UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Criptografía

Tarea 02 - Investigación - AES.

PROFESORA:

Dra. Rocio Alejandra Aldeco Pérez

Alumno	No. Cuenta	Grupo teoría
Becerril Olivar Axel Daniel	317113888	3

FECHA DE ENTREGA: 06/03/2025

ÍNDICE

Desarrollo

Investiga cómo funciona el algoritmo AES particularmente enfócate en:

Qué tipo de algoritmo es

El algoritmo AES (Advanced Encryption Standard) es un algoritmo de cifrado simétrico por bloques el cual se ha adoptado como estándar desde el año 2002.

Qué longitudes de llave acepta

Admite 3 diferentes longitudes de llave las cuales son;

Longitud AES	Descripción
128	Permite 10 rondas de cifrado con 3,4 x 1038 combinaciones.
192	Permite 12 rondas de cifrado con 6,2 x 1057 combinaciones.
256	Permite 14 rondas de cifrado con 1,1 x 1077 combinaciones.

Cuantas etapas tiene y cuales son sus nombres

Tiene 6 etapas.

1. División y expansión
2. Sustitución
3. Desplazamiento
4. Mezcla
5. Round Key
6. Repetir

Cuantas rondas ejecuta

Longitud AES	# Rondas
128	10 rondas de cifrado
192	12 rondas de cifrado
256	14 rondas de cifrado

¿Existen ataques a este algoritmo? ¿Cuales?

- Ataques de Fuerza Bruta: Intentar cada clave posible hasta encontrar la correcta.
- Criptoanálisis Diferencial: Intentar analizar diferencias en el texto plano.
- XSL: Este ataque es considerado especulativo y poco práctico en la actualidad.
- Ataques de Canal Lateral: Estos ataques no se dirigen al cifrador en sí, sino a sus implementaciones.

Referencias

Security, P. (2023, 21 diciembre). *¿Qué es el cifrado AES? - Panda Security*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/

Gálvez, R. A. P. J. A. S. (s. f.). *.:: Algoritmo AES (Advanced Encryption Standard) ::.* https://repositorio-uapa.cuaed.unam.mx/repositorio/moodle/pluginfile.php/2184/mod_resource/content/2/contenido-uapa/index.html

Splashtop. (2024, 25 noviembre). *Explicación del cifrado AES: Cómo funciona, beneficios y usos en el mundo real*. https://www.splashtop.com/es/blog/aes-encryption?srsltid=AfmBOopSX1V5kfekFmFuBu9bc6da3P8oOIHpRVqlyd6yFnWj-4fNXtdw