Laboratorio 4
Authenticated Encryption

Juan Fernando De León	17822
Jose Amado Garcia	181469
Edgar Andree Toledo	18439
Ricardo Antonio Valenzuela	18762
Sara Zavala	18893

1. A.E Galois-Counter Mode (GCM)

¿Cómo funciona?

Es un algoritmo que provee tanto integridad como confidencialidad, está definido para block ciphers que tengan un tamaño de bloque de 128 bits.

Como un Counter Mode normal los bloque son numerados secuencialmente, y luego estos son combinados con un Vector Inicializador, llamado IV, luego es encriptado con un block cipher, normalmente AES. El producto de este cifrado se le hace XOR con el texto plano para obtener el texto cifrado.

Es esencial que un diferente IV sea usado para cada stream que sea encryptado, esto porque esencialmente es un stream cipher como cualquier Counter Mode

¿Cuáles son los usos que actualmente se le da?

- MACsec, ethernet security.
- Es utilizado en OpenVPN desde la versión 2.4
- SSH
- TLS 1.2, 1.3
- Fibre Channel security protocols.
- Utilizado en SoftEther VPN

2. A.E Counter con CBC-MAC(CCM)

- ¿Cómo funciona?

CCM es un cifrado por bloques de 128 bits. Este algoritmo está diseñado para brindar tanto autenticación como confidencialidad. CCM combina CBC-MAC con Counter Mode of encryption. Estas se aplican de tal manera que CBC-MAC se calcula primero en el mensaje para obtener una etiqueta t; el mensaje y la etiqueta se encriptan usando el modo contador.

- ¿Cuáles son los usos que actualmente se le da?

El modo CCM se utiliza en IEEE 802.11i (como CCMP, un algoritmo de cifrado para WPA2), IPsec, y TLS 1.2, así como en Bluetooth Low Energy (a partir de Bluetooth 4.0). Está disponible para TLS 1.3, pero no está habilitado de forma predeterminada en OpenSSL.

3. A.E Encrypt-then-Authenticate-then-Translate (EAX)

¿Cómo funciona?

Es un algoritmo de cifrado autenticado en modo de cifrado de bloque con datos asociados (AEAD) diseñado para proporcionar simultáneamente cifrado autenticado del mensaje con un esquema de dos pasos, un paso para lograr la confidencialidad y otro para la autenticación de cada bloque.

¿Cuáles son los usos que actualmente se le da?

Una modificación del modo EAX, llamado EAX ′ o EAXprime, se usa en el estándar ANSI C12.22 para el transporte de datos basados en medidores a través de una red.

4. PBKDF2

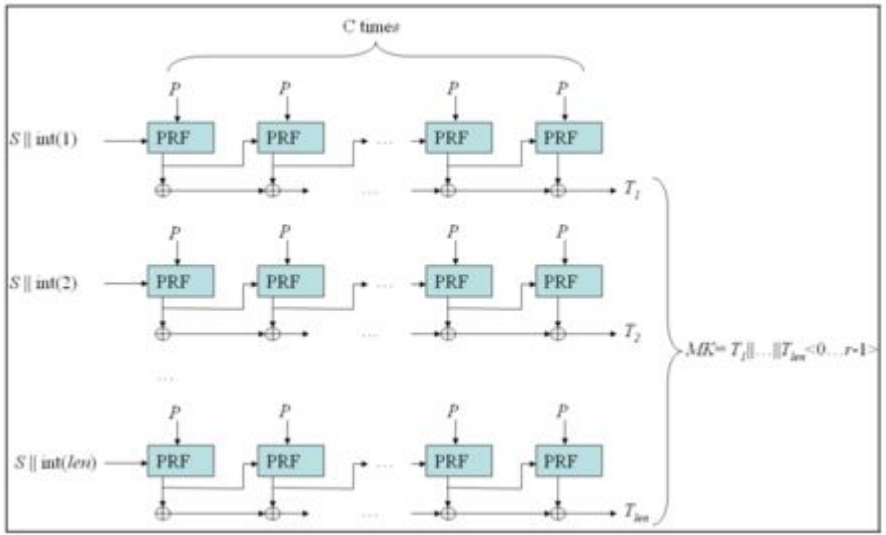
¿Cómo funciona?

En criptografía, PBKDF1 y PBKDF2 (Función 2 de derivación de claves basada en contraseña) son funciones de derivación de claves con un costo computacional variable, que se utilizan para reducir las vulnerabilidades a los ataques de fuerza bruta.

¿Cuáles son los usos que actualmente se le da?

PBKDF2 es parte de la serie PKCS Public-Key Cryptography Standards de RSA Laboratories, específicamente PKCS # 5 v2.0, también publicado como RFC 2898 de Internet Engineering Task Force. Reemplaza a PBKDF1, que solo puede producir claves derivadas de hasta 160 bits de longitud. RFC 8018 (PKCS # 5 v2.1), publicado en 2017, recomienda PBKDF2 para el hash de contraseñas.

4. PBKDF2



5. Expansión de llaves, Argon2

Escriba el algoritmo de su funcionamiento

- Genera el bloque inicial de 64 bytes H0. Todos los parámetros de entrada se concatenan y se introducen como fuente de entropía adicional.
- Los artículos de longitud variable se preparan con su longitud como números enteros de 32 bits.
- Calcula el número de bloques de 1 KB redondeando hacia abajo
- Asignar una matriz bidimensional de bloques de 1 KiB
- Computa el primer y segundo bloque
- Calcula el bloque final C como el XOR de la última columna de cada fila

¿Cuándo se debería usar?

Argon2d está optimizado para configuraciones en las que el adversario no tiene acceso regular a la memoria del sistema o la CPU, es decir, no puede ejecutar ataques de canal lateral basados en la información de tiempo, ni puede recuperar mucho la contraseña más rápido usando la recolección de basura

- ★ Minería de criptomonedas, que toma 0.1 segundos en una CPU de 2 Ghz usando 1 núcleo - Argon2d con 2 carriles y 250 MB de RAM;
- ★ Autenticación del servidor backend, que tarda 0,5 segundos en una CPU de 2 GHz con 4 núcleos: Argon2d con 8 carriles y 4 GB de RAM.

Referencias

- https://en.wikipedia.org/wiki/EAX_mode
- https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf