00,48		00:00:00,53	
	00:00:00,42		00:00:00,42	
289 Bits	00:00:00,98	00:00:01,06	00:00:01,11	00:00:01,05

	00:00:01,03	00:00:00,98		
	00:00:00,97	00:00:00,98		
	00:00:01,13	00:00:01,03		
	00:00:01,17	00:00:01,14		
409 Bits	00:00:02,16	00:00:01,95	00:00:02,41	00:00:02,00
	00:00:01,89	00:00:01,95		
	00:00:01,92	00:00:01,89		
	00:00:01,88	00:00:01,88		
	00:00:01,89	00:00:01,89		
571 Bits	00:00:07,81	00:00:07,33	00:00:06,99	00:00:07,14
	00:00:07,56	00:00:07,56		
	00:00:07,98	00:00:07,83		
	00:00:06,64	00:00:06,67		
	00:00:06,66	00:00:06,66		

A partir de los valores obtenidos se puede graficar los resultados , como lo muestra las figuras 5.1 y 5.2.

FIGURA 5.1.- Cifrado ECC - Tiempo versus tamaño de clave. Fuente: RSA-ECC CryptoService.

FIGURA 5.2.- Descifrado ECC - Tiempo versus tamaño de clave. Fuente: RSA-EC CryptoService.

Como se puede apreciar, claramente en las figuras 5.1 y 5.2, tanto para cifrar como para descifrar el algoritmo de curva elíptica no se demora más de 10 segundos en cada proceso, lo cual corrobora la rapidez de cálculos que realiza este tipo de algoritmo.

5.2.- CIFRADO Y DESCIFRADO DEL ALGORITMO DE RSA CON CLAVE DE DESCIFRADO RÁPIDA.

Para la prueba de Cifrado y Descifrado del Algoritmo de RSA con clave de descifrado rápida se plantea el uso de la palabra "PUCEPRUEBA" y se usaron los siguientes valores NIST:

TABLA 5.3.- Valores de Prueba 02 para validación.

1024 Bits. Valor de P. Número de 309 Dígitos.

Valor de Q. Número de 309 Dígitos.

Valor de Clave Privada. 65537

1024 Bits. Valor de P. Número de 675 Dígitos.

Valor de Q. Número de 675 Dígitos.

Valor de Clave Privada. 65537

3072 Bits. Valor de P. Número de 925 Dígitos.

Valor de Q. Número de 925 Dígitos.

Valor de Clave Privada. 65537

7680 Bits. Valor de P. Número de 2312 Dígitos.

Valor de Q. Número de 2312 Dígitos.

Valor de Clave Privada. 65537

15360 Bits. Valor de P. Número de 4624 Dígitos.

Valor de Q. Número de 4624 Dígitos.

Valor de Clave Privada. 65537

Con los valores ya mencionados se obtuvieron los siguientes resultados arrojados por la herramienta RSA-ECC CryptoService Versión 1.0:

TABLA 5.4.- Valores Resultado de Prueba 02 para validación / RSA-ECC CryptoService Versión 1.0.

TAMAÑO DE CLAVE TIEMPO EN PRUEBAS DE CIFRADO TIEMPO PROMEDIO DE CIFRADO TIEMPO EN PRUEBAS DE DESCIFRADO TIEMPO PROMEDIO DE DESCIFRADO

1024 Bits	00:00:04,52	00:00:04,37	00:00:00,03	00:00:00,03
	00:00:04,34	00:00:00,03		
	00:00:04,33	00:00:00,03		
	00:00:04,33	00:00:00,03		
	00:00:04,34	00:00:00,03		
2048 Bits	00:00:43,33	00:00:43,23	00:00:00,16	00:00:00,15
	00:00:43,13	00:00:00,14		
	00:00:43,33	00:00:00,16		
	00:00:43,13	00:00:00,16		
	00:00:43,23	00:00:00,14		
3072 Bits	00:01:50,17	00:01:49,94	00:00:00,30	00:00:00,30
	00:01:49,86	00:00:00,30		
	00:01:49,83	00:00:00,28		
	00:01:49,91	00:00:00,30		
	00:01:49,92	00:00:00,30		
7680 Bits	00:32:00,09	00:29:32,01	00:00:02,52	00:00:01,92
	00:32:19,36	00:00:01,77		

	00:27:47,41	00:00:01,77			
	00:27:46,58	00:00:01,77			
	00:27:46,63	00:00:01,75			
15360 Bits	03:38:40,02	03:40:05,55	00:00:06,99	00:00:06,99	
	03:39:38,75	00:00:06,98			
	03:41:48,08	00:00:07,02			
	03:41:21,39	00:00:07,03			
	03:38:59,53	00:00:06,95			

Y a partir de los valores obtenidos descritos se tiene las figuras 5.3 y 5.4:

FIGURA 5.3.- Cifrado de RSA con clave rápida - Tiempo versus tamaño de clave. Fuente: RSA-ECC CryptoService.

FIGURA 5.4.- Descifrado de RSA con clave rápida - Tiempo versus tamaño de clave. Fuente: RSA-ECC CryptoService.

Como se aprecia en las figuras 5.3 y 5.4, claramente el proceso de cifrado requiere bastante tiempo de procesamiento a diferencia del proceso de descifrado, esto es debido a que la clave privada es de un menor tamaño.

5.3.- CIFRADO Y DESCIFRADO DEL ALGORITMO DE RSA CON CLAVE DE DESCIFRADO LENTA

Para la prueba de Cifrado y Descifrado del Algoritmo de RSA con clave de descifrado lenta se plantea el uso de la palabra "PUCEPRUEBA" y se usaron los siguientes valores NIST:

TABLA 5.5.- Valores de Prueba 03 para validación.

1024 Bits. Valor de P. Número de 309 Dígitos.

Valor de Q. Número de 309 Dígitos.

Valor de Clave Privada. Número de 616 Dígitos.

1024 Bits. Valor de P. Número de 675 Dígitos.

Valor de Q. Número de 675 Dígitos.

Valor de Clave Privada. Número de 1349 Dígitos.

3072 Bits. Valor de P. Número de 925 Dígitos.

Valor de Q. Número de 925 Dígitos.

Valor de Clave Privada. Número de 1850 Dígitos.

7680 Bits. Valor de P. Número de 2312 Dígitos.

Valor de Q. Número de 2312 Dígitos.

Valor de Clave Privada. Número de 4624 Dígitos.

15360 Bits. Valor de P. Número de 4624 Dígitos.

Valor de Q. Número de 4624 Dígitos.

Valor de Clave Privada. Número de 9247 Dígitos.

Con los valores ya mencionados se obtuvieron los siguientes resultados:

TABLA 5.6.- Valores Resultado de Prueba 03 para validación / RSA-ECC CryptoService Versión 1.0.

TAMAÑO DE CLAVE TIEMPO EN PRUEBAS DE CIFRADO TIEMPO PROMEDIO DE CIFRADO TIEMPO EN PRUEBAS DE DESCIFRADO TIEMPO PROMEDIO DE DESCIFRADO

1024 Bits 00:00:04,31 00:00:04,29 00:00:04,25 00:00:04,25

00:00:04,28 00:00:04,30

00:00:04,31 00:00:04,23

00:00:04,27 00:00:04,25

00:00:04,27 00:00:04,24

2048 Bits 00:00:43,13 00:00:42,43 00:00:42,31 00:00:42,30

00:00:42,17 00:00:42,25

	00:00:42,34	00:00:42,33			
	00:00:42,23	00:00:42,25			
	00:00:42,30	00:00:42,38			
3072 Bits	00:01:47,72	00:01:47,53	00:01:47,53	00:01:47,49	
	00:01:47,45	00:01:47,38			
	00:01:47,61	00:01:47,50			
	00:01:47,48	00:01:47,61			
	00:01:47,38	00:01:47,42			
7680 Bits	00:27:40,83	00:27:33,27	00:27:30,95	00:27:32,20	
	00:27:30,52	00:27:31,58			
	00:27:31,02	00:27:31,63			
	00:27:31,83	00:27:35,63			
	00:27:32,17	00:27:31,19			
15360 Bits	03:37:52,78	03:38:13,20	03:36:42,56	03:38:35,97	
	03:37:53,94	03:37:51,63			
	03:37:57,39	03:40:18,75			
	03:38:13,34	03:38:14,17			

03:39:08,55 03:39:52,72

A partir de los valores obtenidos se tiene las figuras 5.5 y 5.6, cabe destacar que el gráfico está en una escala logarítmica para apreciar de mejor forma los valores expuestos en el gráfico.

FIGURA 5.5.- Gráfico de cifrado RSA con clave lenta tiempo versus tamaño de clave. Fuente: RSA-ECC CryptoService.

FIGURA 5.6.- Gráfico de descifrado RSA con clave lenta tiempo versus tamaño de clave. Fuente: RSA-ECC CryptoService.

Como se observa en las figuras 5.5 y 5.6, el proceso de cifrado requiere un tiempo superior de procesamiento y el proceso de descifrado requiere una cantidad de tiempo de procesamiento muy similar al proceso de cifrado.

5.4.- CURVAS ELÍPTICAS VERSUS RSA

Finalmente se presenta un gráfico comparativo del rendimiento de los 3 tipos de cifrado y descifrado los cuales se pueden apreciar en las figuras 5.7 y 5.8, cabe destacar que para la construcción de este gráfico se usó una escala logarítmica para poder apreciar de mejor forma las diferencias.

FIGURA 5.7.- Gráfico comparativo de cifrado RSA versus ECC. Fuente: RSA-ECC CryptoService.

FIGURA 5.8.- Gráfico comparativo de descifrado RSA versus ECC. Fuente: RSA-ECC CryptoService.

Como se puede apreciar en los gráficos de las figuras 5.7 y 5.8, el proceso de cifrado realizado por el algoritmo de curvas elíptica requiere un menor tiempo para cifrar los mensajes, a diferencia del algoritmo de RSA que requiere un tiempo mucho mayor para realizar el proceso de cifrado.

Para el proceso de descifrado no hay mucha diferencia en tiempo entre el algoritmo de curva elíptica y el algoritmo de RSA cuando se selecciona una clave privada pequeña, se realiza el proceso de descifrado de una manera rápida y con una clave privada de mayor tamaño el tiempo de descifrado se asemeja mucho al tiempo de cifrado.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

Todo el proceso de desarrollo realizado a lo largo de los anteriores capítulos de este trabajo de tesis, sirvieron para fundamentar, desarrollar y evaluar la criptografía de curva elíptica como un método para la gestión de firmas y certificados digitales. Asimismo, se describen los campos de aplicación a nivel de seguridad en canales transaccionales orientados a entidades financieras controladas por la Superintendencia de Bancos y Seguros, como base de un estudio de implementación normativa (Resolución N° JB-2012-2148).

Dentro de los productos obtenidos se propone líneas de acción sobre una propuesta normativa en materia de criptografía. Además se plantea una arquitectura funcional sustentada en la conjunción de compresión con criptografía para el diseño implementación de un sistema de seguridad, así como el desarrollo de entornos de prueba que permitieron validar y comparar el rendimiento de los algoritmos criptográficos asimétricos.

Por otro lado, se desarrolló una herramienta software "RSA-ECC CryptoService" Versión 1.0., para la ejecución de pruebas de cifrado y descifrado a fin de comprobar la eficacia del algoritmo de curva elíptica en comparación al algoritmo de RSA.

6.1.- CONCLUSIONES

La utilización de curvas elípticas para aplicaciones criptográficas permite ofrecer los servicios de autenticidad e integridad en un canal transaccional a través de protocolos criptográficos eficientes (ECDSA, ECIES y WTLS) y con un buen nivel de seguridad, siendo éstos los que fundamentan aplicaciones a nivel de firmas y certificados digitales. Esto abre las puertas al desarrollo de productos comerciales que puedan ofrecer nuevos servicios de seguridad para ser implementados en donde el poder de cómputo, espacio de almacenamiento, la memoria o el ancho de banda sea limitado. Lo que permite su uso en Smart Cards, Teléfonos celulares, Fax, Organizadores de Palma, PCs, entre otros.

De la evaluación y análisis efectuado se concluye que:

1. Las Instituciones Financieras en el Ecuador cuentan con un nivel de seguridad informática limitado tomando en cuenta el constante incremento de riesgos en la transferencia de la información a través de canales de comunicación, además de no contar con herramientas que garanticen la integridad y la autenticidad de la data generando vulnerabilidades en la protección de la información, equipos e infraestructura, siendo la posible causa los delitos detectados e impactos operativos sobre la plataforma tecnológica que soporta los procesos financieros.

2. La Seguridad Informática en las Redes de Comunicación en nuestro país no está orientada al aprovechamiento máximo de los recursos disponibles mediante la utilización de diversas herramientas y técnicas de criptografía asímetrica. La Superintendencia de Bancos y Seguros como organismo de control sobre el riesgo tecnológico establece disposiciones normativas generalizadas sin embargo no se dispone una normativa que brinde

el marco referencial sobre la implementación de soluciones criptográficas aplicadas a los diferentes en canales transaccionales y que permitan disminuir el impacto de los riesgos identificados.

3. Dentro de los métodos criptográficos de cifrado encontramos los sistemas simétricos y los sistemas asimétricos, los cuales difieren en el manejo de las claves que hacen posible sus respectivos procesos de cifrado y descifrado. Ambos tipos criptográficos logran satisfacer algunos de los principios básicos de la seguridad informática como la confidencialidad e integridad, sin embargo, para el caso de los sistemas asimétricos también se logra satisfacer el principio básico de la irrefutabilidad de la información.

4. Existen dos métodos criptográficos asimétricos que destacan en este trabajo de tesis, la criptografía RSA y la criptografía de curvas elípticas. RSA es el método criptográfico más famoso y usado en la actualidad y ha logrado establecerse en la mayoría de los sistemas informáticos seguros, sin embargo resultado de estudio efectuado se afirma concluyentemente que el método de curvas elípticas hoy en día se presenta como una alternativa eficaz para reemplazar a futuro lo que RSA ofrece.

5. Las curvas elípticas ofrecen en criptografía como ventaja frente a los sistemas clásicos como RSA; la posibilidad de tener la misma seguridad con claves de tamaño reducido en el orden mínimo. Otra ventaja del método de curvas elípticas por sobre RSA radica en la capacidad de optimizar y reducir los tiempos de procesamiento matemático ofreciendo un mismo nivel de seguridad con menos cálculos, lo que se traduce a cargas de datos menores y mayor rapidez para ejecutar todo tipo de transacciones. Tanto RSA como curvas elípticas se encuentran respaldados por muchos estudios de alto nivel que

acreditan ser métodos criptográficos eficientes. Poseen además normativas que regulan su utilización en aplicaciones tanto a nivel gubernamental como comercial, como por ejemplo las normativas aplicadas por los estándares fijados por la IEEE, NIST, ANSI entre otras.

6. Los algoritmos basados en curvas elípticas para aplicaciones criptográficas y los desarrollos de software de dominio público, permiten la construcción de aplicaciones (Firmas y Certificados Digitales) para ofrecer los servicios de autenticidad e integridad sobre canales transaccionales con un alto performance y rendimiento sobre los métodos actuales de encriptación.

7. Resultado de las pruebas efectuadas se demostró la eficiencia en la generación de claves del criptosistema de curvas elípticas, contra el ya tradicional método de cifrado-descrifado RSA, específicamente en cuanto a su tiempo de cifrado y su tiempo de descifrado bajo un prototipo de simulación donde podemos observar que las diferencias son significativas, siempre muy a favor de las curvas elípticas. Esto es así porque el logaritmo elíptico puede ser una función mucho más segura que el logaritmo discreto o la factorización cuando se trabaja con números enteros de una determinada dimensión.

8. El diseño de un sistema de cifrado/descifrado de datos mediante criptografía de curva elíptica que opere en tiempo real sustentado en la conjunción de compresión con criptografía no ha sido explotado ampliamente. La compresión ofrece dos ventajas a la criptografía al reducir la cantidad de información que el cifrador procesará y al desaparecer patrones predecibles en los datos que pudieran emplearse para descifrar la información. Los avances logrados en este tema propuesto indican que realizando compresión en tiempo real y realizando las operaciones de ECC en hardware especializado, es posible

tener un sistema de cifrado con la más alta seguridad que realice el procesamiento de los datos con mayor rendimiento.

Con todos los argumentos presentados anteriormente, se puede afirmar que la utilización de curvas elípticas para aplicaciones criptográficas ofrece los servicios de autenticidad e integridad sobre canales transaccionales con un buen nivel de seguridad y alto rendimiento lo que comprueba satisfactoriamente la hipótesis de investigación propuesta.

6.2.- RECOMENDACIONES

a. Es imprescindible que las instituciones financieras y demás organismos utilicen claves seguras con la finalidad de eliminar posibles fraudes y minimizar los riesgos financieros generados, considerando que desde hace 5 años el Departamento Norteamericano que regula el uso de estándares (NIST, National Institute of Standards and Technology) recomienda usar claves de al menos 2.048 bits, mientras que las nuevas autoridades de certificación recomiendan que sean de 4.096 bits. Todos coinciden en que se deberá de empezar a usar las técnicas de cifrado por Algoritmos de curvas elípticas.

b. Las Instituciones financieras deberán adoptar estándares en relación de algoritmos y protocolos criptográficos acreditados a nivel internacional dadas las limitaciones de la legislación ecuatoriana y amparados en las buenas prácticas, siendo la criptografía de curva elíptica una alternativa viable dada la eficiencia demostrada y demás ventajas presentadas sobre los servicios de autenticidad e integridad.

c. Es imprescindible que organismos tales como la Superintendencia de Telecomunicaciones "SUPERTEL" y el Consejo Nacional de Comunicaciones "CONATEL", de acuerdo a su ámbito de aplicación, generen normativa a nivel de soluciones criptográficas, a fin de contar con estudios y estándares que orienten en el uso adecuado de las tecnologías criptográficas.

d. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices por parte de la Superintendencia de Bancos y Seguros del Ecuador que orienten a las entidades financieras en la implementación de soluciones criptográficas en el cumplimiento de las disposiciones contenidas en la resolución N° JB-2012-2148 a fin de asegurar razonablemente su efectividad y minimizar los riesgos generados.

e. Dentro de las líneas futuras de estudio que pueden extender el presente trabajo de tesis se tiene el desarrollo de protocolos de enrutamiento para autentificación, usando criptografía de curvas elípticas para dispositivos móviles que integren una red inalámbrica ad-hoc. Así como, el desarrollo de algoritmos de firma digital para dispositivos móviles. Por otro lado, se sugiere la creación de una entidad generadora de certificados digitales, usando criptografía de curvas elípticas.