Revista Ciencia & Tecnología

No. 13, 31 de enero de 2017
ISSN impreso: 1390 - 6321

Criptografía y seguridad en M-COMMERCE
Cryptography and security in M-COMMERCE

Ing. Cristhian Romero Romero[1]
cristhianromero@uees.edu.ec
Ing. Yasser Alvarado Salinas[1]
yalvarado@uees.edu.ec
Ing. Nixon Paladines Enríquez[2]
nr.paladines@alumnos.urjc.es

Recibido: 1/09/ 2016, Aceptado: 1/11/ 2016

RESUMEN
El presente trabajo analiza los parámetros de seguridad más utilizados en el comercio electrónico realizado a través de dispositivos móviles (m-commerce), dentro de este se hace referencia a los tipos de cifrados que se usan con el fin de precautelar la seguridad de la información, así como también los algoritmos más usados para mantener un alto nivel de confidencialidad, integridad y de disponibilidad de la información financiera de los usuarios. Se investigó el nivel de seguridad que se obtiene mediante el uso de los distintos sistemas criptográficos, y los protocolos más utilizados (SSL-TLS-SE) en las plataformas disponibles para el intercambio de la información. A partir del estudio realizado, se puede concluir que varios de los sistemas de protección de información a nivel criptográfico poseen ciertas falencias a nivel de los protocolos que son usados en las distintas plataformas. Por otra parte, los algoritmos A3, A5, RSA, 3DES y MD5 empleados de la manera correcta son útiles; resulta necesaria la investigación de los restantes, utilizados a nivel del cifrado para comercio electrónico, puesto que se emplean de acuerdo a su requerimiento y arquitectura.

Palabras clave: Criptografía, Comercio móvil, SSL/SET, A3, A5, RSA, 3DES, MD5

ABSTRACT
This paper analyzes the security parameters most commonly used in e-commerce made through mobile devices (m-commerce), within this refers to the types of encryption used in order to safeguard the security of the information, as well as the most common algorithms to maintain a high level of confidentiality, integrity and availability of financial information from users. The level of security obtained through the use of different cryptographic systems, and the most widely used protocols (SSL-TLS-SE) in the available platforms for the exchange of information. Based on the research carried out, it can be concluded that several protection systems information cryptographic level has certain shortcomings in terms of the protocols that are used on various platforms. On the other hand, A3, A5, RSA, 3DES and MD5 algorithms

[1]Maestrante en Auditoría de Tecnologías de la Información, Universidad Espíritu Santo. Ecuador

[2]Maestrante en Ingeniería de Sistemas de Información Universidad Rey Juan Carlos. España

employed in the correct way are useful, it is necessary to investigate the remaining algorithms used at the encryption level for e-commerce, as used according to your requirement and architecture.

Keywords: Cryptography, m-commerce, SSL/SET, A3, A5, RSA, 3DES, MD5

Introducción

En esta etapa de la globalización que el mundo ha vivido a través del tiempo, el conocimiento se vuelve la herramienta que busca ser puesta a disposición mundial, las diversas tecnologías de la información y comunicación no dejan de sorprender con sus avances tanto en la velocidad como la calidad de datos que pueden administrar, de esta manera Pérez-Montoro (2010) sugiere que se vuelve importante el hecho de generar nuevos métodos de protección para la información que se envía a través de cualquier entorno. Si bien a través de los años se ha procurado establecer sistemas cada vez más seguros y confiables, también se procura mejorarlos en otros sentidos, muchas veces estos dos objetivos no son conseguidos de manera simétrica, según Islas (2000), suelen ser aprovechados por algunas personas, aunque en la actualidad existe gran cantidad de protocolos que aseguran la calidad y la integridad de la información que se envía o recibe.

Una de las herramientas que ha tenido gran acogida dentro del mundo moderno es el comercio electrónico o e-commerce, ya que permite interactuar de tal manera que se eliminan en cierta forma el "contacto físico" y la distancia, pero pueden ser vulnerables; algo a tener en cuenta según López, Mata & Domínguez (2009). Dentro del e-commerce, el m-commerce o comercio móvil hace referencia a las transacciones comerciales por medio del dispositivo móvil, para ello ha sido necesaria la elaboración, desarrollo e implementación de protocolos de seguridad, con el fin de proveer la mayor confiabilidad a ambas partes dentro del intercambio de información en la actividad comercial (Balado, 2005; M. B. López & Vicario).

La criptografía se vuelve entonces la herramienta adecuada en este tipo de situaciones, al permitir cifrar información de una manera segura y que se ajuste a los requerimientos de los usuarios (Forouzan & Mukhopadhyay, 2011), esto mediante el uso adecuado de protocolos y algoritmos de seguridad, según (Arturo, 2015; Pabón Cadavid, 2010b; Rodríguez, 2004); uno de los factores a tomar en cuenta es el tipo de conexión utilizada para la transmisión de la información y de los medios, más allá de los mecanismos de seguridad que se impongan dentro del sistema. El presente trabajo tiene como objetivo realizar la descripción y análisis de los protocolos, plataformas y algoritmos implementados en e-commerce, principalmente a través de dispositivos móviles, dentro de los cuales se necesita un elevado nivel de seguridad, debido a que implica transacciones financieras e información delicada de los usuarios y las empresas que oferten productos o servicios.

Desarrollo

Criptografía

Es una ciencia sustentada en la utilización de las matemáticas complejas, con el objetivo de acrecentar la seguridad de las transacciones informáticas (Orozco, 2014). Los sistemas criptográficos son diseñados con el fin de ocultar la información, para descifrarla se requiere de una llave o clave (Merchán, 2013). Las empresas que

participan del e-commerce revisan constantemente sus protocolos de seguridad, en los que son utilizadas herramientas de criptografía. En los sistemas computarizados que presentan fallas en su seguridad, se utilizan técnicas criptográficas para prevenir este tipo de situaciones (Ángel, 2000). La integridad, autenticidad y confiabilidad son las preocupaciones principales en cuanto a la seguridad de las transacciones comerciales de origen electrónico (Gamba, 2010).

Etimológicamente proviene del griego "Kryptos", escondido, y "Graphos", escritura; literalmente se traduce como: "escritura escondida" (Pabón Cadavid, 2010a). Según De Miguel (2008) es la escritura de mensajes, de tal manera que una persona que quiera leerlo no pueda entenderlo, a menos que conozca cómo fue encriptado o cifrado. Según Kem (2008), la criptografía se basa en algoritmos definidos y organizados, a los que corresponden una serie de sendas finitas, describen los pasos para dar solución a un problema planteado, entonces todo algoritmo criptográfico requiere de una clave con la extensión adecuada para ser interpretado (Mendoza & César, 2008). La criptografía requiere de ciertos elementos (Pabón Cadavid, 2010a): el mensaje (información) que se desea transmitir, el sistema de comunicación mediante el cual se envía el mensaje, y el sistema que permitirá el cifrado y descifrado del mensaje (Pabón Cadavid, 2010). Para la consideración de un criptosistema informático, se deben tomar en cuenta las siguientes condiciones generales: poseerá un conjunto finito de unidades de mensajes para transmitir, un conjunto de textos cifrados, un conjunto de claves, un conjunto de funciones de cifrado y por último las de descifrado.

Seguridad y Criptografía

De la necesidad de proteger de manera adecuada la información y los sistemas informáticos que la administran, surge la seguridad informática (Paredes, 2006). Con el fin de que exista seguridad, confidencialidad, disponibilidad e integridad de la información que se desea resguardar, nace la criptografía como un elemento de seguridad informática (Orozco, 2000); a pesar de esto posee ciertas limitaciones que se solucionan a medida que progresan los sistemas, tal es el caso de algoritmos que se "degradan" con el tiempo, como resultado del incremento de la velocidad y la potencia con la que los equipos de cómputo son elaborados (López, 2013).

Cifrado Público Y Privado

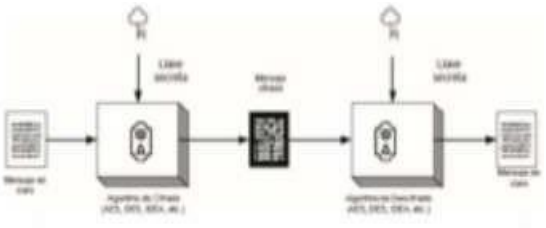

Gráfico 1.- Funcionamiento de una llave privada

Fuente: (Arturo, 2015)

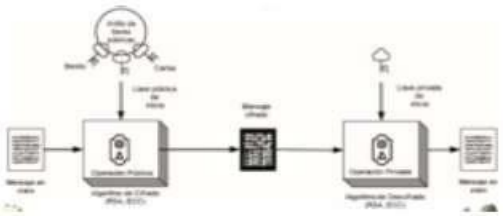

Gráfico 2.- Funcionamiento de una llave pública

Fuente: (Arturo, 2015)

La simétrica es llamada así porque las partes que intervienen poseen la misma clave tanto para cifrar como para descifrar, en cambio en la asimétrica se usa una para cifrar (llave pública) y otra para descifrar (llave privada) (Arturo, 2015).

Firma Electrónica
Es un conjunto de datos agrupados a un mensaje o un componente de software, que garantiza la seguridad de la identidad del firmante y la probidad del mensaje (Rodríguez & Díaz, 2006). También es una modalidad de aplicación de un procedimiento informático criptográfico a un documento de tipo digital, lo cual garantiza su integridad y autenticidad (Formentín, 2013), (Hoch, 2003), y consiste en un dispositivo de caracteres que acompaña a un documento o fichero certificando a su autor (acreditación) y asegurando la integridad de la información (Consejería de Educación y Ciencias, 2013). La mayor y más completa plataforma de firmas digitales es Docusign, es una de las más completas de la industria en lo referente al manejo de firmas digitales en teléfonos móviles. Dentro de las nuevas posibilidades que brinda está la posibilidad de emisión de documentos, la opción de configurar la secuencia de los firmantes y de igual manera la firma en persona, productividad fuera de línea, entre otras (Docusign, 2013).

Comercio Electrónico
Es un tipo de operación comercial, donde la transacción se hace a través de un sistema de comunicación electrónico, eliminando el "contacto físico" entre comprador y vendedor (Balado, 2005).

Tipos de Amenazas
Dentro de los tipos de amenazas en relación a la seguridad informática, está el eavesdropping, que toma su significado literalmente como la posibilidad de escuchar conversaciones sin autorización del emisor, según Bruß (1998); el masquerading es la recepción o el envío de mensajes usando la identidad de un comercio de tipo electrónico (Forouzan & Mukhopadhyay, 2011); message tampering, que se refiere a la posibilidad de interceptar y modificar mensajes que han sido enviados a un servicio de e-commerce (Vigna, 1998); replaying que es la utilización de mensajes enviados de una manera previa, para engañar a una tienda electrónica con el fin de obtener algún beneficio. Entre otros tipos existentes es posible nombrar brevemente, según Reiter (2015): infiltration, traffic analysis y denial of service.

No. 13, 31 de enero de 2017
ISSN impreso: 1390 - 6321

Tipos de Amenazas de Seguridad en Dispositivos Móviles
• Falta de acceso a los recursos del servidor de usuarios
• Ataques DOS
• Web jacking: vandalismo en los sitios
• TCP/IP SYN ataque
• Saturación del servidor con las peticiones de URL
• PING de la muerte (Sambana, 2016)

Protocolos de Seguridad Ssl (Secure Sockets Layer) y Tls (Transport Layer Security)
El SSL/TLS constituye un protocolo de seguridad, el cual citando a Davies (2011), es funcional para cualquier aplicación de internet, siendo posible implementarlo dentro del e-commerce.

SET (Secure Electronic Transaction)
Protocolo especialmente diseñado para el comercio electrónico, requiere la utilización de tarjetas de crédito (Meihua Xiao, Zilong Wan, & Hongling Liu, 2014)-

Dispositivos Móviles y E-commerce
Una de las principales características del e-commerce y la mayor ventaja, es la desaparición de intermediarios y la implementación de nuevos componentes a la transacción como: tecnología, acceso a la red, seguridad, certificación y protección de la información que se administra. Habitualmente su seguridad está dada mediante las siguientes técnicas y protocolos que indica Ponce Vásquez (2002): Transporte (Protocolos TLS6, WTLS7); Contenidos: Protección de la propiedad intelectual (Watemarking, Fingerprinting); Acceso (Firewalls, SHH); Autoría (Firma digital).

Dado que el e-commerce está siendo aceptado a una velocidad realmente impresionante, no se puede dejar de contemplar a su vez el mobile commerce o el comercio móvil, que hasta donde sugiere Abad (2007), es la realización de transacciones del tipo comercial a través de dispositivos móviles (tabletas o teléfonos). La exitosa entrada de la telefonía móvil a nivel mundial, representa un importante punto que viene siendo aprovechado para la realización del e-commerce sobre entornos inalámbricos, según Sandor Otero Rodríguez (2016), aunque para muchos poseen desventajas que deben ser solucionadas, como el ancho de banda, la mayor latencia y la estabilidad de la conexión; sin duda alguna el factor determinante a ser tratado es la seguridad. En el m-commerce se utilizan entidades de software e internet, para conectarse confiablemente, garantizando la autentificación, la confidencialidad e integridad de los procesos que lleven a cabo.

M-Commerce y M-Payment
El m-payment hace referencia a los procesos para el intercambio de valores financieros usando un dispositivo móvil, según varios autores (Duane, O'Reilly, & Andreev, 2014; Thomas, 2002), constituye una manera insegura de realizar transacciones financieras.

M-Commerce Aspectos de Seguridad
Dentro de las principales tecnologías "claves" para el uso de pago móvil, están las mencionadas por Kadhiwal and Zulfiquar (2007): WAP; redes, incluyendo GSM,

GPRS, 3G; software para pago móvil; Bluetooth; Smart Card y SIMs.

El temor de la mayoría de usuarios es ser víctimas de fraudes, una de las tecnologías que termite disipar estos temores es PKI (Public Key Infrastructure), según Ardila (2013), es una infraestructura independiente de las aplicaciones que han sido basadas en servicios de criptografía mediante claves, brinda confidencialidad y seguridad a los usuarios (Pascale, 2000). En cuanto a las redes móviles existe WPKI (Wireless Public Key infrastructure) ("Mobile payment security gets smart," 2001).

Tabla 1.- PKI y otros sistemas de seguridad en internet

	ESTANDAR	NAVEGADORES	CONTROL DE ACCESO	FIRMA DIGITAL	B2C	B2B	VPN
PKI	X	X	X	X	X	X	X
SET	X	-	-	-	-	X	-
TOKEN	-	-	X	-	-	-	-

Fuente: Elaboración propia

Dentro del m-commerce es indispensable la seguridad, pero no la proporciona la especificación de la capa de seguridad WTLS (Wireless Transport Layer Security de WAP), según lo mencionado por Fuquene (2008), aunque el uso de WTLS y la seguridad a nivel de la capa de transporte TLS permite una mayor privacidad en los canales inalámbricos e internet, no es suficiente para el e-commerce. Se sugiere el uso de una capa nueva dentro de WAE (Wireless Application Environment), llamada WAE-SEC (Meihua Xiao et al., 2014). Existen modelos que permiten obtener seguridad en el entorno del m-commerce (Fig. #3), dado que el modelo WAP es muy similar al WWW, posee varias de sus características que son modificadas en el caso del m-commerce (J. R, 2006).

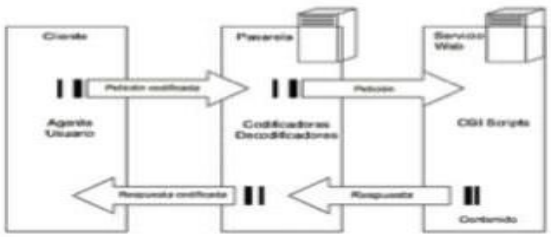

Gráfico 3.- Modelo WAP para e-commerce

Fuente: Ardila, 2013

WAE permite en cierta manera procesar más adecuadamente los servicios de servidores web actuales, estos usan los URL estándar, según Ardila (2013) WAE mejora algunos de los estándares WWW adecuándolos a las características de los móviles y de las redes, por medio de una pasarela que se encarga de codificar y decodificar los datos con el fin de minimizar la carga y el coste de los datos.

La utilización de WTLS para proveer de seguridad en la comunicación entre terminales puede verse en la figura 4, donde se observa que en la parte de la derecha la pasarela recoge los mensajes codificados con TLS del servidor para convertirlos en WTLS, así mismo las peticiones del teléfono hacia el servidor realizan el camino inverso.

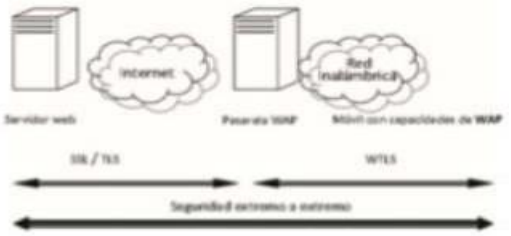

Gráfico 4.- Entidades que intervienen en una transacción Comercial

Fuente: (Ardila, 2013)

Seguridad a Nivel Criptográfico
El principal requerimiento del m-commerce es la posibilidad de realizar pagos a través del dispositivo móvil, por ello resulta indispensable la generación de aplicaciones con altos niveles de seguridad extremo a extremo, en los dispositivos y en la red mediante la cual se realizará la transacción, según Lek and Rajapakse (2012).

Cifrado de Extremo a Extremo (E2ee)
También denominado "End to End encryption", este cifrado supone un extremado nivel de seguridad, el 100%, y es logrado gracias a la utilización de un módulo hardware y de algoritmos únicos; en estos casos los datos que serán enviados se cifran en el dispositivo del remitente, de esta manera el único capaz de descifrarlo es el destinatario (Ron, de las Mercedes, & Ortega Briones, 2009).

Protocolos Ssl y Set en M-Commerce
Según Romero Cando (2005) el SSL es un sistema que asegura una conexión encriptada a través de un esquema denominado "mixto", usa el sistema simétrico y asimétrico, como a continuación se detalla: La clave simétrica se cifra con la clave pública, de esta manera el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un solo paquete, así el destinatario usa su clave privada para descifrar la clave simétrica y seguido a esto usa la clave simétrica para descifrar el mensaje, además mediante el uso de un certificado digital proveniente de una autoridad certificadora se garantiza que la clave pública que estará en los dispositivos móviles corresponde a la clave privada del servidor, comúnmente los algoritmos usados en este esquema suelen ser RSA o DSA para cifrado asimétrico y RC4, IDEA o 3DES para el simétrico.

Para construir una estructura confiable de e-commerce se necesita la participación de dos elementos: certificados para servidores y sistemas de pago seguro en línea. Dentro de los diferentes protocolos de seguridad existentes, para transmitir información a través de un entorno tan inseguro como es el internet existen muchos, pero los protocolos SSL y SET son los más usados en aplicaciones de comercio electrónico (Quintana & Alcivar, 2003), siendo el primero un protocolo para encriptar

transmisiones TCP/IP y el otro para el envío de instrucciones de pago a través de internet. El mundo del internet habitualmente utiliza el protocolo SSL, porque dispone de un nivel seguro de transporte entre el servicio clásico TCP y las aplicaciones que lo utilizan como vía de transporte, como garante de la seguridad a servicios como la compra o venta y transacciones bancarias (M. B. López & Vicario).

El protocolo SSL se compone de dos partes: el Handshake (establece conexión verificando de manera opcional la identidad de las partes y así determinando los parámetros que serán utilizados posteriormente) y la otra Record Protocol (comprime, cifra, descifra y a su vez verifica la información que se transmite luego de realizado el Handshake) (L. M. López et al., 2009). SSL posee tres capas: una capa de mensaje, una de registros (records y alertas) y la capa de transporte (Cobas, 2005). Debido a su estructura, su uso se hace frecuente en compras o transacciones seguras, sobre todo si son dadas para un TPV (Tunel Private Virtual) proporcionado por un banco, dado que no hay manera de conocer si quien usa una tarjeta es el propietario de la misma Visa y Mastercard crearon SET, para de esta manera poder brindar la irrenunciabilidad en el pago mediante tarjetas de crédito.

Tabla 2.- Comparación de los protocolos de seguridad

	SSL	SET	3D SECURE
Confidencialidad	X	X	X
Integridad	X	X	X
Autentifica los titulares de las tarjetas de crédito	X	X	X
Autentifica los comerciantes	X	X	X
Autentifica los bancos		X	X
Verifica que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor			X

Fuente: (L. M. López et al., 2009)

El SSL reemplaza una conexión vía HTTP por otra HTTPS, siendo de esta manera el medio más estandarizado para la transmisión de datos en internet, sobre todo en lo referente a las aplicaciones o sitios de comercio electrónico.

Cifrados GSM

Debido al envío de información "aérea" de los teléfonos celulares, se presenta un entorno que se vuelve inseguro ante la presencia de intrusos con los receptores adecuados, por ello en la tecnología GSM se crearon varias funciones de seguridad para salvaguardar la información, según relata Sandor Otero Rodríguez (2016). GSM utiliza una clave de cifrado con el fin de resguardar la información del usuario y la señalización de la interfaz en el aire; una vez que el usuario es autenticado, el RAND (número aleatorio de 128 bits suministrado por la red); junto con el KI (clave de autenticación) son enviados a través del algoritmo de generación de claves de cifrado A8, con el fin de producir una KC (clave de cifrado), luego de ello el A8 se almacena en la SIM, entonces el KC creado por A8 se utiliza en conjunto con el algoritmo de cifrado A5 para cifrar o descifrar los datos. A5 es implementado en el hardware del

celular, puesto que tiene que cifrar y descifrar durante la marcha (Sandor Otero Rodríguez, 2016).

Aunque el WAP fue diseñado de manera inicial para trabajar con cualquier tecnología móvil existente, actualmente la más usada por WAP es el entorno GSM, se considera que los mecanismos de cifrado de GSM no suelen ser lo suficientemente seguros para cualquier transacción conducida mediante WAP, principalmente por la debilidad de los algoritmos y de igual manera por la porción de camino protegida que se extiende desde la terminal móvil a la BTS (Estación transceptora base).

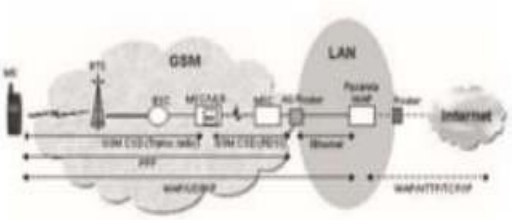

Gráfico 5.- Arquitectura de WAP

Fuente: M. B. López & Vicario

Algoritmos utilizados en m-commerce

Tabla 3.- Principales algoritmos usados en e-commerce / m-commerce

NOMBRE DEL ALGORITMO	CIFRADO SIMETRICO	CIFRADO ASIMETRICO
A5	-	-
A3 Y A8	-	-
RSA	-	X
DSA	-	X
AES	X	-
ECC	-	X
DES	x	-
3DES	X	-
RC4	X	-
IDEA	X	-
MD5	-	X

Fuente: Elaboración propia

En cuanto a los algoritmos A3, A5 y A8, que son comunes en el cifrado de los datos del usuario; A3 es dependiente del operador, es unidireccional, sencillo de calcular los datos de salida, pero muy complejo recuperar los parámetros de entrada (KI Y RAND) (Amador Donado, Ortiz, & López, 2011).

A5

Los más usados son A5/0, que viene sin cifrado; A5/1 es usado en Europa Occidental y América; y A5/2 en Asia (Rodríguez, 2016). A5/1 es el más fuerte porque funciona como un cifrado que realiza la operación xor de tres registros (controlados por un reloj) con el flujo a cifrar, así el bit que controla el reloj de cada registro, es resultante de una función mayoritaria entre 3 bits centrales de cada registro, la longitud de los 3

son 19, 22 y 23 bits (por lo que la longitud de llave es de 64 bits) (Rodríguez, 2004).

Algoritmo de Cifrado de Generación de Clave

Es un algoritmo dependiente del operador, aunque en la mayoría de proveedores se combinan los algoritmos A3 y A8 para dar una función hash llamada COMP128, así este crea el KC y SRES en una misma instancia (Amador Donado et al., 2011).

RSA – Rivest, Shamir y Adleman

Constituye uno de los más utilizados en lo referente a clave asimétrica, mayormente para el cifrado de pequeñas cantidades de datos, como claves y firmas digitales (Franchi, 2013, p. 28). No está diseñado con el fin de reemplazar a otros simétricos, debido a su lentitud de cómputo y el aumento que posee el tamaño del mensaje que se cifra, su utilidad está centrada al permitir un intercambio seguro de claves que luego algoritmos como AES (Advanced Encryption Standard) puedan llevar el cifrado de una manera mucho más eficiente, según (Arturo, 2015; Quisquater & Couvreur, 1982). Su seguridad se logra del problema de factorización de números enteros, los mensajes enviados se representan mediante números, el funcionamiento se basa en el producto "conocido" de dos números primos elegidos al azar y no revelados (García, Morales, & González, 2005).

Gráfico 6.- Diagrama del RSA

Fuente: ULPGC

DSA – Digital Signature Algorithm

Es uno de los principales utilizados para dar la entidad al DSS (Digital Signature Standard). El cual es adoptado por los Estados Unidos para la implantación de firma digital (Naccache & M'raihi, 1995; Panchal, 2015).

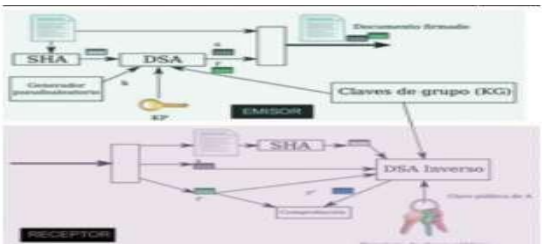

Gráfico 7.- Diagrama del DSA

Fuente: UNAM

Advanced Encryption Standard (AES)
Actualmente es uno de los más utilizados como parte de los algoritmos de cifrado simétrico, fue desarrollado por los estudiantes Vincent Rijmen y Joan Daemen de la Katholieke Universeit Leuven en Bélgica, bajo el nombre de "Rijndael" (Pousa, 2011, p. 13). Se basa en un cifrado por bloques, inicialmente con longitud variable, pero el estándar define el tamaño en 128 bits, entonces los datos son divididos en segmentos de 16 bytes, donde cada segmento puede ser visto como un bloque o matriz 4x4 (Shakir, Abubakar, Yousoff, & Sheker, 2016).

Gráfico 8.- Cifrado AES
Fuente: Pousa, 2011

Criptografía con Curvas Elípticas – ECC
Como solución a la longitud de las claves de RSA, ECC constituye uno de los algoritmos más nuevos de esta familia de clave pública, (Belingueres, 2000). Puede brindar el mismo nivel de seguridad que el RSA o DH, pero utilizando operandos mucho más cortos (160-256 bits contra 1024-3072 bits) (Vera Parra, Alfonso López, Caro, & Cristyan, 2014); además, se basan en el problema de logaritmo discreto (Gómez & Echeverry).

DES (Data Encryption Standard)
Este algoritmo utilizado de la manera apropiada puede constituir una importante barrera de seguridad, su arquitectura se basa en un sistema mono alfabético, aquí se aplican continuas permutaciones y sustituciones al texto por el algoritmo cifrado (Kaba, 2008). Aunque es el algoritmo simétrico más conocido y utilizado en el mundo, se considera inseguro, principalmente por el tamaño de clave de 56 bits (Zibideh & Matalgah, 2015). En la práctica, es calificado como seguro, pero en su variante triple DES.

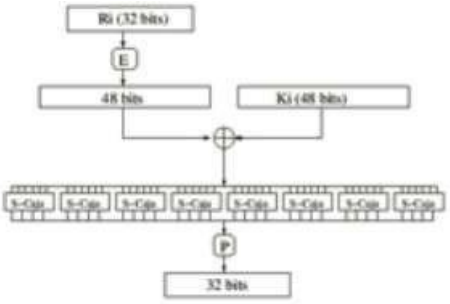

Gráfico 9.- Estructura de red de fiestel para el algoritmo DES

Fuente: NISU.ORG

La creación estuvo a cargo de IBM. Actualmente empieza a desaparecer, siendo reemplazado por AES (Saran, 2005); sin embargo, existe una variante conocida como DES – EDE3, la cual posee 3 claves diferentes y longitud de 192 bits, creando así un sistema de seguridad mucho más robusto (Hielscher & Delgado, 2006).

RC4
En 1987 se desarrolla el RC4, un algoritmo considerado inmune al criptoanálisis diferencial y lineal, es comúnmente usado para el cifrado WEP de la mayoría de accesos WIFI (Hielscher & Delgado, 2006), Es muy seguro, pero aun así el protocolo WEP se considera vulnerable, esto principalmente por problemas con el propio protocolo que dan la posibilidad de determinar la clave en un periodo corto.

IDEA (International Data Encription Algorithm)
Algoritmo cifrado por bloques de 64 bits y emplea claves de 128 bits, a pesar de utilizar claves más largas es considerado dos veces más rápido que DES (González et al., 2002).

MD5
Se ha vuelto popular en la seguridad del comercio electrónico, procesa los mensajes de entrada en bloques de 512 bits y produce una salida de 128 bits (Santra & Nagarajan, 2012). Resulta útil como firma digital de aquellos mensajes que serán compactados y encriptados mediante criptosistema de llave pública. MD5 toma como entrada un mensaje con una longitud arbitraria y como salida se obtiene una "huella digital" con 128 bits del mensaje denominado message-digest (resumen o compendio del mensaje) (Kaba, 2008).

Conclusiones y limitaciones de trabajos futuros
El m-commerce debe realizarse a través de plataformas, servidores y protocolos que aseguren que el proceso será exitoso. El problema general que poseen lo móviles en cuestión de seguridad, es que el acceso a la encriptación sin cable no puede cubrir la conexión entera. Los datos en internet son encriptados con SSL y en la conexión sin cable algunas veces con WTLS, pero el sistema es vulnerable en la pasarela cuando no se utilizan los protocolos correctos.

Una vez que se alcance la seguridad deseada en el entorno web y principalmente en las conexiones inalámbricas de dispositivos móviles, el comercio electrónico se volverá la herramienta más idónea para resolver asuntos comerciales.

El nivel de seguridad que actualmente se obtiene de los algoritmos utilizados para la encriptación de la información comercial que se maneja en las distintas plataformas, como se mencionó en un apartado el algoritmo RSA constituye uno de los más usados, pues conceptualmente se considera que es lo bastante seguro para su utilización, sin embargo existen algunos puntos débiles en la forma de utilizarlo, los cuales pueden ser aprovechados por los atacantes, entre los principales puntos está la debilidad de las claves, puesto que en ciertos casos, RSA deja el mensaje igual al original y sumado a esto la posibilidad de un ataque intermediario en cualquier algoritmo asimétrico. Para efectos de mayor seguridad del comercio electrónico, lo más recomendable es usar la variación 3DES.

Dentro de la existencia de otros algoritmos como RC4 o MD5, empleados en diferentes protocolos, si bien es cierto comprenden sistemas de encriptación seguros, el verdadero problema surge al aplicarse en protocolos que de por sí poseen ciertas vulnerabilidades.

En cuanto al nivel de seguridad que se brinda en los sistemas de comercio electrónico, muchas de las falencias de seguridad se originan por el surgimiento de tecnologías capaces de ser empleadas en la desencriptación de la información, además de esto, otras de las vulnerabilidades son los protocolos que suelen ser ineficientes o estar desprotegidos en ciertas partes, dejando así un espacio para un "ataque" con el fin de obtener la información encriptada.

La seguridad en los sistemas de e-commerce debe ser mejorada en función del avance de la tecnología, los algoritmos utilizados deben ser adecuados de acuerdo a los protocolos, los canales y las necesidades de transmisión de información cifrada, esto en conjunto con la respectiva certificación de las actividades ante el sector financiero, por ser acciones comerciales.

Dentro de las líneas de investigaciones futuras, se puede plantear el mejoramiento de los sistemas de verificación de usuarios en lo correspondiente a la información de seguridad entregada a las plataformas, ya que si el nivel de seguridad de la plataforma resulta deficiente y la información de seguridad de los usuarios resulta vulnerada, el no repudio de las transacciones comerciales con esa información representaría un gran inconveniente tanto financiero como legal, en este sentido para el usuario y la plataforma que se utilice. Así mismo surge cierta necesidad en la investigación de los nuevos métodos de seguridad, ante las nuevas tecnologías de la información que apenas surgen, como Li-fi.

Referencias Bibliográficas

Amador Donado, S., Ortiz, M., & López, F. (2011). Riesgos del algoritmo A3 en el cifrado de telefonía celular. *Generación Digital* (15).

Ardila, H. J. F. (2013). M-commerce: el nuevo protagonista del comercio electrónico.

Vínculos, 4(1), 62-77.

Arturo, R. G. (2015). Criptografía de llave pública.

Balado, E. S. (2005). *La nueva era del comercio/ the new era of commerce*. Ideaspropias Editorial SL.

Belingueres, G. (2000). Introducción a los criptosistemas de curva elíptica. Obtenido en la Red Mundial, 5.

Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters, 81*(14), 3018.

Cobas, J. D. G. (2005). Secure Sockets Layer (SSL), Mayo.

Davies, J. A. (2011). *Implementing SSL / TLS Using Cryptography and PKI*. Hoboken, N.J.: Wiley.

De Miguel, R. (2008). Criptografía clásica y moderna.

DocuSign, I. (2013). DocuSign Establece el Estándar Mundial para la Firma Electrónica (eSignature) Móvil.

Duane, A., O'Reilly, P., & Andreev, P. (2014). Realising M-Payments: modelling consumers' willingness to M-pay using Smart Phones. *Behaviour & Information Technology*, 33(4), 318-334. doi:10.108 0/0144929X.2012.745608

Forouzan, B. A., & Mukhopadhyay, D. (2011). *Cryptography and Network Security.* (Sie): McGraw-Hill Education.

Franchi, M. R. (2013). Algoritmos de encriptación de clave asimétrica. Facultad de Informática.

Fuquene, H. (2008). M-commerce: el nuevo protagonista del comercio electrónico. *Vínculos, 4*(1), 62-77.

Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe.

García, L., Morales, G., & González, S. (2005). Implementación del algoritmo RSA para su uso en el voto electrónico. Presentado en simposio acerca de las urnas electrónicas para la emisión del voto ciudadano.

Gómez, C. B., & Echeverry, G. A. I. Bases matemáticas y aplicaciones de la criptografía de curvas elípticas.

González, I., Gómez, F., López-Buedo, S., Martínez, J., Deschamps, J., Boemo, E., & Martínez, J. (2002). Implementación del Algoritmo Criptográfico IDEA en Virtexusando JBits. *II Jornadas de Computación Reconfigurable y Aplicaciones*, 155-160.

Hielscher, R. P., & Delgado, V. (2006). Introducción a la Criptografía: tipos de algoritmos. Paper presented at the anales de mecánica y electricidad. Hoch, F. G. (2003). La prueba de las obligaciones y la firma electrónica. *Revista Chilena de Derecho Informático* (2).

Islas, O. (2000). *Internet: el medio inteligente*: Compañía Editorial Continental.

J. R, Q. (2006). E-Commerce. *PC Magazine, 25*(18), 92-98.

Kaba, I. (2008). *Elementos básicos de comercio electrónico*. Editora Universitaria, La Habana, Libro en versión digital [Links].

Kadhiwal, S., & Zulfiquar, A. U. S. (2007). Analysis of mobile payment security measures and different standards. *Computer Fraud & Security*, (6), 12-16.

Kem, S. (2008). Introducción a la informática concepto de algoritmos. La Criptografía como elemento de la seguridad informática. (2003). *ACIMED, 11*(6), 90-97.

Lek, K., & Rajapakse, N. (2012). *Cryptography: Protocols, Design, and Applications*. Hauppauge, N.Y.: Nova Science Publishers, Inc.

López, L. M., Mata, F. M., & Domínguez, R. M. R. (2009). Sistemas de pago seguro. Seguridad en el comercio electrónico. *Revista de estudios empresariales. Segunda época* (1).

López, M. B., & Vicario, L. S. D. Seguridad en móviles de segunda generación.

Meihua Xiao, x. e. e. c., Zilong Wan, n. c., & Hongling Liu, n. c. (2014). The Formal Verification and Improvement of Simplified SET Protocol. *Journal of Software (1796217X), 9*(9), 2302-2308. doi:10.4304/ jsw.9.9.2302-2308

Mobile payment security gets smart. (2001). *Financial Technology Bulletin, 18*(16), 2.

Naccache, D., & M'raihi, D. (1995). System for improving the digital signature algorithm: Google Patents.

Orozco, G. N., J. (Producer). (2014). Introducción a la criptografía [Powert Point] Retrieved from http://patux.net/downloads/crypto/crypto.pdf

Orúe López, A. (2013). Contribución al estudio del criptoanálisis y diseño de los criptosistemas caóticos. Telecomunicación.

Pabón Cadavid, J. A. (2010a). La criptografía y la protección a la información digital. *La Propiedad Inmaterial* (14).

Pabón Cadavid, J. A. (2010b). La criptografía y la protección a la información digital. The cryptography and the protection of digital information. (14), 59-90.

Panchal, P. (2015). Mobisecure using DSA. International Journal of Advanced *Research in Computer Science, 6*(8), 88-92.

Paredes, G. G. (2006). Introducción a la Criptografía. *Revista Digital Universitaria, 7*(7).

Pascale, M. (2000). Firma Digital. Paper presented at the Memorias VXl *Congreso Iberoamericano de Derecho e Informática*.

Pérez-Montoro, M. (2010). Arquitectura de la información en entornos web. *El profesional de la información, 19(4)*, 333-337.

Ponce Vásquez, D. A. (2002). Contribución al desarrollo de un entorno seguro de m-commerce.

Pousa, A. (2011). Algoritmo de cifrado simétrico AES. Facultad de Informática.

Quintana, B., & Alcivar, A. (2003). *Implementación de un modelo de comercio electrónico para una empresa privada*. QUITO/EPN/2003.

Quisquater, J.-J., & Couvreur, C. (1982). Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics letters, 18*(21), 905-907.

Reiter, G. (2015). Securing all devices in the Internet of Things. *ECN: Electronic Component News, 59*(6), 20-22.

Rodríguez, S. M. H. (Producer). (2004). Implementación del algoritmo A5/1 (Cifrado de flujo de datos).

Romero Cando, W. F. (2005). *Determinación de los procedimientos para la implementación del protocolo SSL (Secure Sockets Layer) en redes móviles*. QUITO/EPN/2005.

Ron, Z., de las Mercedes, E., & Ortega Briones, J. R. (2009). Análisis de la problemática de interconexión en Ecuador entre los sistemas troncalizados y las redes telefónicas fijas y celulares.

Sambana, B. G. (2016). An Efficient Authentication and Payment Method for M-Commerce. *Computer Science & Telecommunications, 47*(1), 58-63.

Sandor Otero Rodríguez, M. M. S. (2016). Seguridad en redes GSM. http://www.informaticahabana.cu/sites/default/files/ponencias/TEL14.pdf

Santra, A. K., & Nagarajan, S. (2012). A Modified MD5 Algorithm for Wireless Networks. *International Journal of Advanced Research in Computer Science, 3*(2), 292-297.

Saran, C. (2005). Passwords for Oracle was 'cracked in 20 days. *Computer Weekly*, 4-4

Shakir, M., Abubakar, A. B., Yousoff, Y. B., & Sheker, M. (2016). Improvement keys of advanced encryption standard (AES) rijndael_M. *Journal of Theoretical &*

Applied Information Technology, 86(2), 216-222.

Thomas, D. (2002). Vodafone seeks m-payment standards. *Computer Weekly, 8*.

Vera Parra, N. E., Alfonso López, D., Caro, M., & Cristyan, H. (2014). Simulation test-bed for the evaluation of elliptic curve cryptography on next generation wireless IPv6-enabled networks. *Tecnura, 18*(41), 27-37.

Vigna, G. (1998). Cryptographic traces for mobile agents' Mobile agents and security (pp. 137- 153): Springer.

Zibideh, W. Y., & Matalgah, M. M. (2015). Modified data encryption standard encryption algorithm with improved error performance and enhanced security in wireless fading channels. *Security & Communication Networks, 8*(4), 565-573. doi:10.1002/sec.1003