AES como Estándar Internacional de Cifrado

Lic. Reyna García Belmont [1] M. en A. Gabriela Lotzin Rendón [2]
Ing. Luis Cabrera Hernández [3] M. en A. Ma. del Consuelo Puente Pérez [4] y
Ing. Ofelia Verónica Méndez Lemus [5]

[1 3 4 5] Instituto Tecnológico de Tlalnepantla, Av. Instituto Tecnológico S/N Col. La Comunidad, Tlalnepantla de Baz, Edo. de México, 54070. México
rgarciab@itlta.edu.mx, lcabrerah@ittla.edu.mx, cpuentep@ittla.edu.mx, vmendezl@ittla.edu.mx
[2] Instituto Tecnológico de Ciudad Victoria, Boulevard Emilio Portes Gil #1301 Pte. A.P. 175, Ciudad Victoria, Tamaulipas, 87010. México
lotbrenvaz@outlook.com

Fecha de recepción: 15 de junio 2017
Fecha de aceptación: 2 de febrero 2018

Resumen. Con el uso del internet hoy en día estamos inmersos en la sociedad de la información y tecnología, manteniéndonos siempre conectados y al mismo tiempo expuestos, en ese sentido la seguridad de la información busca proteger la información, la seguridad informática no sólo busca proteger la información, sino también la infraestructura que la rodea (como procesos y sistemas) y finalmente se encuentra la ciberseguridad que abarca la infraestructura de una organización y/ó país; teniendo con esto tres áreas de vital importancia enfocadas a la prevención e implementación correcta de controles que permitan contrarrestar las amenazas. Lo anterior nos lleva a la creación de una aplicación que se pueda incluir en sistemas proporcionando aspectos de seguridad basados en el estándar AES, involucrando procedimientos formales de un protocolo criptográfico. Con este trabajo se busca identificar la tendencia ofrecida por los sistemas criptográficos frente al uso de herramientas convencionales.

Palabras Clave: AES, Criptografía, FIPS,NIST.

1 Introducción

En cualquier organización dedicada al desarrollo de software y aseguramiento de la calidad tienen que definir los objetivos de seguridad de la aplicación a diseñar, identificando la categoría de la información a proteger: identidad, financiera, reputación, privacidad y reglamentaria, entre otras; con la finalidad de detectar amenazas y riesgos a los que la información se expone y adaptar los controles necesarios para su protección. Otras fuentes de riesgo emanan de leyes, normas, acuerdos legales y políticas de seguridad de la información corporativas (Open Web Application Security Project, 23).

De lo anterior se deriva que para crear software se deben aplicar prácticas de diseño seguras e incluir técnicas de codificación defensiva y resistente a los ataques. Por lo que este trabajo presenta un panorama del tipo de seguridad que se puede incluir a través de Advanced Encryption Standard (AES) como mecanismo de control para preservar la confidencialidad de la información en su transmisión en un medio inseguro como lo es el internet y contribuir al diseño de aplicaciones seguras basadas en la implementación de estándares probados de cifrado y descifrado.

AES es un estándar de cifrado simétrico definido dentro de un marco internacional uniforme y publicado por National Institute of Standard and Technology (NIST) como FIPS PUB 197, que a lo largo de la historia se ha definido como uno de los más destacados y seguros.

2 Estado del Arte

La criptografía se considera una disciplina matemática e informática relacionada con el cifrado y autenticación a través del uso de algoritmos que ayudan a crear herramientas de acceso haciendo que la información transmitida no sea entendible para garantizar la confidencialidad y la integridad de la misma (Security Standards Council (PCI), 2014). El proceso de cifrado permite desarrollar sistemas criptográficos definiendo el tipo en base al tipo de llave a utilizar distinguiendo dos métodos:

- Sistemas de clave única o métodos simétricos en los cuales el proceso de cifrado y descifrado son llevados por una misma clave.
- Sistemas de llave pública o asimétrica cuyo proceso de cifrado y descifrado son llevados a cabo por llaves distintas y complementarias.

Ambos sistemas protegen los datos utilizados en una comunicación y se han incluido en el desarrollo de aplicaciones de comunicaciones como: Servicio de Seguridad: Secure Socked Layer (SSL), para el intercambio

de registros (Symantec, 2011), Servicio de Seguridad (Secure Electronic Transaction por sus siglas en inglés SET) para servicios de pagos electrónicos creado por VISA y Master Card (Lu & Smolka, 1999) y Servicio de Seguridad (Private Enhanced Mail por siglas en inglés PEM) (Kent, 1998) entre otros.

Estas aplicaciones hacen uso de criptografía a través de cifrado simétrico, asimétrico, funciones Hash y firma digital en parte o bien incluyendo todo en un solo paquete y que en la actualidad han sido de éxito y se mantienen. En particular el cifrado simétrico preserva la confidencialidad tanto en las transmisiones de información como en su almacenamiento, protegiendo los archivos y evitando que personas ajenas a la información tengan acceso (EcuRed, 2006) .

3 Metodología

En ésta sección se describen la secuencia de los pasos a realizar para transformar el texto plano en datos cifrados y viceversa a través del algoritmo AES identificado a través del estándar FIPS PUB-197, considerado como uno de los algoritmos más sólidos y aceptados por la industria publicados en la serie NIST 800-57 (Barker & Dang, 2015), este algoritmo consiste en iteraciones que emplean funciones invertibles donde los bytes se interpretan como campos finitos conocidos también como campos de Galois[3]. AES opera con bloques y a cada paso del algoritmo se le denomina estado (National Institute of Standards and Technology (NIST), 2001).

3.1 Estructura AES

La estructura de éste algoritmo consiste en una serie de rondas donde se realizan un conjunto de cuatro transformaciones orientadas a bytes, el número de rondas depende del tamaño de la clave como se puede observar en la tabla 1.

	Longitud de clave *(Nk words)*	**Tamaño de Bloque** *(Nb words)*	**Número de Rondas** *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Tabla 2. Número de rondas en función de la longitud de clave (National Institute of Standards and Technology (NIST), 2001)

Las transformaciones aplicadas son: SubByte, ShiftRow, MixColumn, AddRoundKey, Empezando con el proceso de expansión de claves en primera instancia.

3.2 Sub Bytes

Esta operación consiste en una transformación no lineal, donde se realiza una sustitución de cada byte por otro byte establecido en la caja definida por la norma FIPS-197, como S-box, la cual está basada en el inverso multiplicativo del byte que hay que transformar en GF (2^8) módulo ($x^8 + x^4 + x^2 + x + 1$), tomando sus bits como los coeficientes de un polinomio en GF (2^8); en la operación de descifrado se invierte la transformación anterior, a través de la tabla inversa mostrada en la norma.

3.3 ShiftRows

Consiste en un desplazamiento cíclico de bytes en cada fila, en AES la primera fila queda sin cambios, la segunda fila se desplaza un byte a la izquierda, incrementando en uno el número de desplazamientos por fila que se va recorriendo, esto es la fila *n* se desplaza de manera circular izquierda por *n*-1 bytes, quedando el número de desplazamientos como se muestra en la figura 1, considerando bloques de 128 bits.

[3] Campos de Galois son muy utilizados en la criptografía debido a que gracias a ellos existe un inverso aditivo y multiplicativo que permite cifrar y descifrar en el mismo cuerpo Z., eliminando los problemas de redondeo o truncamiento de valores, como si tales operaciones de cifrado y descifrado se hubiesen realizado en aritmética real [8]

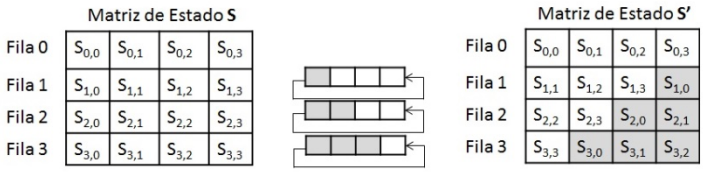

Figura 1. Función ShiftRows para bloque de 128 bits (National Institute of Standards and Technology (NIST), 2001)

3.4 MixColumn

La función MixColumn consiste en multiplicar las columnas de bytes módulo $x^4 + 1$ por el polinomio c(x), expresado de la ecuación 1

$$c(x)= \text{‘03’}x^3 + \text{‘01’}x^2 + \text{‘01’}x + \text{‘02’} \qquad (1)$$

Este polinomio es coprimo con $x^4 + 1$, lo permite que la función sea invertible, ésta fórmula queda expresada de forma matricial en la figura 2.

$$\begin{pmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{pmatrix}$$

Figura 2. Matriz de MixColumn (National Institute of Standards and Technology (NIST), 2001)

En esta matriz “*c*” representa el índice de la columna que se procesa. Cuando se desarrolla la matriz cada byte nuevo de la matriz de Estado es una combinación de varios bytes de las distintas filas que forman una columna específica.

3.5 AddRoundKey

Esta transformación consiste en aplicar una operación OR-Exclusiva entre la matriz de Estado que proviene de la transformación anterior (MixColumn) y una subclave que se genera a partir de la clave del sistema para esa ronda. El bloque resultante es la nueva matriz de estado para la siguiente ronda, siendo en determinado caso el bloque de salida cuando se trata de la última ronda. Esta transformación se expresa en la figura 3.

$$\begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix} \begin{pmatrix} K_0 & K_1 & K_2 & K_3 \\ K_4 & K_5 & K_6 & K_7 \\ K_8 & K_9 & K_{10} & K_{11} \\ K_{12} & K_{13} & K_{14} & K_{15} \end{pmatrix} = \begin{pmatrix} S_{0,0}\oplus K_0 & S_{0,1}\oplus K_1 & S_{0,2}\oplus K_2 & S_{0,3}\oplus K_3 \\ S_{1,0}\oplus K_4 & S_{1,1}\oplus K_5 & S_{1,2}\oplus K_6 & S_{1,3}\oplus K_7 \\ S_{2,0}\oplus K_8 & S_{2,1}\oplus K_9 & S_{2,2}\oplus K_{10} & S_{2,3}\oplus K_{11} \\ S_{3,0}\oplus K_{12} & S_{3,1}\oplus K_{13} & S_{3,2}\oplus K_{14} & S_{3,3}\oplus K_{15} \end{pmatrix}$$

Figura 3. Ejemplo de AddRoundKey [8]

3.6 Expansión de Claves

AES incluye una función de Expansión de Clave, que permite derivar de la clave de cifrado subclaves para cada ronda con la finalidad de permitir la resistencia a ataques. El número de bits necesarios para generar las subclaves depende del número de rondas que se apliquen al algoritmo, determinado por la ecuación 2.

No. De Bits Subclave= $4*N_k * N_b * (N_r + 1)$ □ 32 * 4 * (10 + 1) = 1408 bits (**2**)

Los bytes que conforman las subclaves para cada ronda se derivan de la clave principal, el ejemplo se puede describir como un arreglo lineal mostrado en la figura 4.

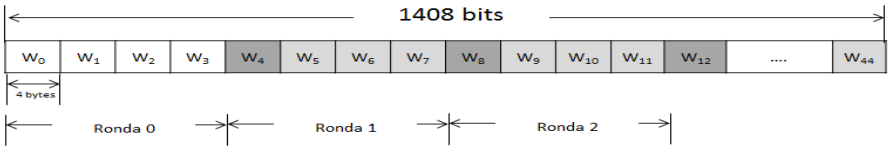

Figura 4. Expansión de Claves

El proceso de expansión de claves se realiza siguiendo el algoritmo mostrado en la figura 5.

```
Key Expansion (byte  key[4*Nk],  word w[Nb * (Nr +1)], Nk)
begin
  word  temp
  i = 0
  while (i < Nk)
        w[i] = word(key[4*i], key[4*i+1], key key[4*i+2], key[4*i+3])
        i = i + 1
  end while
  i = Nk
  while  (i < Nb * (Nr + 1))
        temp = w[i - 1]
        if ( i mod Nk =0)
            temp = SubWord(RotWord(temp)) XOR Rcon[i/ Nk]
        else if (Nk > 6 and i mod Nk  = 4)
            temp = SubWord(temp)
        end if
        w[i] = w[ i - Nk ] XOR temp
  end while
end
```

Figura 5. Pseudocódigo Expansión de Claves

Una vez generadas las claves de expansión se procede a realizar la secuencia de las funciones ShiftRow, SubByte, MixColumn y AddRoundKey en el orden establecido por el estándar dando como resultado el cifrado del mensaje original. El proceso de descifrado, consiste en sustituir las transformaciones utilizadas en el cifrado por las inversas de sus operaciones: InvShiftRows, InvSubBytes e InvMixColumns e invertir el orden de aplicación de dichas transformaciones.

4 Resultados

El desarrollo se realizó utilizando C# de la suite Visual Studio 2013 a través del proceso en la figura 6, el proceso inicia con la entrada del texto a cifrar acomodándolo en una matriz de texto de 4 x 4 y así mismo se genera la expansión de claves a trabajar en cada estado del algoritmo, una vez realizada la expansión de llaves se realiza una transformación inicial AddRoundKey con el bloque de entrada y la clave de cifrado inicial.

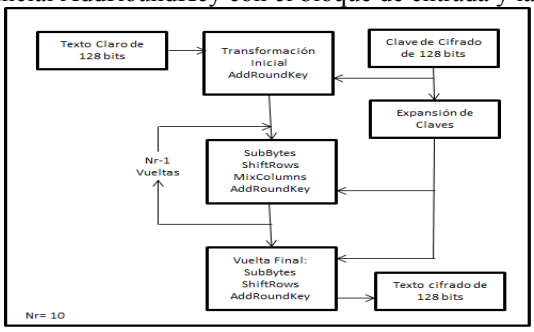

Figura 6. Esquema de cifrado AES

La función AddRounKey realiza una operación XOR entre el bloque del mensaje y la llave inicial, en la función SubByte se realiza una transformación lineal sustituyendo el valor tratado por el correspondiente en la caja S-Box, en ShifRows, se realizan los corrimientos correspondientes a la izquierda, en MixColumns cada columna se multiplica por el polinomio constante y por último se realiza nuevamente AddRoundKey pero en

lugar de la llave inicial se usa la subllave correspondiente a la iteración realizada; dando como resultado el cifrado del mensaje en un bloque de 128 bits. Obteniendo como resultado los datos de cada ronda representados en la figura 7.

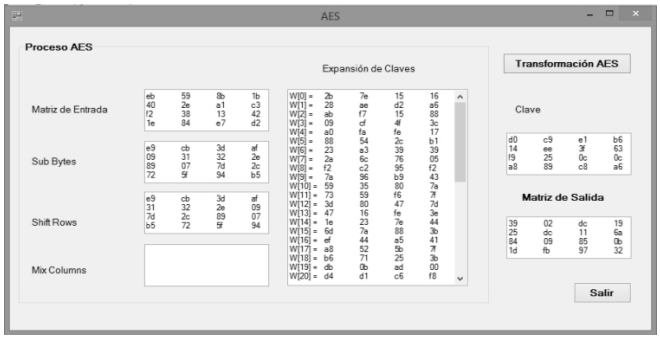

Figura 7. Proceso de cifrado AES

Realizado el proceso de cifrado, se procede a realizar el proceso de descifrado (Figura 8), observando que el resultado obtenido es idéntico a la matriz de entrada que se proporcionó.

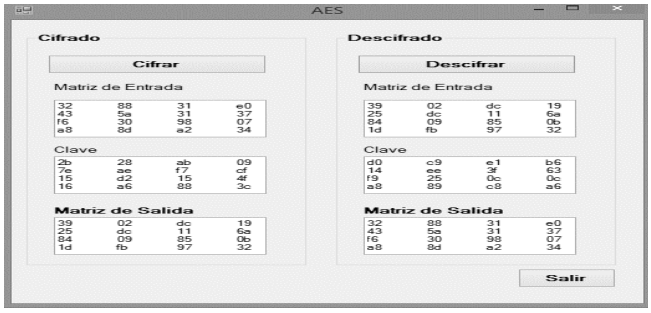

Figura 8. Proceso de cifrado y descifrado AES

Dado que el bloque a trabajar es de 128 bits, el mensaje y la clave pueden variar entre 1 y 16 caracteres, se debe considerar el llenado de las matrices a trabajar en el proceso, en caso de que no se lograra la longitud máxima, los lugares restantes serán llenados por ceros, garantizando el tamaño de una matriz de 4 x 4.

Las pruebas se realizaron sobre diferentes datos con la finalidad de comprobar el funcionamiento y la relación con los resultados del diseño (Figura 9).

a) Clave correcta

b) Clave Incorrecta

Figura 9. Resultado de cifrado y descifrado AES

5 Conclusiones y Trabajos Futuros

La utilización de métodos formales ayuda a lograr especificaciones correctas en pocos pasos, manteniendo los requerimientos desde principio hasta el fin. La particularidad de AES se basa en la fuerza de las claves utilizadas dado que el tiempo requerido para revisar todas las llaves posibles para una longitud de 128

bits es de 5 x 10^{21} años, no importando que la metodología utilizada sea conocida, ya que si no se usa la clave correcta, el descifrado no tendrá éxito. Las aplicaciones que incluyen cifrado AES son seguras, el proceso es rápido y compacto sin embargo el problema radica en que tanto emisor como receptor utilizan la misma clave y en el momento de ser comunicada se corre el riesgo de ser interceptada, por lo que se requiere de una administración compleja de claves. Otro factor vulnerable en el humano, considerado como el eslabón más débil dentro de un esquema de seguridad y se debe en gran medida a la falta de capacitación en el uso de tecnología y cultura de seguridad

La aplicación desarrollada satisface los requerimientos más importantes de la seguridad sin embargo surge la consideración de trabajos que se pueden llevar a cabo y robustecer la seguridad al implementar: AES con manejo de bloques de 256 bits, permutación variable, cambiar el complemento de llenado de las matrices a trabajar y sustituir los ceros con otros valores manejando números trascendentes o bien los valores de la caja S-Box, implementar el cifrado asimétrico para el intercambio de claves y acelerar el cómputo a través de procesamiento paralelo mecanismos que pueden ser implementados en los sistemas a fin de lograr comunicaciones seguras a través de la criptografía basada en estándares probados.

Referencias

[1] Open Web Application Security Project, «Open Web Application Security Project,» Powered By MeiaWiki, 2017 Enero 23. [En línea]. Available: https://www.owasp.org/index.php/Threat_Risk_Modeling#Identify_Security_Objectives. [Último acceso: 23 06 2017].

[2] Security Standards Council (PCI), «Norma de seguridad de datos(DSS) de la industria de tarjetas de pago (PCI) y normas de seguridad de datos para las aplicaciones de pago (PA-DSS),» Enero 2014. [En línea]. Available: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3_Glossary_ES-LA.pdf. [Último acceso: 20 Junio 2017].

[3] Symantec, «Protect the Entire Online User Experience with Always On SSL,» Symantec Enterprise, 28 Febrero 2011. [En línea]. Available: http://www.symantec.com/page.jsp?id=always-on-ssl#. [Último acceso: 26 Febrero 2016].

[4] S. Lu y S. A. Smolka, «Model checking the secure electronic transaction (SET) protocol,» de In Mdeling, Analisys and Simulation of Computer and Telecommunication Systems, 1999.

[5] S. T. Kent, Internet Privacy Enhanced Mail, New York, USA: ACM Press/Addison-Wesley Publishing Co., 1998, pp. 295-318.

[6] EcuRed, «EcuRed Conocimiento con todos y para todos,» Junio 2006. [En línea]. Available: https://www.ecured.cu/Cifrado. [Último acceso: 27 Junio 2017].

[7] E. Barker y Q. Dang, «NIST Special Publications 800-57 Part 1,2 y3,» National Institute of Standards and Technology (NIST), January 2015. [En línea]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf. [Último acceso: 20 Marzo 2015].

[8] National Institute of Standards and Technology (NIST), «Advanced Encryption Standard (AES) FIPS PUB-197,» 26 Noviembre 2001. [En línea]. Available: https://doi.org/10.6028/NIST.FIPS.197 . [Último acceso: 28 Junio 2017].