educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3

Funciones derivadoras de claves (KDF)

KDF: *Key Derivation Function*

Una contraseña o una *frase de paso* son legibles por humanos y no se pueden usar directamente en un algoritmo de cifrado. **Tenemos que usar una clave derivada de la contraseña/frase de paso**.

- ***IKM*** puede ser una contraseña, una frase de paso, una combinación de claves pública y privada.
- ***OKM*** es la clave secreta producida. *IKM* y *OKM* a menudo son de diferente longitud.
- Una ***KDF*** es habitualmente una función *hash* u operaciones de cifrado de bloque ocultas.
- Una función derivadora de claves basadas en contraseñas (***PBKDF***) es un *KDF* diseñado para producir claves secretas a partir de *IKM* de baja entropía tales como las contraseñas. Estas claves pueden usarse para cifrado simétrico. Otro uso de *PBKDF* es el *hasheo* de contraseñas.

Composición de una KDF

Una KDF puede contener los parámetros:

- ***Sal***.
- ***Info***.
- ***PRF***.
- ***Parámetros de resistencia***.
- ***Longitud de OKM***.

Sal

Alguna cantidad de **datos generados de manera aleatoria para añadir azar al proceso de derivación de claves**.

NIST recomienda al menos 128 bits de longitud.

La generación de la *sal* no debe depender del IKM, y puede ser pública o secreta.

Info

Información específica de la aplicación. No añade seguridad, pero puede ser **útil para vincular la clave y su uso**. Puede incluir la versión del protocolo, el identificador del algoritmo, etc.

Utilizar diferentes valores de '`info`' para diferentes propósitos se denomina ***separación de dominio***.

PRF

Una ***función pseudoaleatoria subyacente*** (*PRF*) tal como *HMAC* o una función de cifrado por bloques.

Parámetros de resistencia

Parámetros de **resistencia a los ataques de fuerza bruta** específicos de la función.

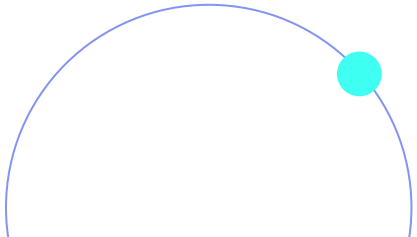
OKM

Longitud de *OKM* deseada.

De todos los parámetros mencionados, el único **obligatoriamente secreto** es ***IKM***.

Propiedades de una KDF

- **Determinístico.**
- **Irreversible**.
- **Resistente**.
- **Entropía de la contraseña**.



Determinístico

Los mismos parámetros de entrada producen siempre **el mismo secreto**.

Irreversible

Es computacionalmente intratable obtener el IKM original a partir del OKM producido.

Resistente

Es resistente a los **ataques de fuerza bruta**.

Entropía de la contraseña

Una contraseña puede usar aproximadamente 80 caracteres diferentes. Al asumir que son todos igualmente probables y que esta probabilidad se distribuye en forma uniforme, la entropía de la contraseña se puede calcular como:

$$Entropía = log_2 (nchar^{plen})$$

Donde:

- **`nchar`** es el número de caracteres posibles (en este caso, 80).
- **`plen`** es la longitud de la contraseña.

La entropía de una contraseña de 8 caracteres será de 51 bits aproximadamente. Si posee 12 caracteres, crecerá hasta 76 bits.

Algoritmos de KDF

- ***PBKDF2*** es un *PBKDF* popular descripto y recomendado por el standard *PKCS#5*. Usa una función *HMAC*, generalmente *HMAC-SHA-256*. Soporta iteraciones variables y puede ser computacionalmente intensiva, pero no usa intensamente la memoria. En 2021 la OWASP (*Open Web Application Security Project*) recomendó 310.000 iteraciones con *HMAC-SHA-256*.
- ***Scrypt*** es un *PBKDF* computacionalmente intensivo y con intensos requisitos de memoria. Usa *HMAC-SHA-256*, pudiendo personalizarse al uso de memoria y paralelismo.
- ***KDF* y *HKDF* de paso simple** no son tan adecuados como *PBKDF*.
- ***ANSI X9.42, ANSI X9.63 y TLS1 PRF*** requieren parámetros específicos de TLS.
- ***SSH KDF*** requiere parámetros específicos de SSH.

> En general, se recomienda el uso de ***Scrypt***.

¡Sigamos trabajando!