Tema 2 – Técnicas Criptográficas y Servicios de Seguridad Asociados

1 Introducción a la criptografía clásica

Un algoritmo de cifrado es uno de los mecanismos fundamentales para implementar servicios de seguridad

- Criptografía: Ciencia que estudia cómo mantener la seguridad en los mensajes, usando, entre otros, algoritmos de cifrado.
- Criptoanálisis: Ciencia que estudia cómo romper los textos cifrados
- Criptología es la combinación de las dos anteriores.

El algoritmo de cifrado es un mecanismo que transforma un texto en claro en texto inteligible (garantizando confidencialidad). Se denota por E (encrypt/cifrar) y opera sobre un texto claro M, para producir el texto cifrado C (criptograma). El algoritmo de descifrado se denota por D (descifrar):

$$E(M) = C$$

$$D(C) = M$$

Los algoritmos como los de hash no tienen descifrado.

1.1 Cifrados por sustitución y transposición

- **Sustitución**: Cada carácter del texto en claro se "sustituye" por otro carácter en el texto cifrado.
  - Caesar: $C: m \rightarrow M + 3\ (mod\ 27)$
  - Homofónico: se asignan a cada símbolo del alfabeto fuente varios del alfabeto cifrado
  - Polialfabético: con alfabetos para posiciones pares e impares distinto.
- **Trasposición**: Cada carácter se permuta.
  - Permutación de filas y columnas
  - Clave: se decide una clave con un tamaño por el cual se escriben las filas, se pueden imponer restricciones con más detalle como orden de la palabra.
  - Nomenclátores: se usa un disco de Alberti junto con nomenclátores que asocia códigos específicos a determinadas palabras con rotaciones al disco.

1.2 Cifrado producto

El método combina ambos anteriores; se puede entender como la aplicación sucesiva de varios cifrados. San lugar a sistemas de cifrados complejos, seguros, más difíciles de atacar y fácilmente trasladables a un ordenador.

1.3 Cifrado Vernam (One-time pad)

Un one-time pad es un conjunto infinito y no repetitivo de letras aleatorias, con la puerta XOR podemos hacer cifrado y descifrado.

2 Algoritmos simétricos o de clave Privada

2.1 Fundamentos

El esquema de intercambio de mensajes con cifrado y descifrado en las partes, no es escalable; para ello una TTP nos podría ayudar, aunque también un parámetro adicional de clave secreta en el algoritmo de cifrado.

Principio de Kerckhoffs:

> *"El sistema no necesita ser un secreto y debe poder caer en las manos del enemigo sin que esto genere problemas."*

En los algoritmos simétricos se tienen dos claves iguales.

El procedimiento suele partir de la semilla, que genera una clave y se aplica con XOR al mensaje. Entre los tipos de generadores pseudo-aleatorios:

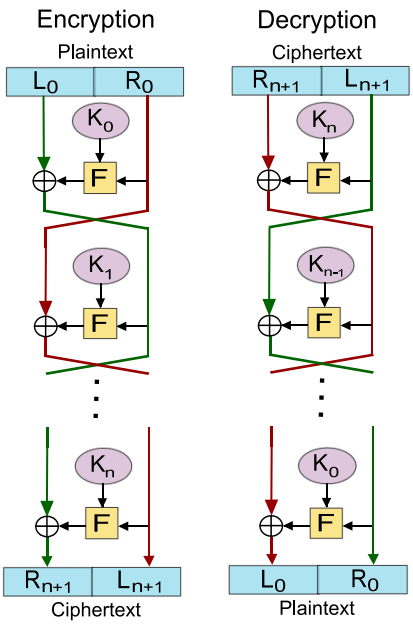
- TRNG, conversión a binario a un flujo de bits aleatorios a partir de un valor aleatorio.
- PRNGm a partir de una semilla.
- PRF, a partir de una semilla e información de contexto.

2.2 Cifrado en bloques

Se divide un texto plano en bloques de información.

2.2.1 Algoritmo DES (Data Encryption Standard)

Parte de un bloque de 64 bits y una clave de igual tamaño. El último byte de cada octeto de la clave se usa como bit de paridad, la longitud efectiva de 56 bits.



Se divide el texto en dos partes, una izquierda y otra derecha y se usa una red de Feistel durante 16 rondas con 16 subclaves en cada etapa.

Esto genera un efecto avalancha en DES de forma que la clave cambia sustancialmente con pequeños cambios. Concepto que se acompañaba de la difusión (cada carácter depende de varias partes de la clave) y confusión (la relación entre el texto cifrado y la clave debe ser tan complicada como sea posible).

La difusión se realiza en la función de Feistel (nº subclaves) y la confusión con las permutaciones (pasos).

2.2.2 Algoritmo triple-DES

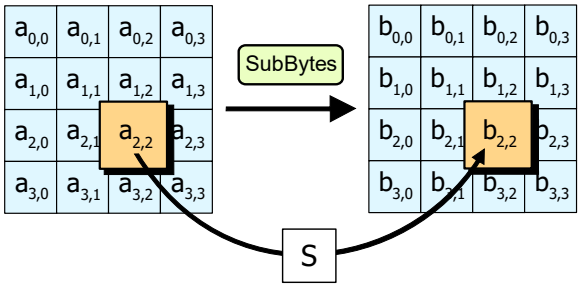
Se aplica el DES en tres partes, en el cifrado se cifra con la clave 1, se descifra con la clave 2 y se cifra con la clave 3; mientras que el descifrado se descifra con la clave 3, cifra con la clave 2 y descifra con la clave 1.

La variante con dos claves ha sido bastante atacada.

2.2.3 Algoritmo AES (Advanced Encryption Standard)

En este caso no se usa una red de Feistel, sino de sustitución-permutación-operaciones aritméticas.

El algoritmo consiste en matrices de 4 x 4 donde se alterarán sustitución de bits, desplazamiento y otras operaciones.



2.2.4 Recomendaciones y otros algoritmos simétricos

Recomendaciones generales, la longitud mínima de clave es 128 bits, el tamaño mínimo de 128 bits y donde la cantidad máxima de información a cifrar debería ser $2^{\frac{n}{2}}$ por clave, donde n es el tamaño del bloque de datos.

Blowfish (IPSEC), Kasumi (UMTS y GSM) o **Camellia** (TLS) son otros posibles algoritmos simétricos.

2.3 Cifrado en flujo

Bit a bit.

2.4 Modos de operación

Entre otros modos de operación podemos encontrar:

- ECB
- CBC: se cuenta con un vector de inicialización
- Cipher Feedback - CFB
- Counter – CTR:
- Galois-CTR (GCM), permite comprobar la autenticidad e integridad del mensaje.

3 Algoritmos Asimétricos o de clave pública

Mientras tanto, los algoritmos asimétricos necesitan dos claves distintas, claves de sesión. Se utilizan por pares, de tal forma que cada usuario posee dos claves; si se cifra con una, se descifra con la otra:

- Una clave pública, conocida por todos los usuarios
- Una clave privada, conocida por el usuario.

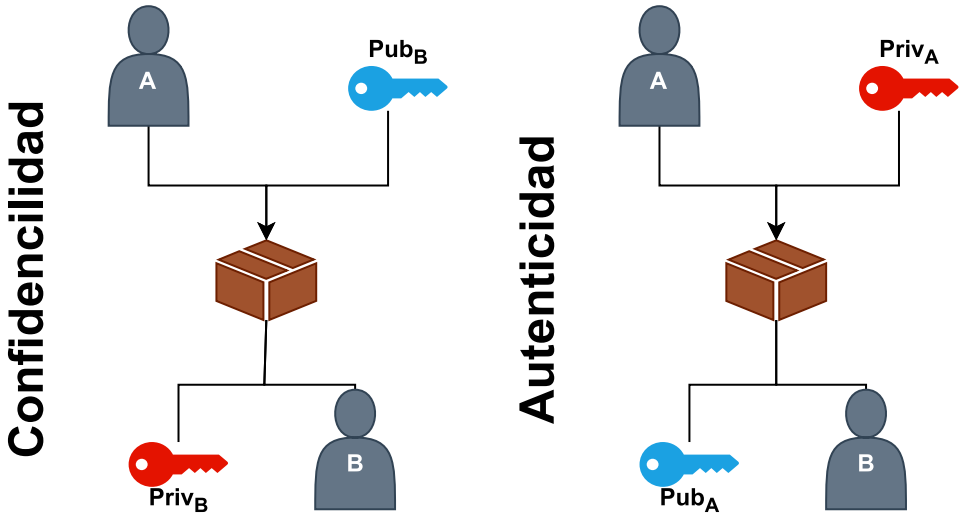
Se puede usar con los siguientes propósitos para una comunicación de A a B:

- **Autenticidad** (Firma digital):

$$D_{K_{Pub_a}}\left(E_{K_{Priv_a}}(M)\right) = M$$

- **Confidencialidad**:

$$D_{K_{Priv_b}}\left(E_{K_{Pub_b}}(M)\right) = M$$



3.1 Cifrado / Descifrado

- No se puede deducir la clave privada de un usuario.
- El número de claves necesarias pasa a ser 2 · n.
- Las claves son de gran tamaño, las funciones matemáticas son complejas y, por tanto, el rendimiento es más lento que el simétrico/clave privada.

No todos los algoritmos permiten las funcionalidades siguientes:

Algoritmo	Cifrado/Descifrado	Firma Digital	Intercambio de Clave
RSA			
Curvas Elípticas			
Diffie-Helman			
DSS			

3.2 Intercambio de Claves

Un criptosistema híbrido combina los criptosistemas de clave pública y privada.

$$D_{K_{Priv_b}}\left(E_{K_{Pub_b}}(K_{AB})\right)$$

, siendo K_{AB}, una clave de sesión (privada).

3.3 Algoritmo de Diffie-Hellman

Si α es una raíz primitiva del número primo q tal que $\alpha < q$, entonces los números

$$\alpha \bmod q, \alpha_2 \bmod q, \ldots, \alpha_{q-1} \bmod q$$

, son distintos entre sí y sus valores son los enteros 1 a q - 1, en cualquier orden.

3.4 Algoritmo RSA (Rivest, Shamir y Adleman)

Es un criptosistema basado en la factorización de producto de números primos grandes distintos. Las variables serán el módulo y clave pública, y la clave privada. Si los bloques son demasiado pequeños, podría romperse con más facilidad.

4 Otras Primitivas criptográficas

4.1 Hash

No se considera algoritmo de cifrado (no se puede descifrar).

Son funciones unidireccionales de cifrado, que toman unos datos y devuelven un valor (digest). Ya que no sirve para el intercambio de mensajes, no se permite el descifrado, sí nos puede garantizar la integridad del mensaje. Firmando digitalmente el hash podremos comprobar la integridad del mensaje si el resultado es el mismo.

$$E_{Priv_a}(H(M))E_{KAB}(M)$$

Por lo general, su rapidez debe ser notable. Entre otras funciones encontramos las siguientes funciones no seguras por ataques criptoanalíticos y colisiones teóricas:

- **MD-5**
- **RIPEMD-128**
- **SHA-1**
- **SHA-2 (256, 384, 512)**, colisiones muy reducidas

Alternativas más seguras:

- **SHA-3** (224, 256, 384, 512)
- **Whirlpool** (512), con un comportamiento similar al AES

4.2 MAC

Es un código de autenticación de mensajes o checksum criptográfico. Una función MAC toma como parámetro un mensaje y una clave y devuelve un MAC. Introduce un hash al final del texto para comprobar la integridad cuando se descifre.

5 Test

5.1 Camellia se caracteriza porque:

a. **por ser uno de los posibles algoritmos de cifrado en TLS.**
b. por presentar una serie de problemas que no afectan a su uso práctico en aplicaciones móviles.
c. por ser uno de los posibles algoritmos de cifrado en SSL.
d. por gestionar bloques de 64 bits.

5.2 ¿Cuáles son las operaciones primitivas del proceso de cifrado/descifrado AES?

a. **AddRoundKey, SubBytes, ShiftRows, MixColumns**
b. XOR, S-Box
c. ShiftLeft, ShiftRight, MoveRows, MoveColumns
d. Rotword, SubBytes, XOR, Rcon

5.3 ¿Cuáles son las tres funcionalidades básicas con la criptografía asimétrica?

a. Cifrado, Firma Digital, Control de acceso.
b. **Cifrado, Firma Digital, Intercambio de claves.**
c. Cifrado, Descifrado, Intercambio de claves.
d. Póker mental, "bit commitment", ZKP.

5.4 ¿Qué modo de operación simula un cifrado en flujo, y proporciona tanto cifrado como autenticación?

a. CFB
b. OFB
c. CTR
d. **GCM**

5.5 E y P en el algoritmo de DES corresponden a:

a. Dos matrices de permutación con objetivos específicos de expansión.
b. Una matriz de permutación y una matriz de permutación de expansión, respectivamente
c. Una matriz de expansión y una matriz de compresión, respectivamente.
d. **Una matriz de permutación añadiendo expansión y una matriz de permutación, respectivamente.**

5.6 El principio de Kerckhoffs se define como:

a. "The system must be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience".
b. "The system must be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience".
c. **"The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience".**
d. "The system must not be required to be secret, and it must not be able to fall into the hands of the enemy without inconvenience".

5.7 ¿Qué modo de operación establece un contador único?

a. CFB
b. **CTR**
c. OFB
d. GCM

5.8 El tamaño mínimo para la clave pública generada con RSA y ECC es de:RSA: 1024; ECC: 172

a. RSA: 2048; ECC: 172.
b. RSA: 1024; ECC: 190.
c. RSA: 2048; ECC: 190.
d. **RSA: 1024; ECC: 172.**

5.9 ¿Qué es la criptografía?

a. Ciencia que estudia cómo ocultar mensajes u objetos dentro de otros objetos (p.ej. imágenes).
b. **Ciencia que estudia cómo mantener la seguridad en los mensajes.**

c. Ciencia que estudia cómo romper los textos cifrados.
d. Ciencia que estudia cómo analizar mensajes cifrados.

5.10 ¿En qué problema matemático se basa el protocolo Diffie Hellman original de 1976?

a. **La dificultad de computar logaritmos discretos.**
b. Hallar la factorización del producto de dos números primos.
c. Encontrar el logaritmo discreto de un elemento de curva elíptica aleatoria, con respecto a un punto base conocido públicamente.
d. Todo lo anterior.

5.11 ¿Cuáles son las longitudes de clave en RSA?

a. Entre 128 y 160 bits
b. Entre 128 y 256 bits
c. Entre 4096 y 16384 bits
d. **Entre 1024 y 2048 bits, aunque puede llegar a ser 4096**

5.12 ¿Cuáles funciones hash son a día de hoy seguras de utilizar?

a. SHA-1, SHA-2
b. MD5
c. SHA-1, Keccak
d. **SHA-2, SHA-3**

5.13 El tamaño mínimo de bloque de datos recomendado para cifrar datos (y usando cualquier algoritmo de cifrado) es de:

a. **128 bits**
b. 256 bits
c. 192 bits
d. 56 bits

5.14 César consiste en un cifrado:

a. por transposición
b. por monenclaturas
c. **por sustitución**
d. por sistemas polialfabéticos

5.15 El cifrado 3-DES con dos claves consiste en:

a. **Cifrar, Descifrar y Cifrar con K1, K2 y K1 claves en cada etapa**
b. Cifrar con K1, K2 y K1 claves en cada etapa
c. Cifrar, Descifrar y Cifrar con K2, K1 y K1 claves en cada etapa
d. Cifrar usando K1 dos veces

5.16 En una función hash criptográfica, ¿Qué significa ser "weak collision resistant" (resistencia débil a colisiones)?

a. Es computacionalmente imposible encontrar un par (x,y) tal que H(y) = H(x)
b. La función H proporciona un valor pseudoaleatorio
c. Para una huella digital h, es computacionalmente imposible encontrar una y tal que H(y) = h

d. **Para cualquier bloque x, es computacionalmente imposible encontrar una y != x tal que H(y) = H(x)**

5.17 En RSA: e, d y n corresponden a:

a. e: clave pública, d: el módulo y n: clave privada
b. e: clave privada, e: clave pública y n: el módulo
c. e: el módulo, d: clave privada y n: clave público
d. **e: clave pública, d: clave privada y n: el módulo**

5.18 ¿A qué se refiere E = E1 . E2 . ••• . Er?

a. Cifrado de algoritmos de transposición
b. Cifrado de algoritmos por sustitución
c. Cifrado César
d. **Cifrado producto**

5.19 ¿Qué operaciones utilizarias para descifrar el siguiente dato? Cifrado(Padding(Hash(dato)))

a. Descifrado, Unpadding, Unhashing
b. Descifrado con la clave pública
c. **Descifrado, Unpadding**
d. Descifrado con la clave privada

5.20 La clave secreta de DH se computa de la siguiente forma:

a. K = alpha^(Xa) mod q
b. Ninguna es correcta
c. K = yb^(Xb) mod q
d. **K = Yb^(Xa) mod q**

5.21 ¿Qué problemática resuelve el uso de claves secretas K con respecto a los algoritmos de cifrado "clásicos"?

a. Hace que Alice pueda utilizar el mismo algoritmo E en sus comunicaciones con todos los usuarios
b. En comparación con los algoritmos de cifrado clásico, es más escalable, ya que no hace falta usar un algoritmo de cifrado para cada destinatario.
c. **Todo lo anterior**
d. Evita el "security by obscurity": Ya no es necesario mantener en secreto el algoritmo de (des)cifrado

5.22 ¿Cuántas etapas tiene la operación de cifrado de DES?

a. 20
b. **16**
c. 12
d. 18

5.23 $E_{K_{Priv}}(H(M)) \,||\, E_{K_{Pub}}(K_{KS}) \,||\, E_{K_{KS}}(M)$

a. Hay confidencialidad e integridad.
b. Hay confidencialidad y autenticación.
c. Hay integridad y autenticación.
d. **Hay confidencialidad, integridad y autenticación.**

5.24 ¿En qué consiste el cifrado César en el alfabeto español?

a. **Cada carácter de texto en claro se reemplaza por el carácter tercero a la derecha, módulo 27.**
b. Se Hace uso del disco de Alberti junto con nomenclátores.
c. El texto en claro se escribe como secuencia de filas (con una cierta profundidad) y se lee como secuencia de columnas.
d. Asigna a un símbolo del alfabeto fuente varios del alfabeto cifrado.

5.25¿Qué es una función MAC?

a. Una función que toma como entrada un mensaje M y una clave asimétrica privada Kpr, y produce un valor hash
b. Una función que toma como entrada un mensaje M y una clave asimétrica pública Kpb, y produce un valor hash
c. **Una función que toma como entrada un mensaje M y una clave simétrica K, y produce un valor hash**
d. Una función que toma como entrada un mensaje M y un one-time-pad, y produce un valor hash

5.26En criptografía de clave pública:

a. El término de criptografía de clave pública no existe, ser criptografía asimétrica
b. Existen dos claves K y K* equivalentes pero se aplican de forma distinta
c. Existe sólo una clave para cifrar y descifrar
d. **Existen dos claves K y K* distintas**

5.27 ¿Cuáles son las propiedades definidas por Claude Shannon para evitar (o dificultar) los ataques basados en análisis estadísticos?

a. Confusión y Permutación
b. **Difusión y Confusión**
c. Difusión y Diseminación
d. Permutación y Diseminación

5.28 El cifrado 3-DES con tres claves consiste en:

a. Cifrar con K1, K2 y K3 claves en cada etapa
b. Cifrar, Descifrar y Cifrar con K1, K2 y K1 claves en cada etapa
c. **Cifrar, Descifrar y Cifrar con K1, K2 y K3 claves en cada etapa**
d. Cifrar usando K1 tres veces

5.29¿Cuál es la forma de escoger la clave pública en el algoritmo RSA?

a. $\alpha^{X_A * X_B} \ mod \ q$
b. $PHI(n) = (p - 1) \cdot (q - 1)$
c. $\boldsymbol{MCD\left(e, PHI(n)\right) = 1;\ siendo\ e < PHI(n)}$
d. $e \cdot d = 1 \left(mod\ PHI(n)\right);\ siendo\ d < PHI(n)$

5.30 Con ECC se puede:

a. Firmar e intercambiar claves
b. Cifrar y firmar
c. Intercambio caves

d. Cifrar, firmar e intercambiar claves

Bibliografía

Tema 2 – Técnicas Criptográficas y Servicios de Seguridad Asociados, Antonio Muñoz, LCC UMA.

De User:Matt Crypto - Trabajo propio, Dominio público, https://commons.wikimedia.org/w/index.php?curid=1118913

By Feistel_cipher_diagram.svg: Amirkiderivative work: Amirki (talk) - Feistel_cipher_diagram.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=16419258