Seguridad de Redes de Computadores

Redes de Computadores

FIEC04705

Sesión 23

Agenda

- Terminología
- Introducción a criptografía
- Criptografía de clave simétrica
- Criptografía de clave asimétrica

Terminología

Terminología

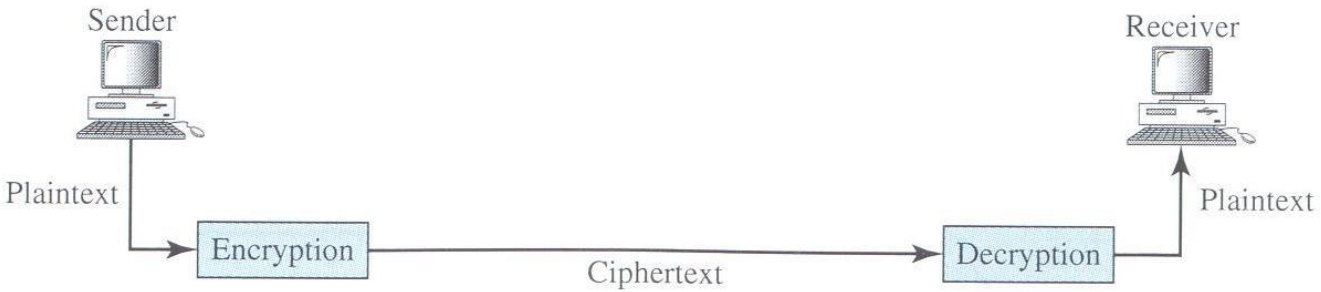
- **Criptografía** es una palabra de origen griego que significa escritura secreta. Se utiliza el término para referirse a la ciencia y arte de transformar mensajes para hacerlos seguros e inmunes a ataques.

Introducción a la criptografía

Introducción a la criptografía

- Texto plano es el mensaje original antes de ser transformado.
- Texto cifrado es el mensaje después de ser transformado.

Figure 30.1 *Cryptography components*



Introducción a la criptografía

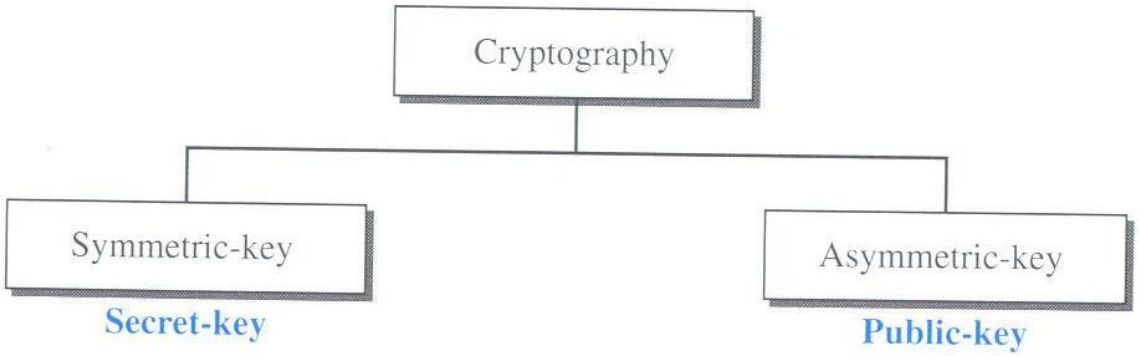
- Un algoritmo de encriptación transforma el texto plano en texto cifrado.
- Un algoritmo de desencriptación transforma el texto cifrado al texto plano original.
- Los ciphers es el término para referirse a los algoritmos de encriptación y descriptación.
- La llave es un número o conjunto de números que el cipher utiliza para encriptar o desencriptar un mensaje.

Notación de Alice y Bob

- En criptografía para representar a los participantes en un escenario de intercambio de información se utilizan los nombres Alice, Bob y Elvis (Eve, Malice).
- Alice necesita enviar datos con seguridad
- Bob es el destinatario de los datos
- Elvis es la persona que intenta perturbar la comunicación entre Alice y Bob:
  - Interceptando los mensajes para descubrir los datos
  - Enviando sus propios mensajes disfrazados

Taxonomía de Ciphers

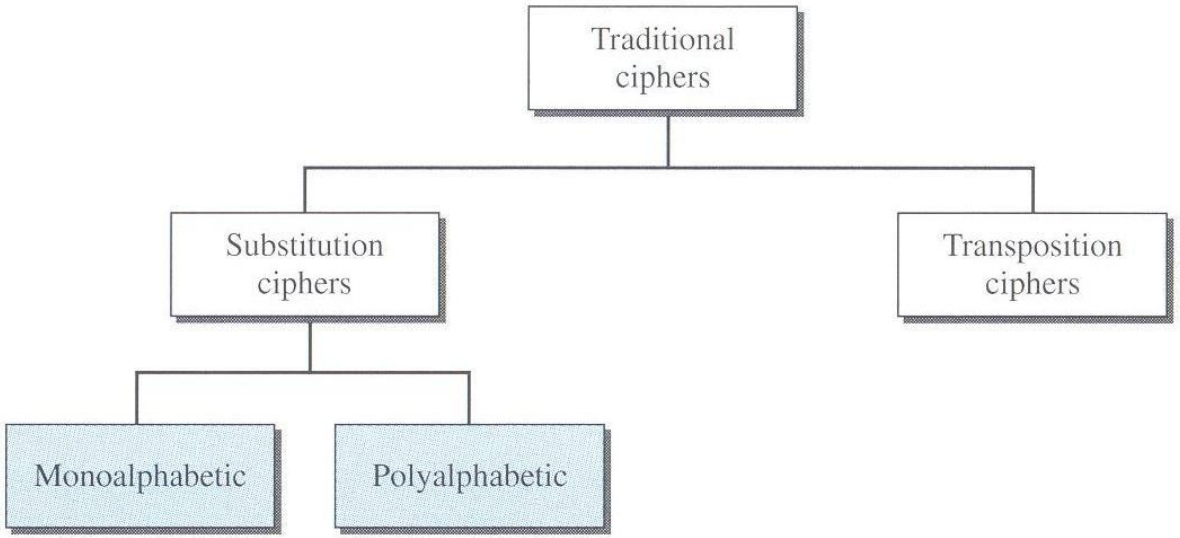
Figure 30.2 *Categories of cryptography*



Criptografía de clave simétrica

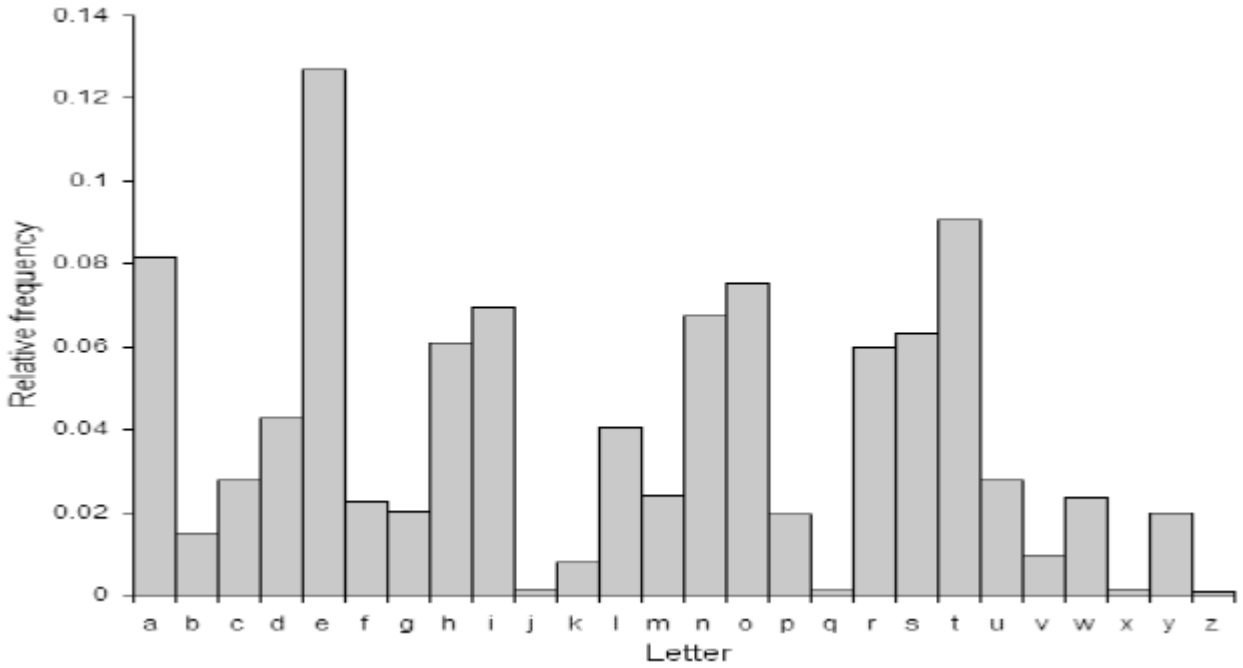
Criptografía de clave simétrica

Figure 30.7 *Traditional ciphers*



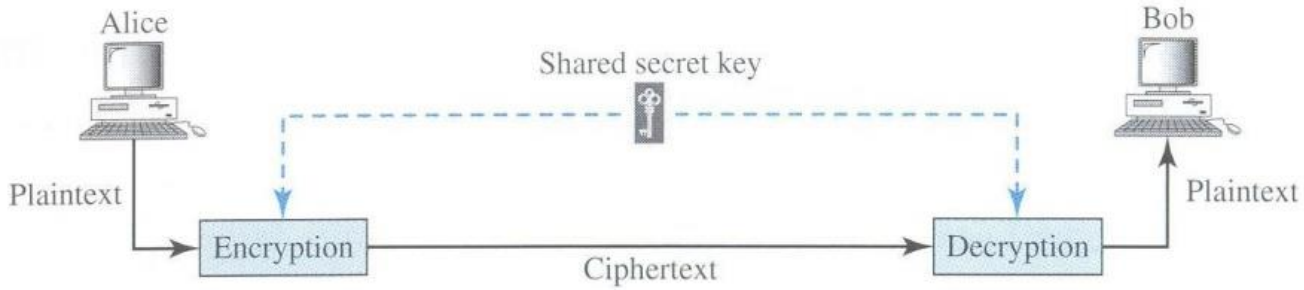
Análisis de frecuencia

- Cuenta el número de veces que cada símbolo se repite y en base a lo cual trata de derivar conclusiones.



Criptografía de clave simétrica

Figure 30.3 *Symmetric-key cryptography*



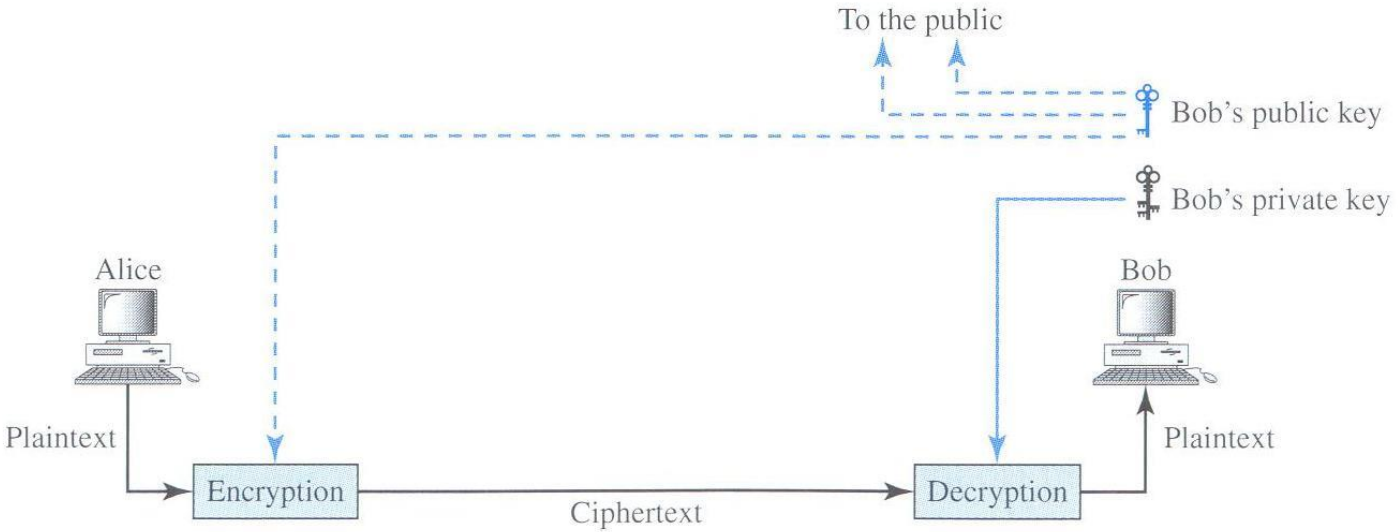
In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Criptografía de clave asimétrica

Criptografía de clave asimétrica

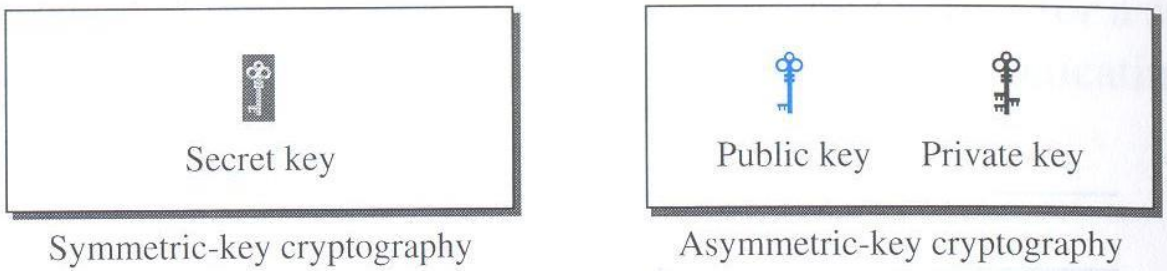
- Existen dos llaves:
  - Una privada que es mantenida por el receptor
  - Una pública que es publicada para conocimiento de todos

Figure 30.4 *Asymmetric-key cryptography*



Tipos de llaves

Figure 30.5 *Keys used in cryptography*



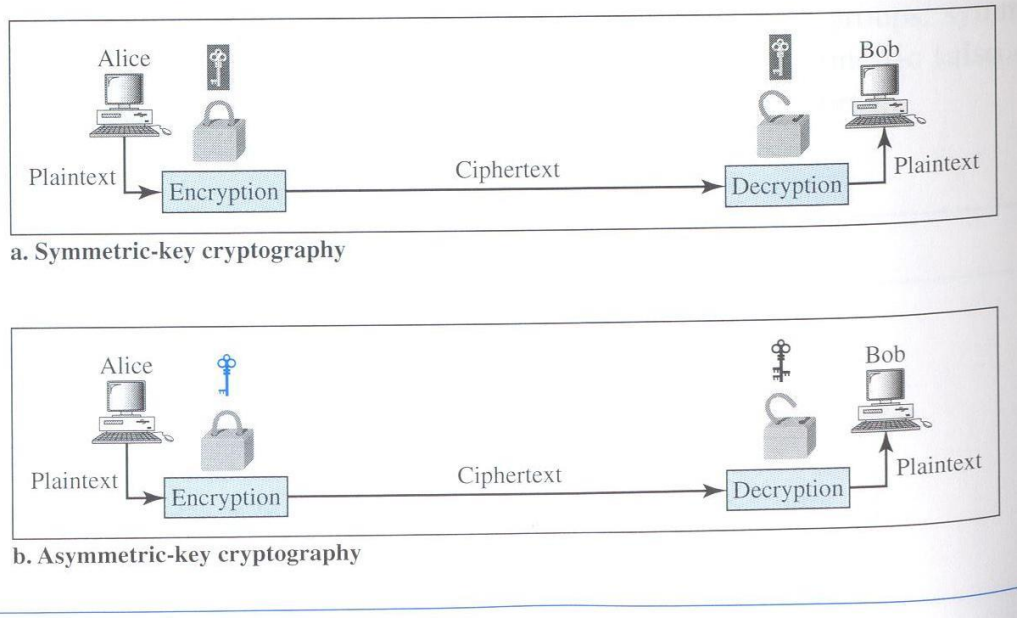
Symmetric-key cryptography

Asymmetric-key cryptography

Comparación entre tipos de algoritmos

- En los de clave simétrica, la misma llave encripta y desencripta.
- En los de llave asimétrica, una llave encripta y la otra desencripta.

Figure 30.6 *Comparison between two categories of cryptography*



Ciphers de clave simétrica

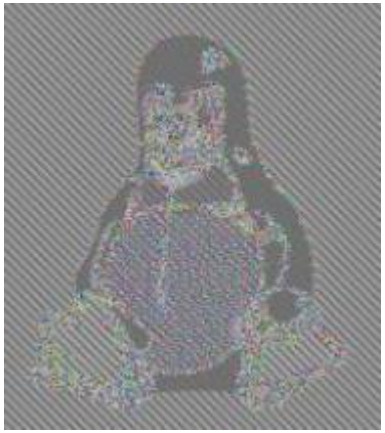
Block Ciphers

- Advanced Encryption Standard (AES)
  - Trabaja en bloques de 128 bits
  - Utiliza una permutación: ShiftRows y tres sustituciones: SubBytes, MixColumns, AddRoundKey
- Data Encryption Standard (DES)
  - Diseñada por IBM al inicio de los 70s
  - En 1990, Biham & Shamir descubrieron el criptoanálisis diferencial
  - Se puede romper por fuerza bruta
- 3-DES
  - Toma tres llaves de manera que $E_{K1K2K3}(M) = E_{K3}(D_{K2}(E_{K1}(M)))$
  - Se espera que sea bueno hasta el 2030
  - Usado en tarjetas bancarias y chips RFID

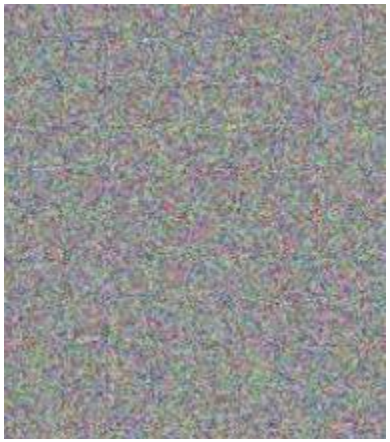
Block ciphers modes

- Electronic codebook mode (ECB)
  - Cada bloque es encriptado individualmente
- Cipher Block Chaining mode (CBC)
  - Cada bloque es un XOR con el bloque previo
  - Existe un vector de inicialización

Original



ECB



CBC

Ciphers de llave asimétrica

Diffie-Hellman

- Alice y Bob escogen números r_A and r_B para encontrar
- "$t_A = g^{rA} \bmod p$" y "$t_B = g^{rB} \bmod p$"
- El protocolo intercambia estos números:
- 1. A → B: p, g, t_A
- 2. B → A: t_B
- "Alice" calcula "$t_B{}^{rA} \bmod p$" y "Bob" "$t_A{}^{rB} \bmod p$"
- La llave es: $K = g^{rArB} \bmod p$

Ciphers de llave asimétrica

- Diffie-Hellman
  - Es utilizado como un protocolo de agreement
- Elgamal
  - Es Diffie-Hellman convertido a un esquema de llave pública. Utiliza un g y p fijos.
  - Alice escoje r_A como su llave privada y $t_A{}^{rA}$ mod p como su llave pública.
- RSA
  - Es el más popular y eficiente
  - Se utiliza para firmas

Límite de la longitud del mensaje

- RSA no puede encriptar mensajes más largos que la longitud de la llave.
- RSA es lento
- Por lo tanto, se debe encriptar la llave AES con la llave RSA, luego encriptar el mensaje utilizando AES
- $E_{RSA}(M) = E_{KRSA}(K_{AES}),E_{KAES}(M)$
- Usando RSA tenemos: $E_{pub}(D_{priv}(M)) = M$

Puntos para recordar

- Notación de Alice y Bob
- Uso y limitaciones de la criptografía de clave simétrica
- Uso y limitaciones de la criptografía de clave asimétrica

Próxima Sesión

- Seguridad en capa de red