Redes de computadoras

Seguridad de red

Las diapositivas están basadas en en libro:
“Redes de Computadoras – Un enfoque descendente”
de James F. Kurose & Keith W. Ross

Seguridad de red

La seguridad de red apunta a una comunicación “Segura”

Se desea que los mensajes lleguen del emisor al receptor de modo tal que:

- Solo el receptor pueda entender el mensaje
- Que el emisor sea quien dice ser
- Que el contenido del mensaje no fue alterado
- Garantías para la posibilidad de comunicación

Seguridad de red

Confidencialidad

Sólo el emisor y el receptor deseado deberán comprender el contenido de los mensajes transmitidos.

Los mensajes son cifrados de algún modo para que no puedan ser entendidos por un interceptor.

Autenticación

Tanto el emisor como el receptor deberán poder confirmar la identidad del otro en el proceso de comunicación.

Confirmar que el otro es de hecho quien dice ser.

Seguridad de red

Integridad del mensaje

Aún existiendo una autenticación un mensaje podría ser modificado en el camino por un tercero.
Técnicas similares a las de suma de comprobación son utilizadas para garantizar la integridad del mensaje.

Seguridad operacional

Es deseable tener ciertas garantías de acceso al sistema de comunicación. En la actualidad es necesario tomar medidas para mantener operativo los servicios, a salvo de posibles ataques de denegación de servicios o intrusos maliciosos

Seguridad de red

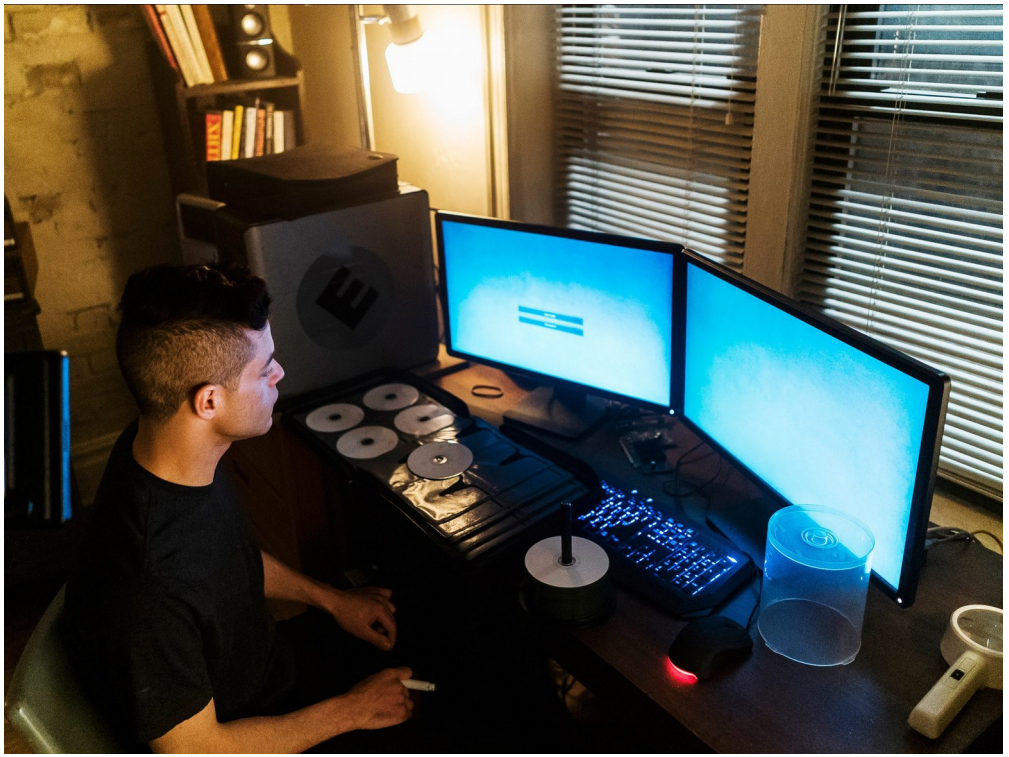
Un intruso podría:

Escuchar las comunicaciones

Robando contraseñas y datos

Suplantar la identidad de un emisor.

Denegar el servicio a usuarios legítimos.



Principios de criptografía

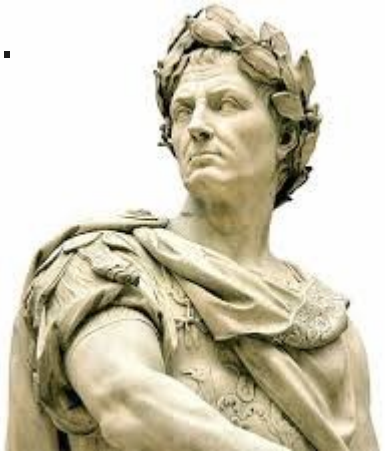
Las técnicas criptográficas permiten a un emisor ocultar los datos de modo que intrusos no puedan recuperarlos en caso de interceptarlos.

La criptografía se remonta a la época de Julio César

El mensaje en formato original
se conoce como **“texto plano” plaintext.**

En la actualidad muchas técnicas de cifrado
son una técnica conocida “estándar” y no un secreto.

Pero sí existe un elemento secreto que
se utiliza para descifrar los datos transmitidos.
Esto se denomina como clave. **key**



Principios de criptografía

El emisor cuenta con una clave Ka, una cadena de números o caracteres como entrada de un algoritmo de cifrado.

El algoritmo toma la clave y el mensaje en texto plano como parámetros de entrada.

Lo retornado será el mensaje cifrado.

Así mismo ocurre con un algoritmo de descifrado, el que recibe el texto cifrado y una clave Kb como parámetros de entrada y retorna el texto plano.

En caso de las claves para uno y otro procedimiento ser las mismas se dice que es un **sistema de clave simétrica**.

En caso de ser claves diferentes la cual una es conocida por el emisor y otra por el receptor, es un **sistema de clave pública**.

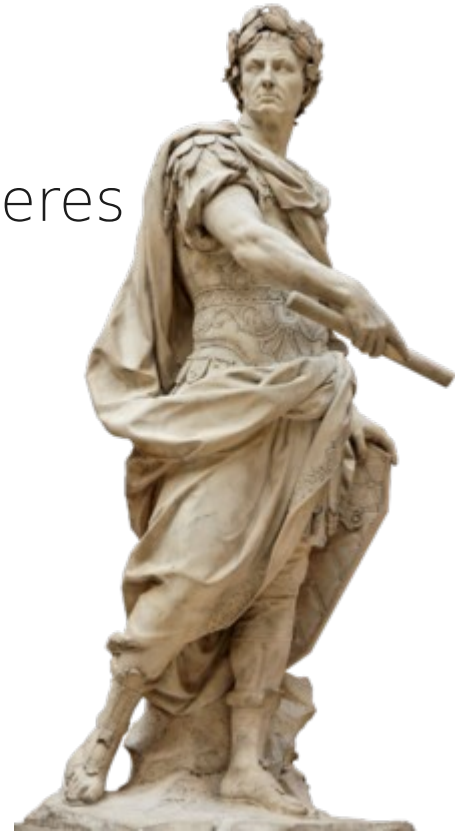
Criptografía de clave simétrica

El primer mecanismo de criptografía se le atribuye a Julio César

(conocido como el cifrado César)

Consistía en realilzar un desfasaje de los caracteres por un número k.

En caso de un k=3 la letra “a” encriptada se representaría por la “d”.



Criptografía de clave simétrica

Una mejora de este algoritmo es el cifrado monoalfabetico.

En este caso cada letra tiene su correspondiente cifrado, así se sustituye una letra por otra.

En este caso la palabra “hola”
se podría representar como “akgm”

Plaintext letter:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext letter:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

Figure 8.3 ♦ A monoalphabetic cipher

Criptografía de clave simétrica

El **cifrado monoalfabetico** es una gran mejora con respecto al cifrado César, en el primero un **ataque de fuerza bruta** debería probar 27 combinaciones mientras que con un cicfrado monoalfabetico las posibilidades aumentan en el rango de 10^{27}

De todos modos ambos algoritmos tienen una gran debilidad cuando se emplea análisis de sintaxis, conociendo que determinadas letras se repiten con frecuencia y viendo patrones en el mensaje podría ser fácil determinar algunas palabras y así romper el cifrado.

Criptografía de clave simétrica

Hace unos 500 años se desarrollaron técnicas para mejorar estos mecanismos, el **cifrado polialfabetico** funciona de modo en que se utilizan multiples cifrados monoalfabeticos cada uno con su particular codificación.

La idea es que una misma letra en caso de aparecer más de una vez no sea cifrada del mismo modo.

Se podría tener dos cifrados César con k=3 y k=7, de modo que se utilizará un patron C1, C2, C2, C1, C2... para las apariciones de los caracteres.

La primera vez que aparezca una letra se cifrará con el cifrado C1, la segunda con el C2, nuevamente con el C2, C1 y así...

Plaintext letter:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
$C_1(k = 5)$:	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
$C_2(k = 19)$:	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

Criptografía de clave simétrica

Los ataques a un cifrado se suelen clasificar teniendo en cuenta la información que posee el atacante.

Ciphertext-only attack: El atacante sólo posee el texto cifrado interceptado.

Know-plain-text attack: El atacante tiene la certeza de que determinadas palabras se encuentran presentes en el mensaje y puede determinar pares de palabras (texto-plano, cifrado)

Chosen-plain-text attack: El intruso es capaz de encriptar un mensaje.

Ej: “The quick brown fox jumps over the lazy dog,”

Mientras más sofisticado sea un algoritmo de cifrado menos probable de que un ataque de este tipo pueda realmente romper el cifrado.

Criptografía de clave simétrica

Cifrado de bloques

En la actualidad se divide el mensaje en palabras de k bits denominados **bloques** que son cifrados de forma independiente.

Para esto se utiliza una “tabla”, en la práctica la utilización de una tabla resulta inaplicable para cifras realmente seguras, más de 64bits

La implementación es mediante una función que simula una tabla.

Protocolos que utilizan el cifrado de bloque en la actualidad:

- DES
- 3DES
- AES

Clave pública

Desde la época del cifrado de César hasta la década de los 70, se requería el **intercambio de una clave compartida** para lograr un cifrado.

En esta época surge una nueva técnica en la que se cuenta con dos claves **K-** (clave privada) y **K+** (clave pública), en donde **K-** será privada y **K+** será publica y visible para todos, incluso para potenciales intrusos.

Para la comunicación el emisor utilizará la clave **K-** del receptor para cifrar el mensaje, y posteriormente el receptor utilizará su clave privada para descifrarlo.

Clave pública

Para realizar el cifrado y descifrado se utiliza un algoritmo estándar y públicamente conocido.

Las propiedades de las llaves son tales que:

$$K-(K+(m)) = K+(K-(m)) = m$$

A su vez este sistema de cifrado debe ser inmune a los ataques chosen plain-text-attack, ya que cualquier sujeto puede mediante la clave pública cifrar un mensaje y analizarlo.

Protocolos que utilizan el sistema de clave pública son entre otros:

- Diffie-Hellman Key Exchange
- RSA
- Ellis

Clave pública
RSA

RSA hace un uso extensivo de aritmética de módulo, en combinación de números primos, de modo de generar identidades.

Los elementos principales son:

- La elección de las claves públicas y privadas
- Los métodos de cifrado des-cifrado

Este sistema tiene un costo muy elevado de computo en comparación a algoritmos de clave simétrica.

Clave pública
Claves de Sesión

En la práctica se utiliza RSA en combinación con claves simétricas.

- Se realiza una negociación e intercambio de clave con el uso de RSA.

- Posteriormente se utiliza la **clave de sesión** simétrica para cifrar el resto del mensaje.

RSA + (DES o AES)

Integridad del mensaje

La integridad de los datos provee la certeza de que el mensaje que recibimos es el mismo que fue enviado.

El mensaje no fue alterado en el camino.

Red con sistema de enrutamiento OSPF:
¿cómo asegura un router que el mensaje es confiable?

Receptor de un correo

Documentos de valor legal

- Veterinarios deben “firmar” documentos PDF.
- Facturación digital implica intercambio de comprobantes en tiempo real.

Funciones Hash

Una función Hash toma determinado mensaje **m** y lo procesa retornando un mensaje **H(m)** de tamaño fijo.

A ese resultado se le conoce como **hash**.

Las funciones Hash deben tener la propiedad tal que:

Para cualquier mensaje **x** e **y** tal que x != y → H(x) != H(y)

Funciones Hash

MD5

[RFC 1321]

Se agrega un uno y se realiza un padding de ceros hasta completar determinado tamaño, se le agrega el mensaje codificado en base 64 y se realiza un proceso de cifrado de a bloques.

SHA-1

160bit de digest, resumen del mensaje.

Implementado por el gobierno de Estados Unidos y obligatorio en la encriptación de los archivos Federales.

Codigo de mensaje

- Se crea un mensaje y se aplica un algoritmo hash H(m), por ejemplo SHA-1

- Se agrega el hash h al mensaje y se envía el mensaje y el hash al receptor (m, h)

- El receptor al recibir el mensaje puede verificar la integridad del mensaje H(m) = h

Un tercero podría generar un mensaje m' y realizar el mismo proceso, el receptor recibiría un mensaje m' con un hash h' el cual H(m') = h'

Codigo de mensaje

Para solucionar este problema se utiliza un secreto compartido

De modo que se sume al mensaje para generar un hash particular denominado MAC (message authentication code).

Se calcula el hash:

$H(m + s) = h$

Se envía junto con el mensaje:

$(m, H(m + s)$

Firma Digital

En las comunicaciones a distancia es requerido que el receptor pueda verificar la identidad del emisor, así como el emisor pueda garantizar el no repudio del mensaje enviado.

Dada las propiedades del par de claves privadas esto podría lograrse “firmando” el mensaje con la clave privada, de modo que se pueda verificar mediante el uso de la clave pública.

El procedimiento es costoso, por lo que lo que se firmará será el hash.