

**Encriptación AES**

**Asignatura:** Programación III

**Docente:** Ing. Oscar Gutiérrez Rivera.

**Integrantes:**

Hernández Reyes, Marvin Ernesto HR100616

Ramírez Cerón, Carlos Fabricio RC100617

Sigüenza Figueroa, José Miguel SF100317

**Fecha de entrega:** 13 de marzo de 2019

**Contenido**

[**Resumen** 3](#_Toc3356403)

[**Introducción** 4](#_Toc3356404)

[**Objetivos** 5](#_Toc3356405)

[**Generales** 5](#_Toc3356406)

[**Específicos** 5](#_Toc3356407)

[**Alcances** 6](#_Toc3356408)

[**Limitaciones** 6](#_Toc3356409)

[**Marco Teórico** 8](#_Toc3356410)

[**Historia** 8](#_Toc3356411)

[**Descripción** 8](#_Toc3356412)

[**Cifrado** 9](#_Toc3356413)

[**Descifrado** 12](#_Toc3356414)

[**Producto de Software** 16](#_Toc3356415)

[**Conclusiones** 17](#_Toc3356416)

[**Referencias** 18](#_Toc3356417)

[Bibliografía. 19](#_Toc3356418)

# **Resumen**

La criptografía, se utiliza desde hace un par de décadas atrás, cuando su uso era exclusivo militar, pero gracias a la inmensa evolución que le mundo informático ha tenido podemos encontrar algoritmos de encriptación en aplicaciones como banca electrónica, comunicación inalámbrica, telefonía, mensajería digital y cualquier aplicativo que requiera ocultar información de mucha importancia. Es por eso que hoy en día su implementación es bastante común y siempre se busca obtener la mayor confiablidad e integridad. Actual entente, existe diversos algoritmos de encriptación, aunque muchos de ellos son vulnerables por no tener una implementación segura.

En el presente proyecto empleamos el algoritmo AES(Advanced Encryption Standard), controles de Java swings, las librerías de BufferedReader and Bufferedwriter con nuestros conocimientos básicos de programación orientada a objetos.

Como resultado implementamos AES en un aplicativo que sea capaz de encriptar texto, desde frases pequeñas como “Hola mundo” hasta párrafos completos, mostrando una interfaz gráfica innovadora y amigable. Además, se logró agregar una función extra que se trata de encriptación de archivos textos (“.txt”), utilizando la clase FileChooser se le dio la ahabilidad al aplicativo de seleccionar el archivo a encriptar/desencriptar y poder guardarlo con el nombre y dirección desead.

# **Introducción**

Advance Encryption Standard, es un algoritmo de encriptación utilizado para cifrar datos y protegerlos contra cualquier acceso no autorizado, este utiliza una clave de longitud variada y se denomina según su longitud de clave usada AES-128. AES-192 y AES-256.

Es un método de encriptación muy eficiente y es bastante común verlo en las claves de wifi tipo de conexión WPA2, además para protección de VOIP, algo que se debe destacar de este es que es de licencia libre además utiliza pocos recursos del hardware y almacenamiento.

En el presente proyecto se implementará la encriptación AES -256, desde un modo simple como frases, o pequeños párrafos utilizando controles de texto para capturar la información en nuestra interfaz, hasta uno avanzado que consiste en encriptar archivos de texto en formato (.txt). De igual manera se ha implementado el desencriptado de estos, utilizando una llave simétrica para proteger el contenido en el texto y así esta encriptación pueda ser segura y confiable.

# **Objetivos**

## **Generales**

* Adquirir los conocimientos necesarios sobre el funcionamiento del algoritmo AES para la implementación de un programa utilizando dicho algoritmo.

## **Específicos**

* Implementar el algoritmo AES haciendo uso el lenguaje de programacion de JAVA y el IDE de NetBeans.
* Mostrar el funcionamiento de encriptacion y descriptacion del programa realizado con el algoritmo de AES.

# **Alcances**

* Mostrar información relevante y acertada de la encrpitacion y desencriptación de la investigación realizada acerca del algoritmo AES (Advanced Encryption Standard).
* Creación de un aplicativo capaz de encriptar texto a través de una interfaz gráfica, utilizando los conocimientos del algoritmo AES adquiridos en la investigación y previos conocimientos básicos de programación en JAVA
* Implementación de una función extra que nos permite encriptar archivos de texto en formato (.txt), utilizando conocimientos adquiridos en investigaciones extras realizadas para mejorar el uso de interfaz grafica con JAVA
* Implementación de un Login con usuarios predefinidos y contraseñas encriptadas utilizando previos conocimientos adquiridos durante investigación sobre AES.

# **Limitaciones**

* Dificultades al momento de recopilar la información, y asimismo que fuera de facil entendimiento a los integrantes del grupo.
* Dificultades a la hora de reunirnos como grupo, debido a que nuestros horarios de clases y de trabajo nos impedían movilizarnos para estar como grupo debatiendo lo que iria en el codigo del programa.

# **Marco Teórico**

## **Historia**

AES es una Norma Federal de Proceso de Información (FIPS), es un cifrado de bloques simétricos. Esto significa que se utiliza la misma clave para el cifrado y descifrado.

En 1997 el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) dio una nueva denominación al criptosistema Rijndael, después de un concurso, nombrándolo como AES. Dicho algoritmo es muy seguro en el cifrado de datos, sin embargo, en la actualidad se usa para encriptar imágenes.

En un principio AES tenía que cumplir con requerimientos mínimos como son:

* Ser público
* Bloques simétricos
* Sus longitudes de los bloques tenían que ser al menos de 128 bits.
* Su implementación tenía que ser mediante hardware y software.
* Consta de una longitud de llaves de 128,192 y 256 bits.

Al cumplir con estos requisitos pasa a una segunda fase en la cual se calificó lo siguiente: seguridad, simplicidad y flexibilidad.

## **Descripción**

AES tiene un tamaño de bloques fijos de 128, 192 o 256 bits con diferencia de Rijndael en el que sus bloques son múltiplos de 32 bits. AES opera una matriz de 4 X 4 Para encriptar implementa de 10, 12 o 14 rondas dependiendo la longitud de la llave. Utilizando dos algoritmos uno para mezclar la información y el otro desarrolla un programa de llaves. El cual trabaja solo con ASCII de 256.

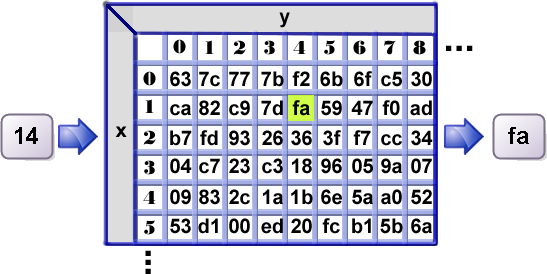


El algoritmo comienza en la primera ronda con un XOR seguida de 9 rondas de cuatro etapas y la décima ronda de tres etapas. Esto se aplica tanto para el cifrado y descifrado con la excepción de que cada etapa de una ronda del algoritmo de descifrado es la inversa de la que es contraparte en el algoritmo de cifrado.

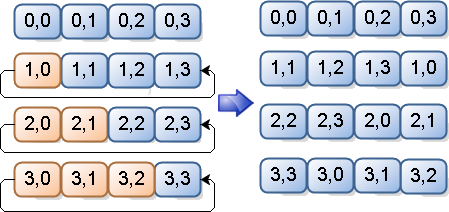
## **Cifrado**

Para realizar el cifrado se necesitan realizar las siguientes cuatro etapas:

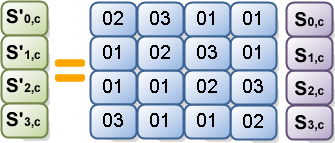
**SubByte**: Se realiza una sustitución no lineal donde cada byte es reemplazado a través de la caja correspondiente como se muestra en la Tabla.



**ShiftRows:** Se realiza una transposición donde la fila de estado es rotada de manera cíclica, un número determinado de veces.



**MixColumns:** Se realiza un mezclado de columnas de los estados combinados con los cuatro bytes en cada columna usando una transformación lineal



Es decir:

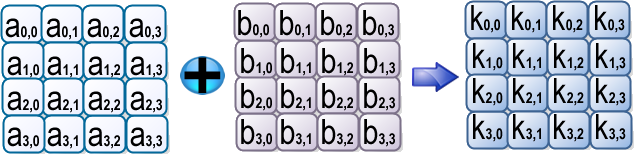
S ı00= {02} • S00 ⊕ {03} • S10 ⊕ {01} • S20 ⊕ {01}S30

S ı01= {01} • S00 ⊕ {02} • S10 ⊕ {03} • S20 ⊕ {01}S30

S ı02= {01} • S00 ⊕ {01} • S10 ⊕ {02} • S20 ⊕ {03}S30

S ı03= {03} • S00 ⊕ {01} • S10 ⊕ {01} • S20 ⊕ {02}S30

**AddRoundKey:** Cada byte es combinado con la clave.

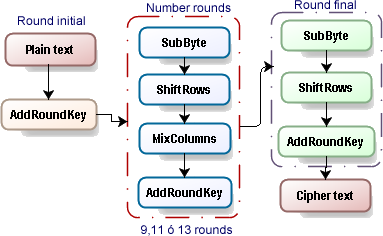


K0,0 = a0,0 ⊕ b0,0

K1,0 = a1,0 ⊕ b1,0

K2,0 = a2,0 ⊕ b2,0

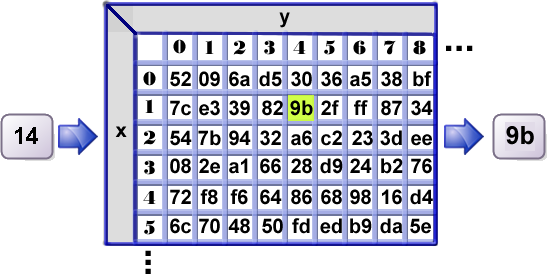
Estructura del algoritmo AES para el cifrado



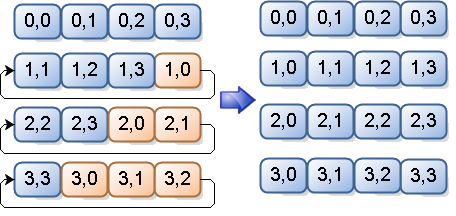
## **Descifrado**

La décima ronda, simplemente deja de lado la etapa MixColumns. Las primeras nueve rondas del algoritmo de descifrado consisten de los siguientes puntos:

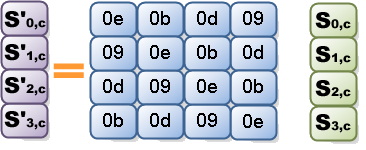
**Inverse SubBytes:**



**Inverse ShiftRows:**



**Inverse MixColumns:**



Es decir:

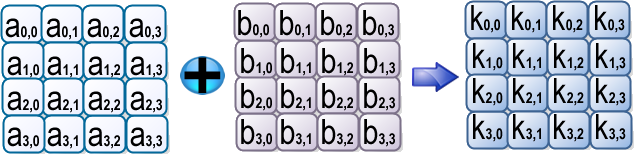
S ı00= {0e} • S00 ⊕ {0b} • S10 ⊕ {0d } • S20 ⊕ {09}S30

S ı01= {09} • S00 ⊕ {0e} • S10 ⊕ {0b} • S20 ⊕ {0d }S30

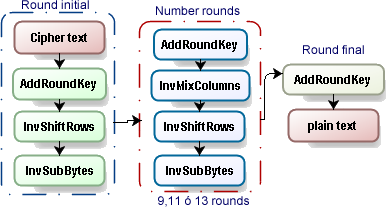
S ı02= {0d } • S00 ⊕ {09} • S10 ⊕ {0e} • S20 ⊕ {0b}S30

S ı03= {0b} • S00 ⊕ {0d } • S10 ⊕ {09} • S20 ⊕ {0e}S30

**Inverse AddRoundsKey**

En cuestión de ataques todavía no es vulnerable ya que en estudios anteriores los ataques han llegado a la segunda ronda en cuestión de software.

Estructura del algoritmo AES para el descifrado



# **Producto de Software**

# **Conclusiones**

Según la información encontrada la encriptación es algo muy importante en siglo XXI debido a que toda casi toda la información esta en la red, gobiernos y empresas muchas veces tienen cierta información sensitiva que necesita ser protegida para que esta no caiga en manos equivocadas. El cifrado AES nos ayuda a poder mantener segura nuestra información y a la vez poder confiar en las tecnologías de la información. Se recomienda utilizar el algoritmo especialmente si se trabaja con base de datos ya que este puede ayudar a proteger contraseñas de una manera muy eficiente además información sensible que no puede ser develada a quien no sea propietario de ella ya que es muy complicado de descifrar.

# **Referencias**

Rouse, M. (2019). What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard [Accessed 13 Mar. 2019].