Junio
2015
Edición N° 9
Pág
14 - 21

Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES

Comparison of Algorithms Based Cryptography Symmetric DES, AES and 3DES

Yuri Tatiana Medina Vargas , Haider Andrés Miranda Mnedez[2]

RESUMEN

La seguridad es uno los aspectos más desafiantes de la internet y las aplicaciones de red. Las cuales están creciendo muy rápido, por lo que la importancia y el valor de los datos intercambiados a través de Internet u otros tipos de medios están aumentando. De ahí la búsqueda de la mejor solución para ofrecer la protección necesaria contra ataques de intrusos a nuestros datos, junto con la prestación de estos servicios en el tiempo es uno de los temas más interesantes en las comunidades relacionadas con la seguridad. La criptografía es la una de las principales categorías de la seguridad informática que convierte la información de su forma normal en un formato ilegible. Las dos características principales que identifican y diferencian algoritmo de cifrado uno de otro son su capacidad para asegurar los datos protegidos contra ataques y su velocidad y eficiencia en hacerlo. Este artículo ofrece una comparación equitativa de tres algoritmos de criptografía de clave simétrica más comunes: DES, AES y 3DES.
Palabras clave: Criptografía, DES, AES, 3DES, cifrado, descifrado.

ABSTRACT

Security is one of the most challenging aspects of the internet and network applications. Which are growing very quickly, so that the importance and value of the data exchanged via the Internet or other media types are increasing. Hence the search for the best solution to provide the necessary protection against attacks by intruders to our data, together with the provision of these services in the time it is one of the most interesting topics in the communities related to security. Cryptography is the one of the major categories of computer security that converts the information from its normal form in an unreadable format

1. Universidad de Pamplona, Facultad de Ingenierías y Arquitecturas, Ingeniería de Sistemas (Villa del Rosario), Email: yuri.medina@unipamplona.edu.co
2. Universidad de Pamplona, Facultad de Ingenierías y Arquitecturas, Ingeniería de Sistemas (Villa del Rosario), Email: haider.miranda@unipamplona.edu.co

The two main characteristics that identify and differentiate encryption algorithm from one another are its ability to ensure the data protected against attacks and their speed and efficiency to do so. This article provides a fair comparison of three algorithms for symmetric key cryptography more common: DES, AES and 3DES.

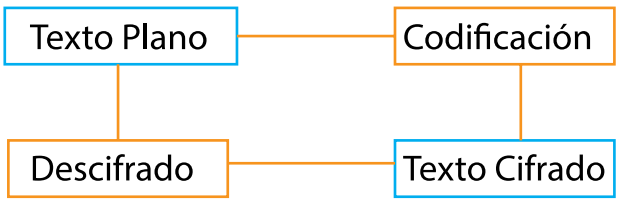
Keywords: Cryptography, DES, AES, 3DES, encryption, decryption.

1. INTRODUCCIÓN

La criptografía se refiere generalmente como "el estudio de secreto". El cifrado es el proceso de convertir texto normal a un formato legible. El descifrado es el proceso de convertir texto cifrado en texto normal en el legible.

Figura 1: Modelo Convencional de Encriptación

Pasos involucrados en el modelo de cifrado convencional:



• Un remitente quiere enviar un mensaje "Hola" a un destinatario.

• El mensaje original, también llamado de texto claro, se convierte en bits aleatorios conocidos como texto cifrado mediante el uso de una clave y un algoritmo. El algoritmo que se utiliza puede producir una salida diferente cada vez que se usa, basado en el valor de la clave.

• El texto cifrado se transmite a través del medio de transmisión.

• Al final del destinatario, el texto cifrado se convierte de nuevo al texto original utilizando el mismo algoritmo y la clave que se utilizó para cifrar el mensaje.

Tal como se define en el RFC 2828 [1] [2], un sistema criptográfico es "un conjunto de algoritmos criptográficos junto con los procesos de gestión de claves que apoyan el uso de los algoritmos en un contexto de aplicación." La definición da todo el mecanismo que proporciona el necesario nivel de seguridad consta de protocolos de red y algoritmos de cifrado de datos.

A. Objetivos de la Criptografía:

Hay cinco objetivos principales de la criptografía. Cada sistema de seguridad debe proporcionar un conjunto de funciones de seguridad que pueden asegurar el secreto del sistema. Estas funciones se refieren generalmente comolos objetivos del sistema de seguridad. Estos objetivos pueden ser listados bajo las siguientes cinco categorías principales [3]:

1. Autenticación: El proceso de probar la identidad de uno. Esto significa que antes de enviar y recibir datos utilizando el sistema, la identidad del receptor y el remitente debe ser verificada.

2.Privacidad/confidencialidad:asegurar que nadie puede leer el mensaje, excepto el receptor previsto. Por lo general, esta función es como la mayoría de la gente se identifica un sistema seguro. Esto significa

que sólo las personas autenticadas son capaces de interpretar el contenido del mensaje y de nadie más.

3.Integridad: Asegurar el receptor que el mensaje recibido no ha sido alterado de ninguna manera de la original. La forma básica de la integridad es paquete de suma de comprobación en los paquetes IPv4.

4.No repudio: Un mecanismo para probar que el remitente realmente envió este mensaje. Significa que ni el emisor ni el receptor pueden falsamente negar que hayan enviado un mensaje determinado.

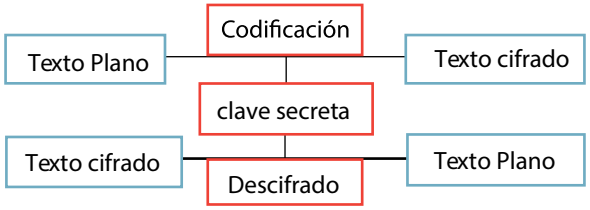
5.Servicio Fiabilidad y disponibilidad: Desde sistemas seguros generalmente atacados por intrusos, que pueden afectar la disponibilidad y el tipo de servicio a sus usuarios. Estos sistemas proporcionan una forma de otorgar a sus usuarios la calidad de servicio que esperan.

B. Cifrados simétricos y asimétricos:

Hay dos categorías principales de la criptografía en función del tipo de claves de seguridad utilizadas para cifrar / descifrar los datos. Estas dos categorías son: técnicas de cifrado simétricas y asimétricas [4].

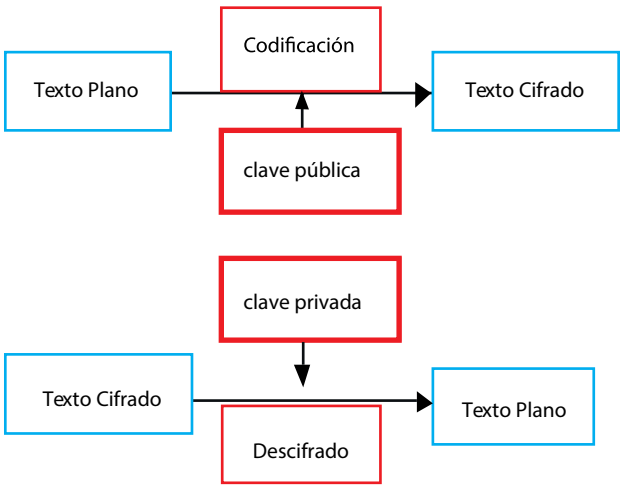
1) Cifrado simétrico: También se conoce como la criptografía de clave única. Se utiliza una sola clave. En este proceso de cifrado del receptor y el emisor tiene que ponerse de acuerdo sobre una sola clave secreta (compartido). Dado un mensaje (denominado texto plano) y la clave, cifrado produce datos ininteligibles, que es aproximadamente la misma longitud que el texto en claro era. El descifrado es la inversa de la codificación, y utiliza la misma clave de cifrado.

Figura 2: Proceso de clave para criptografía simétrica.



2) Cifrado asimétrico: También se conoce como la criptografía de clave pública. Se utiliza dos claves: clave pública, que es conocido por el público, que se utiliza para el cifrado y la clave privada, que es conocida sólo por el usuario de esa clave, que se utiliza para el descifrado. Las claves públicas y la privada están relacionados entre sí por cualquier medio matemático. En otras palabras, los datos cifrados por una clave pública pueden ser encriptados sólo por su clave privada correspondiente. El cifrado y descifrado procedimiento se muestra a continuación en la figura 3:

Figura 3: Proceso de clave para criptografía asimétrica.



C. Modos de cifrado y descifrado:

1. ECB (Electronic Code Book): En este modo de datos se divide en bloques de 64 bits y cada bloque se cifra uno a la vez. Cifrados separados con diferentes bloques son totalmente independientes entre sí. Esto significa que si los datos se transmiten a través de una red o línea telefónica, los errores de transmisión sólo afectarán al bloque que contiene el error. También significa, sin embargo, que los bloques pueden ser reorganizados, luchando así un archivo de más allá del reconocimiento, y esta acción sería pasar desapercibido. ECB es el más débil de los distintos modos porque no hay medidas de seguridad adicionales se aplican además del algoritmo básico DES. Sin embargo, ECB es la más rápida y fácil de implementar, por lo que es el modo más común de DES visto en aplicaciones comerciales.

2. CBC (Cipher Block Chaining): En este modo de operación, cada bloque de texto cifrado con ECB se le aplica una operación XOR con el previo bloque ya cifrado. De este modo, cada bloque cifrado depende de todos los bloques de texto claros usados hasta ese punto. Esto significa que, a fin de encontrar el texto completo de un bloque determinado, lo que necesita saber el texto cifrado, la clave y el texto cifrado para el bloque anterior. El primer bloque a cifrar no tiene texto cifrado anterior, por lo que el texto plano es XOR con un número de 64 bits llamado vector de inicialización, o IV, para abreviar. Así que si los datos se transmiten a través de una red o línea de teléfono y no es un error de transmisión (adición o eliminación de bits), el error se arrastrará a todos los bloques posteriores ya que cada bloque depende de la última. Si los bits se acaba de modificar en tránsito (como es el caso más común) el error sólo afectará a todos los bits en el bloque modificado, y los bits correspondientes en el bloque siguiente. El error no se propaga más allá. Este modo de funcionamiento es más seguro que el ECB porque el paso XOR adicional añade una capa más para el proceso de cifrado.

3. CFB (Cipher Feedback): En este modo, los bloques de texto plano menores de 64 bits de longitud se pueden cifrar. Normalmente, este proceso especial tiene que ser usado para manejar los archivos cuyo tamaño no es un múltiplo de 8 bytes perfecto, pero este modo elimina esa necesidad. El texto plano en sí no se pasa realmente a través del algoritmo DES, sino simplemente se le aplica XOR con un bloque de salida de ella, de la siguiente manera: Un bloque de 64 bits llamada el registro de desplazamiento se utiliza como entrada para el texto plano DES. Esto se ajusta inicialmente a un valor arbitrario, y encriptado con el algoritmo DES. El texto cifrado se pasa luego a través de un componente adicional denominado la caja M, que simplemente selecciona el más a la izquierda M bits del texto cifrado, donde M es el número de bits en el bloque deseamos cifrar. Este valor se XOR con el verdadero texto plano, y la salida de ese es el texto cifrado final. Por último, el texto cifrado se alimenta de nuevo en el registro de desplazamiento, y se utiliza como la semilla de texto plano para el siguiente bloque a cifrar. Al igual que con el modo CBC, un error en un bloque afecta a todos los bloques posteriores durante la transmisión de datos. Este modo de funcionamiento es similar al CBC y es muy seguro, pero es más lento que el ECB debido a la complejidad añadida.

4. OFB (Output Feedback): Es similar al modo CFB, excepto que la salida de texto cifrado de DES se alimenta de nuevo en el registro de desplazamiento, más que el texto cifrado final real. El registro de desplazamiento se establece en un valor inicial arbitrario, y se pasa por el algoritmo DES. La salida del DES se pasa a través de la caja M y luego vuelve a entrar al regis-

tro de desplazamiento para prepararse para el siguiente bloque. Tenga en cuenta que a diferencia de CFB y CBC, un error de transmisión en un bloque no afectará bloques posteriores debido a que una vez que el destinatario tiene el valor inicial Registro de desplazamiento; que continuará generando nuevas Registro de desplazamiento entradas de texto plano sin ninguna entrada de datos adicional. Sin embargo, este modo de operación es menos seguro que el modo CFB porque sólo se necesita la salida de texto cifrado real y DES texto cifrado para encontrar el texto plano del bloque más reciente.

ESTUDIO DE ANTECEDENTES:

(Tamimi, 2008) proporciona una comparación de rendimiento entre cuatro algoritmos más comunes: DES, 3DES, AES, Blowfish y. La comparación se ha llevado a cabo mediante la ejecución de varios ajustes diferentes para procesar diferentes tamaños de bloques de datos para evaluar la velocidad de cifrado / descifrado del algoritmo. La configuración de la simulación era en lenguaje C # de programación. Los resultados de este trabajo muestran que el pez globo tiene un mejor rendimiento que otros algoritmos de cifrado común. AES mostró los resultados de rendimiento pobre en comparación con otros algoritmos, ya que requiere más potencia de procesamiento [5].

• (Penchalaiah, 2010) discutió las principales ventajas de AES con respecto a DES, así como sus limitaciones. Dijeron que AES se puede implementar con bastante comodidad en alto nivel o lenguajes de bajo nivel [6].

• (Elminaam et. Al., 2010) presenta una comparación de AES, DES, 3DES, RC2 y RC6. Utilizaron diferentes configuraciones para cada algoritmo como diferentes tamaños de bloques de datos, diferentes tipos de datos, el consumo de energía de la batería, diferente tamaño de la clave y, finalmente, la velocidad de cifrado / descifrado. Llegaron a la conclusión de que en caso de cambio de tamaño de paquete Blowfish mostró un mejor rendimiento que otros algoritmos seguido por RC6 [7].

• (Singhal y Raina, 2011) presentan un análisis comparativo entre AES y RC4 para una mejor utilización. En este trabajo los autores trataron de averiguar comparación de rendimiento entre las cifras de bloque (AES) y cifrado de flujo (RC4) algoritmo. Con base en el análisis y el resultado, este trabajo concluye que el algoritmo es mejor utilizar en base a diferentes parámetros de rendimiento. Los diversos indicadores fueron: tiempo de cifrado, descifrado tiempo, rendimiento, tiempo de proceso de la CPU, uso de la memoria [8].

CIFRADO POR BLOQUES

En Criptografía, una unidad de cifrado por bloques es una unidad de cifrado de clave simétrica que opera en grupos de bits de longitud fija, llamados bloques, aplicándoles una transformación invariante. Cuando realiza cifrado, una unidad de cifrado por bloques toma un bloque de texto plano o claro como entrada y produce un bloque de igual tamaño de texto cifrado. La transformación exacta es controlada utilizando una segunda entrada — la clave secreta. El descifrado es similar: se ingresan bloques de texto cifrado y se producen bloques de texto plano.

3.1 DES: (Data Encryption Standard): fue el primer estándar de cifrado que será publicado por el NIST (Instituto Nacional de Estándares y Tecnología). Fue diseñado por IBM en función de su cifra de Lucifer. DES se convirtió en un estándar en 1974. DES usa una clave de 56 bits, y los mapas de bloque de entrada de 64 bits en un bloque de salida de 64 bits. La clave parece realmente una cantidad de 64 bits, pero un bit en cada uno de

los 8 octetos se utiliza para la paridad impar en cada octeto. Hay muchos ataques y métodos registrados hasta ahora los que explotan las debilidades de DES, lo que hizo que un cifrado de bloques inseguro [10].

3.2 AES: (Advanced Encryption Standard): también conocido como el algoritmo Rijndael (pronunciado como lluvia muñeca), es un cifrado simétrico de bloques que puede cifrar bloques de datos de 128 bits utilizando claves simétricas 128, 192, o 256. AES se introdujo para sustituir el DES. Ataque de fuerza bruta es el único ataque efectivo conocido en contra de este algoritmo [10] [11].

3.3. 3DES: Triple DES fue desarrollado para hacer frente a lo obvio fallas en DES sin diseñar toda un nueva criptosistema. Triple DES simplemente extiende el tamaño de clave de DES mediante la aplicación del algoritmo de tres veces en sucesión con tres llaves diferentes. El tamaño de la clave combinada es, pues, 168 bits (3 veces 56), más allá del alcance de la fuerza bruta técnicas tales como los utilizados por el FEP DES Cracker. Triple DES siempre ha sido considerado con cierta sospecha, ya que el algoritmo original nunca fue diseñado para ser usado de esta manera, pero sin defectos graves se han descubierto en su diseño, y que es hoy un criptosistema utilizado en un gran número de Internet protocolos [9], [10].

COMPARACIÓN ENTRE AES, 3DES Y DES.

Avance Encryption Standard (AES) y Triple DES (TDES o 3DES) se utilizan comúnmente en cifrados de bloque. Ya sea que se elija AES o 3DES dependiendo de sus necesidades. En esta sección se quiere destacar las diferencias en términos de seguridad y rendimiento. DES fue desarrollado en 1977 y fue diseñado cuidadosamente para funcionar mejor en hardware que en software. de bits en sustitución y permutación en cajas cada una de 16 rondas. Por ejemplo, el cambio de 30 bits con 16 bits es mucho más simple. DES cifra los datos en Tamaño de bloque de 64 bits y utiliza eficazmente una clave de 56 bits. Esta hace que las cantidades de espacio para la clave sean aproximadamente de 72 mil billones posibilidades. A pesar de que parece grande, actualmente no es suficiente y es vulnerable a los ataques de fuerza bruta. Por lo tanto, DES podía no seguir el ritmo de avance de la tecnología y no es más apropiado para la seguridad. Debido a que DES fue ampliamente utilizado en ese momento. La solución rápida era introducir 3DES, que es lo suficientemente seguro para la mayoría de los propósitos de hoy en día.

3DES es una construcción de la aplicación de DES tres veces en secuencia. 3DES con tres llaves diferentes (K1, K2 y K3) tiene la longitud efectiva de la clave es 168 bits. Otra variación de 3DES utiliza dos llaves (K1 y K3), en esta se reduce el tamaño de clave eficaz de 112 bits que es menos segura. Esta se utiliza ampliamente en electrónica industria de pagos. 3DES toma tres veces más potencia, que si se compara con su predecesor el impacto en el rendimiento es significativo.

AES supera 3DES tanto en software y en hardware [12], [13]. El Algoritmo Rijndael ha sido seleccionado como el Avance Encryption Standard (AES) para reemplazar 3DES. AES es versión modificada de Rijndael algorithm y ha sido evaluada bajo los siguientes criterios [8], [9], [10], [11]:

- Seguridad.
- El rendimiento de Software y Hardware.
- doneidad en entornos de espacio restringido.
- Resistencia al análisis del poder y otros ataques de implementación.

Rijndael fue presentado por Joan Daemen y Vincent Rijmen. Se considera en conjunto una combinación de seguridad, vrendimiento, eficiencia, aplicabilidad y flexibilidad. Por esto el diseño de AES es más rápido en software y trabaja eficientemente en hardware. Trabaja rápido, incluso en pequeños dispositivos como teléfonos inteligentes; tarjetas inteligentes etc. Además AES proporciona más seguridad debido a un mayor tamaño de bloque y claves más largas. AES utiliza 128 bits y el tamaño de bloque es fijo para claves de 128, 192 y 256 bits. El Algoritmo en general es lo suficientemente flexible para trabajar con clave y el bloque de cualquier múltiplo de 32 bits con los bits mínimo de 128 y un máximo de 256 bits. AES es el reemplazo para 3DES según NIST ambas cifras coexistirán hasta el año 2030 permitiendo una transición gradual a AES. A pesar de que AES tiene ventaja teórica sobre 3DES para la velocidad y la eficiencia de alguna implementación de hardware 3DES puede ser más rápido algunas veces.

La tabla 1 proporciona un análisis comparativo entre los algoritmos simétricos de criptografía: DES, AES y 3DES. El análisis se ha llevado a cabo mediante la ejecución de doce importantes factores que influyen en la ejecución y rendimiento de estos algoritmos de cifrado.

CONCLUSIÓN

En este artículo se presenta un estudio comparativo entre DES, 3DES y AES donde se presentaron doce factores, que son longitud de la clave, el tipo de cifrado, tamaño de bloque, desarrollado, resistencia criptoanálisis, la seguridad, la clave posibilidad, posible ASCII teclas de caracteres imprimibles, el tiempo necesario para marque todas las claves posibles en 50 mil millones segundos, éstos demostraron que AES es mejor que DES y 3DES.

Tabla 1. Comparación entre AES, 3DES y DES

FACTORES	AES	EDES	EDES
LOGITUD DE LA CLAVE	128,192 y 256 bits	K1 ,K2 YK3 168 bits (k1yk2 168 bits (k1yk2 es mismo) 112bits	56 bits
TIPO DE CIFRAS	Simétrica bloques de Cifrado	Simétrica bloques de Cifrado	Simétrica bloques de Cifrado
TAMAÑO DE BROQUE	128, 192.0 256 Bits	64 BITS	64 BITS
DESARROLLO	2000	1978	1977
RESISTENCIA CRIPTOANALISIS	Diferencial En Contra De Fuerte, truncado Diferencial e Interpolación Lineal y Plazas de Ataques	Vulnerable al diferencial De fuerza Bruta Atacante Podría Ser Analizada de texto Plano con Criptoanálisis diferencial	Vulnerables a diferencial Y lineal criptoanálisis! Las Las tablas de sustitución Débiles
SEGURIDAD	Considerado Seguro	Sólo uno débil Que Es Salir En Des	Resultado insuficiente
POSIBLES CLAVES	$2; 2^{-}$ y 95^{-}	2^{-}, y 2^{-}	2^{-}
POSIBLES TECLA DE CARACTRES ASCII IMPRIMIR	95^{-}, 95^{-} Y 95^{-}	95^{-}, y 95^{-}	95^{-}
IMPRIMIBLE REVISION TODA LA LLAVE EN 50 MIL MILLONES DE CLAVES	para una clave de 128 Bits 5 x10 Años	Para Una Clave de 112 Bits 800 Dias	Para Una Clave de 56 Bits 400 Dias
RONDA	10 (128-Bist) ,12 (192 Bits) , 14 (256 Bits)	48	16
RENDIMIENTO (ENCRIPTACIÓN DESENCRIPTACIÓN)	4.174 / 6.452	3.45/ 5. 665	4.01/6347
CLAVE	solo	Sola(dividida en 3 partes	sola

BIBLIOGRAFÍA

[1]. [Edney2003],” Real 802.11 Security: Wi-Fi Protected Access and 802.11i”. Addison Wesley 2003.

[2]. [RFC2828] Internet Security Glossary, Recuperado el 31 de marzo de 2015 de http://www.faqs.org/rfcs/rfc2828.html.

[3]. [IDRBT CA]“Public Cryptography”, Recuperado el 01 de abril de 2015 de: http://idrbtca.org.in/inf_pki.htm

[4]. [How PGP works] “The Basics of Cryptography” Recuperado el 03 de abril de 2015 de: http://www.pgpi.org/doc/pgpintro/

[5]. Tamimi, A Al; “Performance Analysis of Data Encryption Algorithms”, Oct 2008.

[6]. Penchalaiah, N. and Seshadri, R. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No. 05, 2010, 1641-1645.

[7]. Elminaam, D S Abd; Kader H M Abdual and Hadhoud, M Mohamed. "Evaluating the Performance of Sysmmetric Encryption Algorithms", International Journal of Network Security, Vol. 10, No. 3, pp. 216-222, May 2010.

[8]. Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[9]. A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.

[10]. M. Abomhara, Omar Zakaria, Othman O. Khalifa , A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore.

[11]. Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.

Junio
2015
Edición N° 9
Pág
14 - 21