Instituto Politécnico Nacional

Escuela Superior de Cómputo

Cryptography

Homework 3

Santiago Mancera Arturo Samuel

Sánchez José Erick

Carlos Eduardo Caballero Huesca

Brando Josué Martínez García

Grupo: 3CV1

Profesora: Díaz Santiago Sandra

14 de septiembre del 2016

1.-

Preguntas.

a) Which are the most important block ciphers till now? Who design each of them and when?
- ✓ 1971, when a team leaded by H. Feistel and his colleagues at IBM designed a family of ciphers known as Lucifer.
- ✓ The strongest variant which was released in 1973, operated on 128-bit blocks and 128-bit secret keys.
- ✓ A revised version of that Lucifer variant, known as the Data Encryption Standard (DES), was adopted as a US FIPS standard in 1974
- ✓ Some other examples of famous block ciphers include IDEA, AES, RC6

b) According to the paper, what is the definition of block cipher?
- ✓ Block ciphers are one of the most important primitives in cryptology. They are based on well-understoodmathematical and cryptographic principles. Due to their inherent efficiency, these ciphers are used in many kinds of applications which require bulk encryption at high speed.

c) What is a round? How many rounds does DES have ? How many rounds does AES have?
- ✓ Typically, the number of rounds in modern ciphers ranges from 10 up to 32.
- ✓ Each round transformation is composed of a sequence of four transformations, namely: Byte Substitution (BS), ShiftRows (SR), MixColumns (MC) and AddRoundKey (ARK).
- ✓ AES rounds 1 to 9, were implemented using two main building blocks.

d) What is the definition of mode of operation?
- ✓ A mode of operation is a specific way to use a block cipher for encrypting arbitrarily long messages. We now discuss some of the traditionalmodes of operations which have been in use for long.

e) Describe each mode of operation: ECB, CBC, OFB, CFB and counter mode (CTR)?
- ✓ Electronic Code Book Mode.This is probably the simplest of all modes. In the Electronic Codebook (ECB) mode the plaintext P is segmented as P = P1||P2|| . . . ||Pm, where each Pi is n-bit long block. Thereafter, the encryption function EK is applied separately on each Pi.
- ✓ Cipher Block Chaining Mode. The output of one block cipher is fed into the other block cipher along with the next blockmessage.
- ✓ Cipher Feedback Mode. In CFB mode also the cipher blocks are chained but the output is produced in a manner much different from that of CBC. For each block, the cipher produced is just xor-ed with the message.
- ✓ Output Feedback Mode. In this mode the IV is repeatedly encrypted to get a stream of random bytes.Unlike the other modes described before in OFB no part of the plaintext is ever given as an input to the blockcipher.
- ✓ Counter Mode. The counter (CTR) mode is a bit different from the other modes defined above. It takes in an IV , and in each iteration the value of the IV incremented

by one gets encrypted. The ciphertext is produced by xor-ing the encryption results with the plaintext blocks.

f) What is the problem if use ECB?

- ✓ The ECB mode is not suitable for encrypting bulk messages as it can reveal much information about a message.
- ✓ This is because in ECB, every block is encrypted using the same key and so all equal plaintext blocks gets encrypted into equal ciphertext blocks

h) What is the main purpose of authenticated encryption?

- ✓ A tag can be considered as a checksum of the message that was used to generate the ciphertext. A sender after decrypting the ciphertext can always compute the tag and match the tag which she computed using the decrypted message with the tag that she received. If the tags do not match the receiver can know that a tampering of the ciphertext has taken place during the transit.

2.-

Cifrado Lucifer

Fue desarrollado en la década de los sesenta por un grupo científicos encabezado por Horst Feistel en los laboratorios de investigación de IBM. Pertenece a la clase de cifrados Feistel, de cifrado por bloques. [1]

El cifrado Lucifer utiliza una llave de 128 bit y bloques del mismo tamaño. Por lo tanto, para procesar los bloques de llaves y textos, éstos son divididos en 16 bytes y son procesados en 16 rondas o iteraciones. [2]

En cada ronda, los 8 bytes de la mitad derecha de un bloque (64 bits) son procesados independientemente de los otros bytes. No obstante, cada ronda consiste en una sustitución y una permutación. La sustitución se da al dividir cada bloque de 8 bits en 4 bits. A cada uno de estos 4 bits se le aplica una transformación de sustitución dada por *S-boxes*, (tablas de sustitución). El resultado se somete a una operación XOR con los bits de la llave. [2]

La permutación se aplica inmediatamente después en cada bit, para después llevar a cabo otra operación XOR entre el resultado y los 8 bytes izquierdos. Por último, el bloque de 64 bits se rota, pasando a ser los bytes del lado izquierdo los del lado derecho repitiéndose toda la operación. [2]

Al contar con una llave de 128 bits, se puede considerar que existen 2^128 soluciones, esto es 34 seguido de 37 ceros. Si se pudiera comprobar un trillón de soluciones por segundo tomaría 1.08 x 10^19 años; mucho más tiempo que la existencia del universo. [3]

En 1973 la Oficina Nacional de Estándares (NBS) de los Estados Unidos convocó a las empresas a presentar candidatos de algoritmos de cifrado que serían adoptados por el gobierno para el

almacenamiento y transmisión de información. IBM presentó una variante del cifrado Lucifer, el cual después de largas pruebas por parte de la NSA (*National Security Agency*), fue adoptado como DES (*Data Encryption Standard*). [1]

Diferencias entre el cifrado Lucifer y cifrado DES

- El cifrado Lucifer cuenta con dos *S-boxes* mientras que el cifrado DES cuenta con 8. [1]
- El cifrado Lucifer utiliza bloques y llaves de 128 bits, mientras que el cifrado DES utiliza llaves de 56 bits y bloques de 64 bits. [1]

Horst Feistel

El doctor Horst Feistel nació en Alemania en 1915 y emigró a los Estados Unidos en 1934. Fue investigado en este país por posible espionaje en 1941 durante la segunda guerra mundial. Por ello, mantuvo un interés reservado en la criptografía. No fue sino hasta después de la guerra cuando comenzó a trabajar en la Fuerza Aérea de los Estados Unidos desarrollando nuevos cifrados. [4]

No obstante, la Agencia Nacional de Seguridad (NSA) se oponía a que la Fuerza Aérea realizará investigación de forma independiente, por lo cual Feistel tuvo que ceder sus investigaciones. [4]

En 1960, comenzó a trabajar en *Mitre Corporation*, pero nuevamente la NSA intervino para detener su trabajo. Finalmente, ingresó a IBM, lo cual le permitió continuar sus investigaciones a costa de la NSA. [4]

Desarrolló el cifrado Lucifer en la década de los setenta y no tuvo mayores proyectos posteriormente. Murió en el año 1990. [4]

3.-

Redes de Feistel

Horst Fiestel de los primeros investigadores no militares en el campo de la criptografía y puede ser considerado el padre de la criptografía. Nació en Berlín en 1915.

En 1973 publicó en una revista un artículo llamado “Criptografía y privacidad en la informática”, en la que trato el tema de la máquina de cifrado y la conocida red de Feistel. [1]

La red Feistel se convirtió en la base del Estándar de Cifrado de Datos (DES).

Muchos de los cifrados de producto tienen en común que dividen un bloque de longitud n en dos mitades, L y R. Se define entonces un cifrado de producto iterativo en el que la salida de cada ronda se usa como entrada para la siguiente según la relación. [2]

A este tipo de estructura se le llama red de Feistel en la cual se basa algoritmos como el DES, Lucifer, Blowfish, CAST

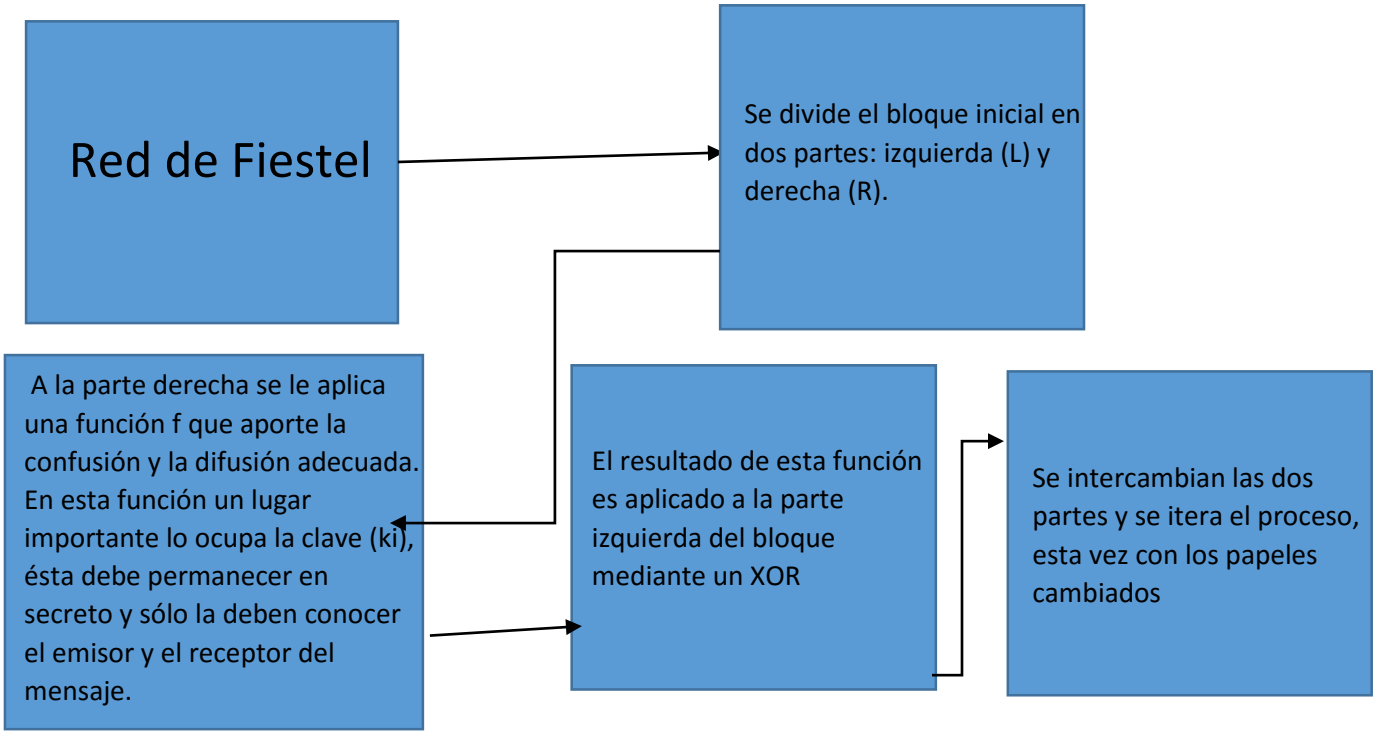
La propuesta de Feistel propuso alterna sustituciones y permutaciones, es una aplicación práctica de una propuesta de Claude Shannon en 1945 para desarrollar un cifrado producto que alterna funciones de confusión y difusión.

La seguridad depende de secreto de la clave, no del algoritmo por lo que:

Opera sobre un bloque de texto plano de n bits para producir un texto cifrado de n bits. Típicamente, la longitud de un bloque es de 64 bits.

Pueden adaptarse para funcionar como cifradores de flujo (más generales y mayor aplicabilidad)

Para que sea reversible (descifrado), cada entrada debe producir un bloque de texto cifrado único. [3]



Bibliografía

[1] Sabrina Schanhart, S. (2016). The Feistel Network. [En línea]. Disponible en : http://cs-exhibitions.uni-klu.ac.at/index.php?id=261 [Visitado el 15 Sep. 2016].

[2] Serdis.dis.ulpgc.es. (2016). Red de Feistel. [En línea] Disponible en: http://serdis.dis.ulpgc.es/~ii-cript/FICHEROS%20WEB/criptografia%20moderna/redes%20Feistel_files/voila_data_002/voila_data_002/voila_002.htm [Visitado 15 Sep. 2016].

[3] Acuayte, L.(2012). Cifrado Feistel. [En línea] Cifradofeistel.blogspot.mx. Disponible en: http://cifradofeistel.blogspot.mx/ [Visitado 15 Sep. 2016].

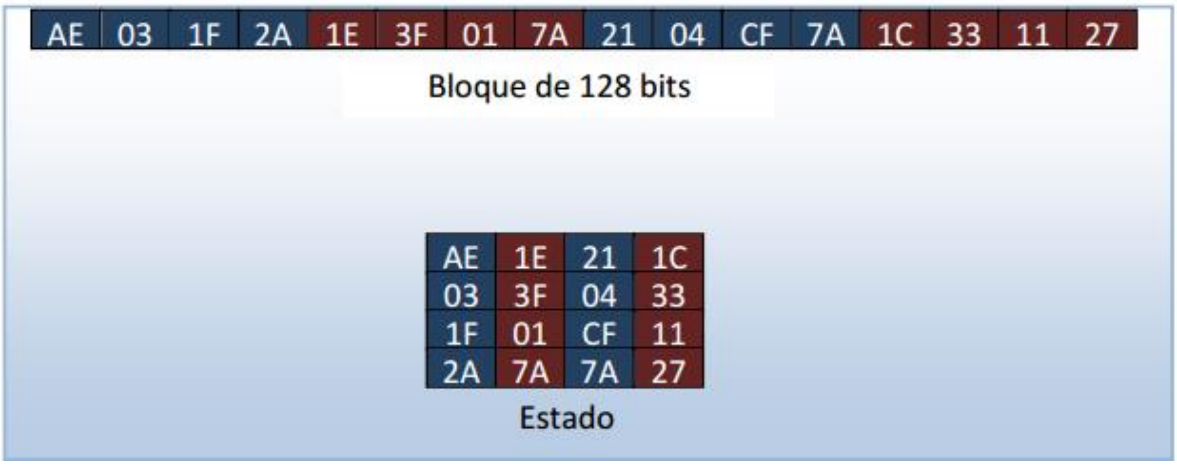
4.-

Características del cifrado AES (Advanced Encryption Standard)

AES toma como elemento básico al byte (8 bits) y ve a los bytes como elementos del campo finito de Galois o GF (2^8), toda operación del algoritmo está basada en operaciones sobre este campo finito, rotaciones de bytes y operaciones de suma módulo 2.

-Tamaños de bloque (Block Size)

AES es un algoritmo de cifrado por bloques, **inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits**, por lo tanto los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se lo pude ver como un bloque o matriz de 4x4 bytes al que se le llama estado, este se organiza de la siguiente forma:

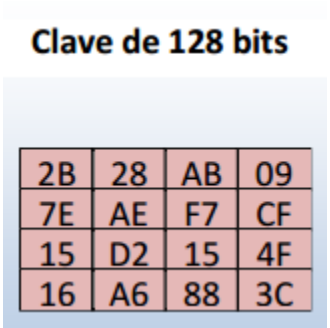


-Tamaño de la clave (Key Size)

Por ser simétrico, se utiliza la misma clave para cifrar como para descifrar, **la longitud de la clave puede ser de 128, 192 o 256 bits según especifica el estándar**, esto permite tres implementaciones conocidas como AES-128, AES-192 y AES-256.

Partiendo de una clave inicial de 16 bytes (128 bits), que también se puede ver como un bloque o matriz de 4x4 bytes, se generan 10 claves, estas resultantes junto con la *clave inicial* son denominadas *subclaves*.

El proceso de generación de subclaves parte de la clave inicial vista como una matriz de 4x4 bytes:



Para mostrar claramente cómo se calculan las subclaves, el conjunto de subclaves puede verse como una matriz de 4 filas x 44 columnas, o sea una subclave a continuación de otra.

-Numero de Rondas (Number of rounds)

El proceso de cifrado del algoritmo consiste en aplicar a cada estado un conjunto de operaciones agrupadas en lo que se denominan rondas, el algoritmo realiza 11 rondas, donde en cada ronda se aplica una subclave diferente.

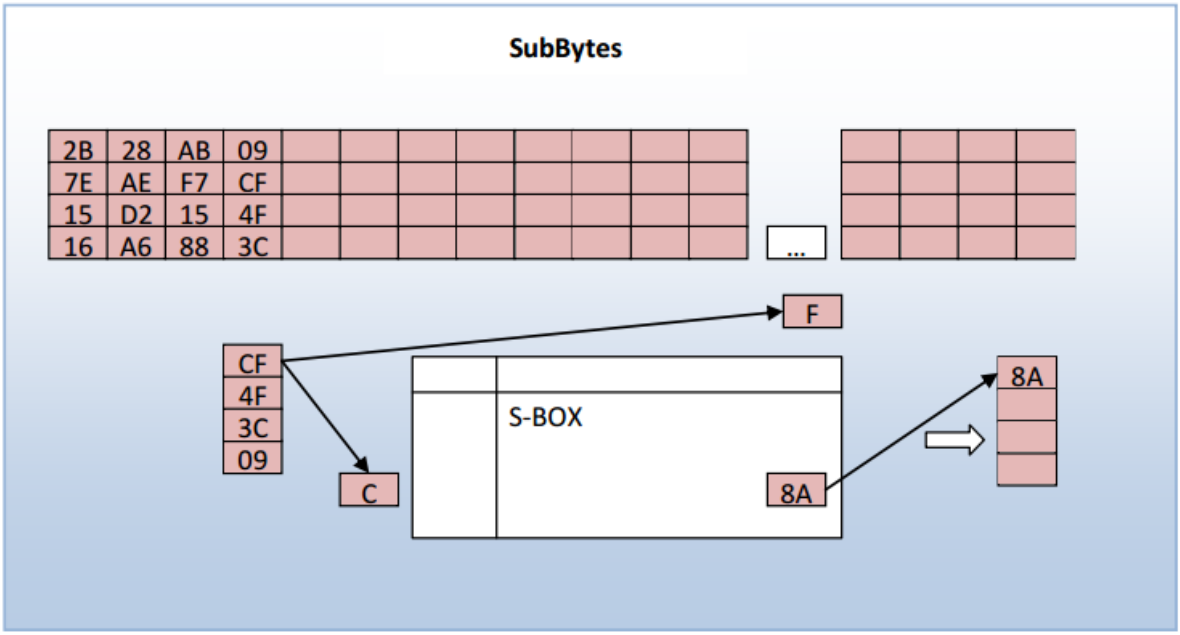
Las 11 rondas se pueden clasificar en 3 tipos:

- 1 ronda inicial (se aplica la subclave inicial).
- 9 rondas estándar (se aplican las 9 subclaves siguientes, una en cada ronda).
- 1 ronda final (se aplica la última subclave).

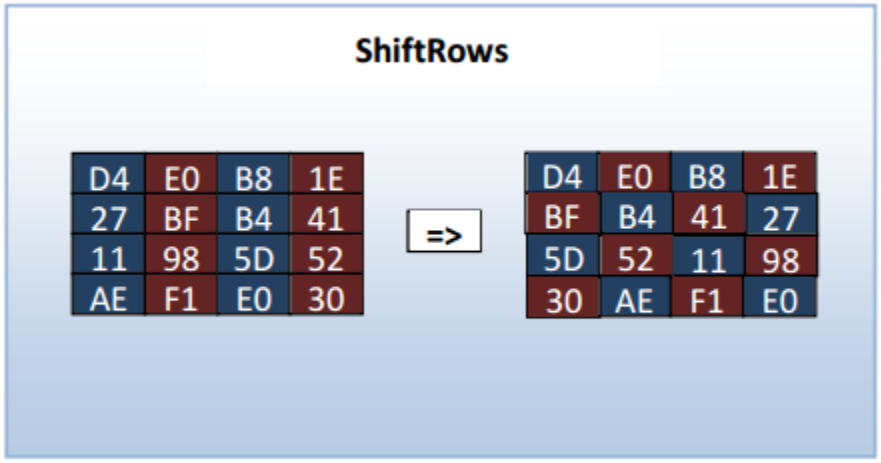
-Operaciones principales (Main operations)

Las operaciones que realiza el algoritmo dentro de las rondas se reducen a 4 operaciones básicas:

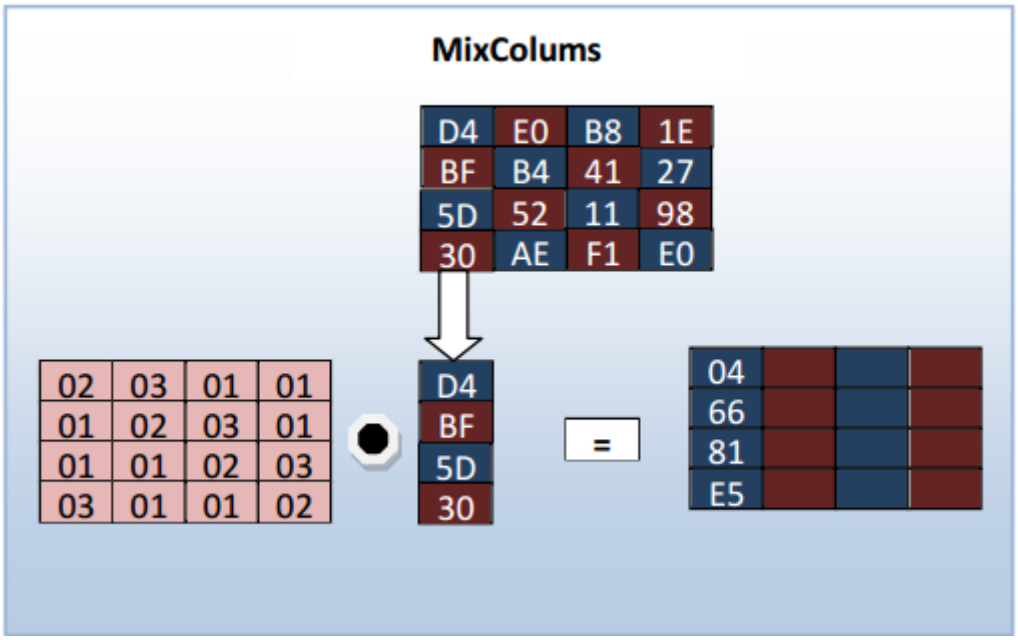
- **SubBytes** – Consiste en reemplazar cada byte de la columna ya rotada por un byte almacenado en una tabla llamada S-Box, esta tabla contiene pre calculados el resultado de aplicarle a cada byte la inversión en el campo GF y una transformación afín, la dimensión de la tabla es de 16x16 bytes donde los índices tanto de las columnas como de las filas van de 0 a F, para obtener la transformación S-Box de un byte se toman los primeros 4 bits como el índice de la fila de la tabla y los segundos 4 como índice de la columna de la tabla:



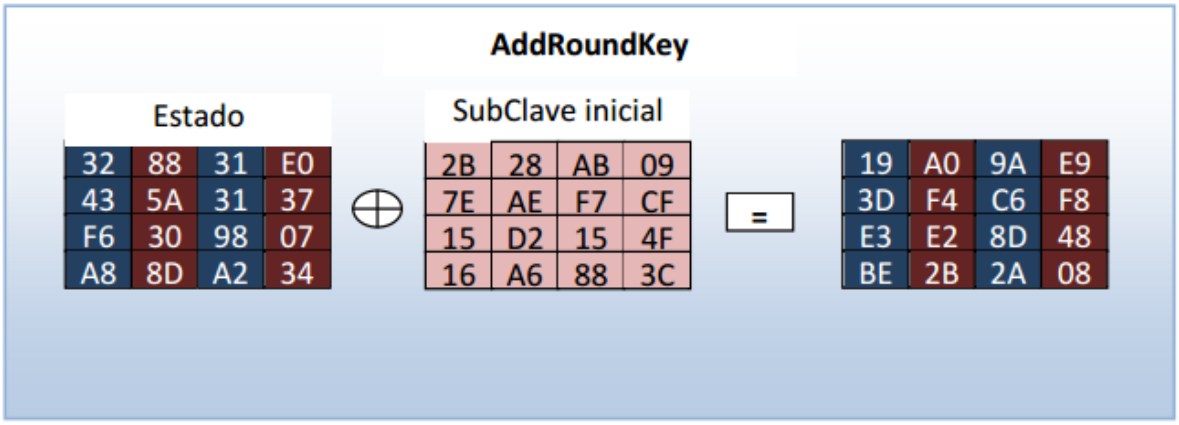
- **ShiftRows** – En cada fila del estado, a excepción de la primera, se rotan circularmente hacia la izquierda los bytes, en la segunda fila se rotan una posición, en la tercera dos posiciones y en la cuarta tres posiciones.



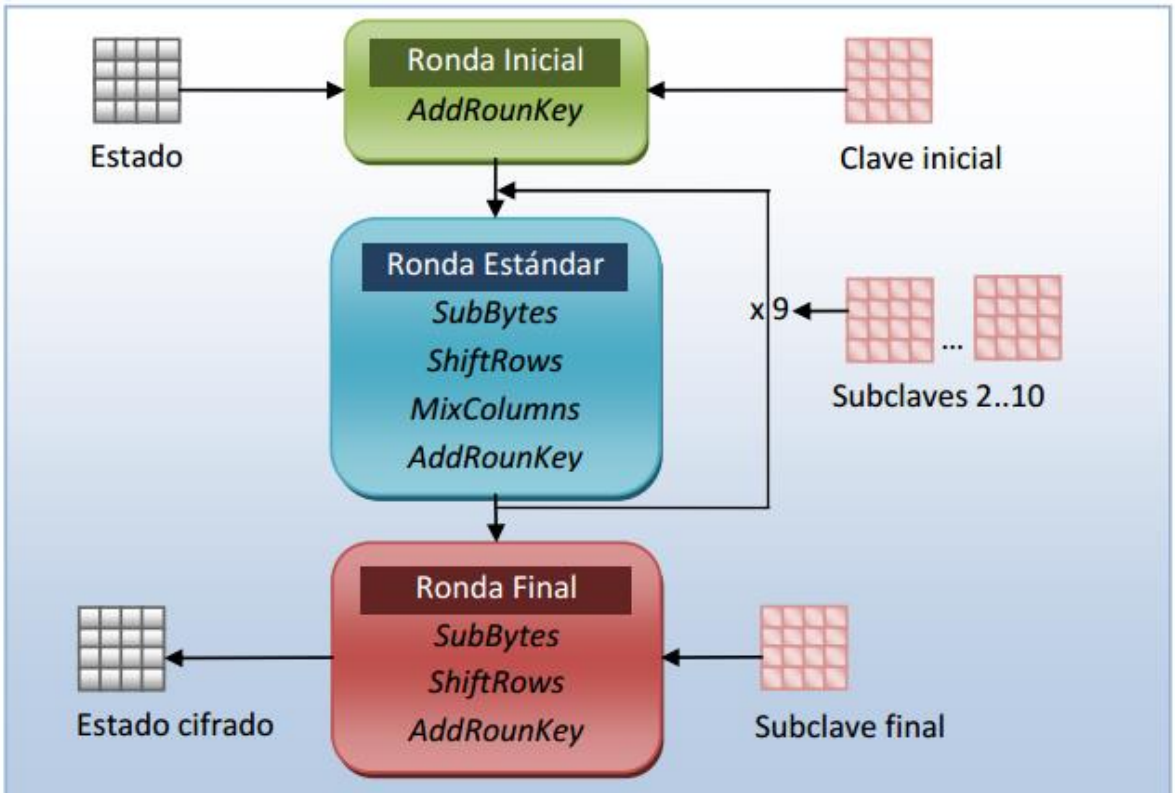
- **MixColumns** – A cada columna del estado se le aplica una transformación lineal, esto es multiplicarlo por una matriz predeterminada en el campo GF.



- **AddRoundKey** – No es más que un XOR byte a byte entre el bloque a cifrar y la clave inicial. Para las rondas estándar se aplica la misma operación pero utilizando otra subclave, y en la ronda final se utiliza la ultima subclave.



A continuación se muestra un diagrama de cómo se aplican las operaciones y claves en cada una de las rondas:



-¿AES utiliza una estructura Feistel?

En la estructura clásica de Feistel, la mitad del bloque de datos se usaba para modificar la otra mitad, y entonces se intercambiaban entre sí. El AES procesa todo el bloque de datos en paralelo durante cada etapa, realizando sustituciones y permutaciones.

Bibliografía

[1] S. Bosworth, M. Kabay y E. Whyne, Computer Security Handbook, Ney Jersey: Wiley, 2009.

[2] P. Klaus, «Johannes Gutenberg-Universität Mainz,» 20 Marzo 2000. [En línea]. Available: https://www.staff.uni-mainz.de/pommeren/Cryptology/Bitblock/2_Feistel/Lucifer.pdf. [Último acceso: 14 Septiembre 2016].

[3] R. F. Graf y W. Sheets, Video Scrambling & Descrambling for Satellite & Cable TV, Estados Unidos: Newnes, 1998.

[4] S. David, Coding for Data and Computer Comunications, Nueva York: Springer, 2005.