

Introducción a la Criptografía

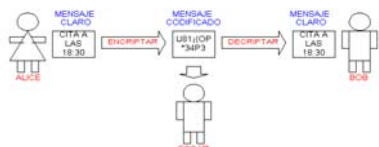
Alfredo Villalba
villalb0@etu.unige.ch

Contenido

- Introducción.
- Servicios de seguridad, riesgos y ataques.
- Criptografía simétrica.
- Criptografía asimétrica (llave pública)
- Servicios de seguridad en Internet.
- Conclusiones.

Introducción (I)

- El objetivo principal de la Criptografía es de permitir la comunicación entre dos personas sin que una tercera persona pueda comprender el mensaje transmitido.



Introducción (II)

- Julio César utilizaba por ejemplo la Codificación por Desplazamiento para transmitir sus mensajes secretos.

ATACAMOS ESTA NOCHE
↓ (desplazar 3 letras a la derecha)
DWAFFDPRV HVWD QRFKH

Introducción (III)

- Los métodos antiguos como la Codificación por Desplazamiento son fáciles de descodificar.
- En nuestros tiempos se utilizan métodos mucho más resistentes a los ataques efectuados por terceras personas.

Servicios de Seguridad, Riesgos y Ataques (I)

- CONFIDENCIALIDAD
 - **Objetivos:** Protección contra una divulgación no autorizada de la información.
 - **Riesgos:** Divulgación no autorizada de la información.
 - **Ataques:** Escuchar ilícitamente, analizar el tráfico.
 - **Protección clásica:** Cajas fuertes, cadenas, candados.
 - **Protección digital:** Encriptar, autorización lógica.

Servicios de Seguridad, Riesgos y Ataques (II)

- INTEGRIDAD
 - **Objetivos:** Protección contra la modificación no autorizada de la información.
 - **Riesgos:** Modificación de la información.
 - **Ataques:** Creación, alteración o destrucción ilícita.
 - **Protección clásica:** Tinta especial, hologramas.
 - **Protección digital:** Funciones de sentido único + encriptación.

Servicios de Seguridad, Riesgos y Ataques (III)

- DISPONIBILIDAD
 - **Objetivos:** Asegurar la utilización de los recursos informáticos por usuarios legítimos.
 - **Riesgos:** Utilización ilícita.
 - **Ataques:** Virus, accesos repetitivos tratando de colapsar un sistema.
 - **Protección clásica:** Control de acceso físico, vigilancia por video.
 - **Protección digital:** Control de acceso lógico, anti-virus.

Servicios de Seguridad, Riesgos y Ataques (IV)

- AUTENTIFICACIÓN DE ENTIDADES
 - **Objetivos:** Verificar la identidad de una persona o sistema.
 - **Riesgos:** Acceso no autorizado.
 - **Ataques:** Robo del password, falla del protocolo de autenticación.
 - **Protección clásica:** Presencia física, voz, C.I., retina ocular.
 - **Protección digital:** Password, tarjeta de crédito + PIN, dirección IP + login.

Servicios de Seguridad, Riesgos y Ataques (V)

- AUTENTIFICACIÓN DEL ORIGEN DE LA INFORMACIÓN
 - **Objetivos:** Verificar que una cierta entidad es el origen de la información de interés.
 - **Riesgos:** Falsificación de la información.
 - **Ataques:** Falsificación de la firma, fallas en el protocolo de autenticación.
 - **Protección clásica:** Sello y firma.
 - **Protección digital:** Funciones de sentido único + encriptación.

Servicios de Seguridad, Riesgos y Ataques (VI)

- NO-REPUDIACIÓN
 - **Objetivos:** Garantiza que una entidad no pueda negar su participación en una transacción.
 - **Riesgos:** Negar la participación.
 - **Ataques:** Pretender un robo de password o una falla en el protocolo de la transacción.
 - **Protección clásica:** Sello, firma, firma notarial, envío certificado.
 - **Protección digital:** Funciones de sentido único + encriptación + firma digital.

Servicios de Seguridad, Riesgos y Ataques (VII)

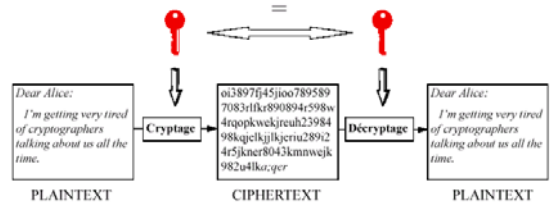
- NO-DUPLICACIÓN
 - **Objetivos:** Protección contra las copias ilícitas.
 - **Riesgos:** Duplicación.
 - **Ataques:** Falsificación, imitación.
 - **Protección clásica:** Tinta especial, hologramas, tatuajes.
 - **Protección digital:** Tatuaje digital (watermarking).

Servicios de Seguridad, Riesgos y Ataques (VIII)

- ANONIMATO
 - **Objetivos:** Garantiza el anonimato de una entidad durante una transacción.
 - **Riesgos:** Identificación.
 - **Ataques:** Análisis de una transacción, acceso no autorizado al sistema para poder identificar.
 - **Protección clásica:** Alteración de la voz, disfraz, pagos en efectivo.
 - **Protección digital:** Mezcladores, dinero electrónico.

Criptografía simétrica (I)

- Con la ayuda de UNA SOLA LLAVE SECRETA, encriptar y decriptar un mensaje.



Criptografía simétrica (II)

- Servicios soportados: Confidencialidad, Autenticación, Integridad.
- Siendo la llave compartida entre las dos entidades, no es posible elaborar las firmas digitales.
- La llave secreta debe ser previamente intercambiada entre las entidades a través de un canal seguro (correo, teléfono, etc.)
- Existen varios sistemas criptográficos simétricos, entre los cuales: AES, DES, IDEA, RC4, RC5, etc.

Criptografía simétrica (III)

- IDEA (International Data Encryption Algorithm)
 - Creado por Xuejia Lai y James Massey en 1990.
 - Es el algoritmo de codificación por bloques más seguro hasta el momento.
 - Utiliza una llave secreta de 128 bits para encriptar bloques de información de 64 bits.
 - Más precisamente, utiliza 52 sub-llaves de 16 bits generadas a partir de la llave secreta, a fin de realizar operaciones aritméticas y XOR's con los bloques de 64 bits.
 - Operaciones utilizadas: adición modulo 2^{16} y multiplicación modulo $2^{16}+1$

Criptografía simétrica (IV)

- IDEA – Generación de las sub-llaves
 1. La llave de 128 bits está dividida en 8 sub-llaves de 16 bits.
 2. Los bits de la llave de 128 bits sufren una rotación circular de 25 bits a la izquierda. Con esta nueva llave se continúa en el paso 1.
 3. Los pasos anteriores se repiten hasta obtener las 52 sub-llaves de 16 bits, llamadas: Z_1, Z_2, \dots, Z_{52} .

Criptografía simétrica (V)

- IDEA – Encriptación
 - El mensaje se divide en bloques de 64 bits, los cuales son codificados uno por uno.
 - Cada bloque de 64 bits se divide en 4 sub-bloques de 16 bits, llamados: X_1, X_2, X_3 y X_4 .
 - A estos cuatro bloques se aplica 8 veces los pasos 1 a 14 de la transparencia consecutiva.
 - Finalmente, a los cuatro bloques resultantes se les aplica los pasos 15 a 18 de la transparencia consecutiva.
 - Estos últimos cuatro bloques resultantes forman el bloque de 64 bits codificado.

Criptografía asimétrica (V)

- RSA
 - Sistema criptográfico desarrollado por Rivest, Shamir y Adleman en 1977.
 - Basado en la dificultad de la factorización en factores primos de números enteros bastante grandes ($\sim 10^{300}$)
 - Ampliamente utilizado en nuestros tiempos.
 - Longitud típica de las llaves: 512 y 1024 bits.

Criptografía asimétrica (VI)

- RSA – Publicación de la llave pública.
 - Bob genera dos enteros primos bastante grandes p y q .
 - Bob calcula $n=pq$ y $\phi(n)=(p-1)(q-1)$.
 - Bob escoge aleatoriamente un b tal que $1 < b < \phi(n)$ y $\text{mcd}(b, \phi(n))=1$.
 - Bob calcula $a=b^{-1} \text{mod } \phi(n)$.
 - Bob guarda su llave privada (a,n) .
 - Bob publica su llave pública (b,n) .

Criptografía asimétrica (VII)

- RSA – Encriptación de un mensaje
 - Alice compone el mensaje x (un entero).
 - Alice recupera la llave pública de Bob (b,n) .
 - Alice encripta el mensaje $y=x^b \text{mod } n$.
 - Alice envía el mensaje codificado y a Bob.
- RSA – Decriptación de un mensaje
 - Bob recibe el mensaje codificado y .
 - Bob decripta el mensaje $x=y^a \text{mod } n$ con su llave privada (a,n) .

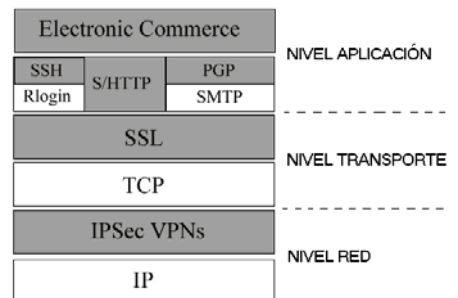
Criptografía asimétrica (VIII)

- RSA – Intento de Ataque.
 - Oscar recupera la llave pública de Bob (b,n) .
 - Oscar recupera el mensaje codificado y enviado a Bob por Alice.
 - Oscar necesita conocer a para poder descodificar el mensaje. Factorizando n en p y q , se puede calcular $\phi(n)=(p-1)(q-1)$, y con b se puede calcular $a=b^{-1} \text{mod } \phi(n)$.
 - Pero la FACTORIZACIÓN es un problema MUY DIFÍCIL.

Servicios de seguridad en Internet (I)

- Los servicios de seguridad en Internet se encuentran en diferentes niveles de la red (cf. modelo OSI/ISO):
 - Nivel Red:
 - IPsec, VPNs (Virtual Private Networks).
 - Nivel Transporte:
 - SSL (Netscape), PCT (Microsoft).
 - Nivel Aplicación:
 - Secure HTTP, PGP, SSH, S/MIME, etc.
 - Protocolos de pago electrónico.
 - Protocolos de dinero electrónico.
 - ...

Servicios de seguridad en Internet (II)



Servicios de seguridad en Internet (III)

- SSL (Secure Socket Layer)
 - Tiene por objetivo establecer una conexión segura a nivel transporte.
 - Creado e implantado por Netscape.
 - Se ubica entre el nivel transporte y los protocolos del nivel aplicación (HTTP, SMTP, FTP, etc.)
 - Ofrece los servicios de seguridad sgtes.:
 - Confidencialidad.
 - Integridad.
 - Autenticación del servidor (y del cliente).

Servicios de seguridad en Internet (IV)

- SSL (Secure Socket Layer)
 - Basado en la criptografía asimétrica (RSA, Diffie-Hellman).
 - Está en vías de convertirse un standard para la seguridad en WWW.
 - Trabajos recientes para adaptarlo a los protocolos SMTP y FTP.
 - El lenguaje JAVA tiene paquetes que permiten al programador abrir fácilmente una conexión segura utilizando SSL (programación de sockets, cliente-servidor).

Servicios de seguridad en Internet (V)

- PGP (Pretty Good Privacy)
 - Utilizado en el correo electrónico (protocolo SMTP).
 - Ofrece los sgtes. servicios de seguridad:
 - Confidencialidad.
 - Integridad.
 - Autenticación.
 - Firma digital.
 - No-Repudiación.
 - La autenticidad de las llaves públicas utilizadas es verificada por una red de confianza que se establece entre los usuarios.

Servicios de seguridad en Internet (VI)

- SSH (Secure Shell)
 - Reemplaza el Telnet para ejecutar comandos a distancia de manera segura.
 - Telnet tiene los sgtes. inconvenientes:
 - Autenticación insegura del cliente: password transmitido sin ser codificado.
 - Todas las transmisiones subsiguientes se hacen sin ser codificadas.
 - SSH utiliza la criptografía asimétrica para iniciar la sesión y fijar una llave secreta. Luego durante la transmisión se utiliza la criptografía simétrica para codificar la información que circula.

Conclusiones

- La resistencia de la criptografía a los ataques está basada en la dificultad calculatoria de ciertos problemas matemáticos, o en la extrema confusión y dispersión aplicada a la información.
- En un entorno distribuido y abierto como es Internet, la criptografía juega un rol muy importante.
- Existen una diversidad de sistemas criptográficos, muchos de los cuales vienen en las librerías de los lenguajes y listos para ser utilizados, por ejemplo Java.
- Cuando se desarrolla un programa serio para Internet, es necesario pensar en la seguridad.
- Existe bastante información en Internet para profundizar los diferentes métodos criptográficos.

Bibliografía

- [Men97]: Menezes, A et al. *Handbook of Applied Cryptography*. CRC press series on discrete mathematics and its applications. 1997. URL (Mars 2002): <http://cacr.math.uwaterloo.ca/hac/>
- [Sch96]: Schneier, B. *Applied Cryptography*. Second Edition. John Wiley & Sons. 1996.
- [Sti95]: Stinson, D. R. *Cryptography: Theory and Practice*. CRC Press Series on Discrete Mathematics and Its Applications. CRC Press, Inc. 1995.
- [Kau95]: Kaufman, C. et al. *Network Security*. Private Communication in a Public World. Prentice-Hall PTR. 1995.
- [Sta95]: Stallings, W. *Network and Internetwork Security*. Prentice-Hall International, 1995.