educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 2

Algoritmos de cifrado simétrico

Algoritmos DES y 3DES

DES se basa en el algoritmo ***Lucifer,*** desarrollado por IBM a principios de la década de los ’70.

Fue adoptado como estándar por el gobierno de Estados Unidos, para comunicaciones no cifradas, en 1976.

La NSA lo diseñó para implementarlo por *hardware*, pero la NIST publicó su especificación con tanto detalle que le permitió a cualquier persona implementarlo por *software*.

En 1998 se demostró que por la escasa longitud de su clave permitía un ataque por fuerza bruta.

Dispone de bloques de 64 bits y longitud de clave de 96 bits, ambos muy cortos para ser considerado seguros.

3DES o **Triple DES** consiste en aplicar tres veces DES con 2 o 3 claves diferentes con 80 bits y 112 bits de seguridad respectivamente. **Ambos se consideran obsoletos.**

Algoritmo AES

En 1999, NIST certifica solamente a 3DES como estándar y llama a un concurso mundial para hallar un reemplazo.

En octubre de 2000 se adopta el algoritmo ***Rijmdael*** (Vincent Rijmen y Joan Daemen) como parte del nuevo **Estándar Avanzado de Cifrado (AES).**

Es el algoritmo más popular, rápido y confiable. Utiliza cifrado por bloques de 128 bits.

Existen tres variantes, con claves de 128, 192 y 256 bits (AES-128, AES-192 y AES-256).

Los ataques actuales reducen la fortaleza de la seguridad en 2 bits, a 126, 190 y 254 para AES-128, AES-192 y AES-256 respectivamente.

Muchas CPUs actuales soportan aceleración por *hardware* para AES.

Algoritmo ChaCha20

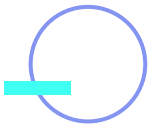
Moderno cifrado por flujo, seguro y rápido. Puede ser usado con claves de 128 bits o de 256 bits.

No se conocen ataques que reduzcan su nivel de seguridad. Es una modificación con rendimiento mejorado de *Salsa20*. Se ha vuelto popular a partir de la adopción por Chrome.

Una desventaja menor es que usa un contador de bloque de solo 32 bits.

Debido a la longitud de su contador de bloque, no se considera seguro para textos claros contiguos de más de 256 GiB.

De usarse con este fin, se debería fraccionar el texto plano en bloques de menos de 256 GiB y resetear el contador de bloque y el *nonce* antes de cifrar cada fracción.



Otros algoritmos

RC4

Es un antiguo cifrado por flujo con claves de 40 bits a 2048 bits. Muy popular en el pasado, por su simplicidad y velocidad. Obsoleto.

CAST5

También conocido como CAST-128. Usado por el gobierno de Canadá. Usa claves de 128 bits. No se conocen ataques (su seguridad se mantiene en 128 bits).

GOST89 o Magma

Antiguo cifrado de la ex URSS. Desarrollado por la KGB en la década del 70, estandarizado en 1989. Aún funcional. Posee claves de 256 bits y nivel de seguridad 178 bits.

GOST2015 o Kuznyechik

Sucesor de Magma. GOST significa *GOvernment STandard*. Usado por Rusia.

CAST5

También conocido como CAST-128. Usado por el gobierno de Canadá. Usa claves de 128 bits. No se conocen ataques (su seguridad se mantiene en 128 bits).

SEED y ARIA

Son cifrados de Corea del Sur. SEED fue desarrollado en 1998 y ARIA en 2003. Ambos cifran por bloques de tamaño de 128 bits. ARIA está basado en AES y soporta las mismas longitudes de clave: 128, 192 y 256 bits. SEED usa claves de 256 bits. No se conocen ataques prácticos contra ellos, y su nivel de seguridad se mantiene al máximo.

Camellia

Es un cifrado por bloques de 128 bits desarrollado en Japón por Mitsubishi Electric. Es similar en diseño a AES con seguridad y rendimiento comparables. Está patentado pero disponible bajo una licencia libre de regalías.

SM4

Desarrollado en China. No se conoce el origen de su desarrollo, fue desclasificado en 2006 y usa bloques y claves de 128 bits. Su seguridad se mantiene en 128 bits.

Otros cifrados RC

RC2, predecesor de RC4, fue desarrollado en 1987. No existe mucha investigación sobre él. RC5 fue desarrollado en 1994. Es notable por su simplicidad de implementación. Al igual que RC2, soporta claves de longitud variable y no se le conocen ataques, pero la comunidad criptográfica en general no confía en ellos.

IDEA (*International Data Encryption Algorithm*)

Desarrollado en 1991 como intento de reemplazo de DES. Por problemas de patentes se desarrolló una versión libre de uso, Blowfish.

Blowfish

Soporta longitud de clave variable de 32 a 448 bits. No se conocen ataques, pero la posibilidad de usar claves inseguras es un riesgo. Otro problema es su bloque pequeño, de solo 64 bits de tamaño.

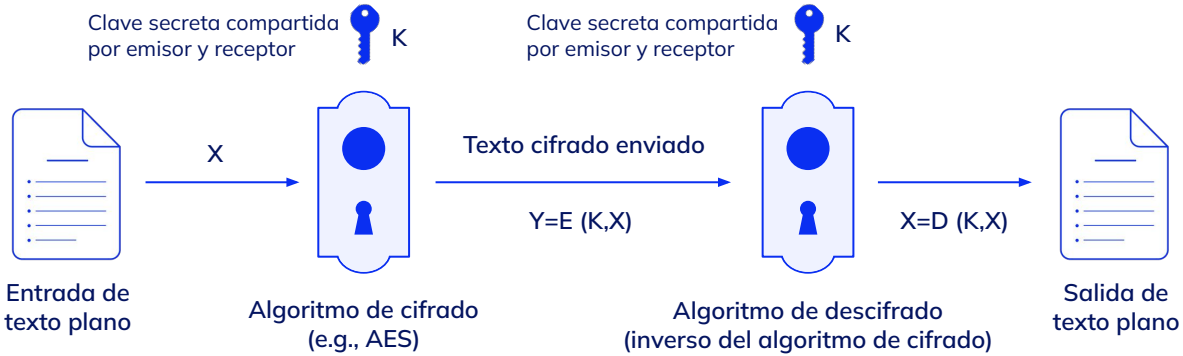
Twofish

Sucesor de Blowfish, con tamaño de bloque de 128 bits y longitudes de clave de 128, 192 o 256 bits.

Esquema de uso

Ventajas: alta velocidad, alta seguridad con claves pequeñas, solo atacables por fuerza bruta

Desventajas: gestión y distribución de claves, no poseen firma digital. Cantidad de claves necesarias según la cantidad de participantes `(n):n(n-1)/2`.



¡Sigamos trabajando!