



## Tema 6 Seguridad en redes LAN y corporativas

**Tecnologías de red**  
Grado en Ingeniería Informática, Esp. Ing. de Computadores  
*Curso 2015/2016*

**Jesús Esteban Díaz-Verdejo**  
Departamento de Teoría de la Señal, Telemática y Comunicaciones  
E.T.S. Ingenierías Informática y Telecomunicación – Universidad de Granada  
C/ Periodista Daniel Saucedo Aranda, s/n - 18071 – Granada (Spain)  
Phone: +34-958 242304 / 05 - Fax: +34-958 243032 - Email: jedv@ugr.es





## Esquema

- 1. Introducción a la seguridad
  - 1.1 Seguridad en comunicaciones
- 2. Fundamentos de seguridad en redes
  - 2.1 Arquitectura de seguridad OSI
  - 2.2 Ataques a la seguridad
  - 2.3 Servicios de seguridad
  - 2.4 Mecanismos de seguridad
  - 2.5 Modelo de seguridad en redes
- 3. Seguridad de los sistemas en red
  - 3.1 Ataques y vulnerabilidades
  - 3.2 Gestión de la seguridad
  - 3.3 Despliegue de la seguridad
  - 3.4 Seguridad perimetral

Apéndice: Fundamentos de criptografía en redes

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

2

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016



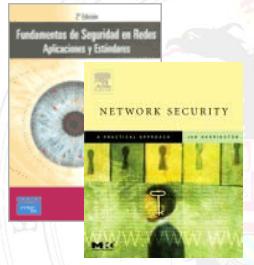
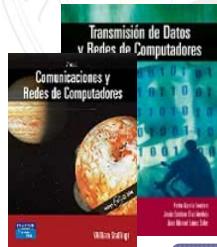
**Bibliografía**

**Básica**

- Stallings, w.; **Fundamentos de seguridad en redes, aplicaciones y estándares.** 2<sup>a</sup> ed.; Pearson (2004) ISBN: 978-84-205-4002-3
- Jan Harrington, **Network Security : A Practical Approach;** Morgan Kaufmann Pub. (2005), ISBN:123116333

**Complementaria**

- P. García Teodoro y otros; **Transmisión de datos y redes de computadores,** Pearson, 2003. ISBN: 84-205-3919-8 (**Tema 12**)
- Stallings, W.: **Comunicaciones y redes de computadores,** Prentice-Hall, 7<sup>a</sup> ed., 2004 ISBN: 84-205-4110-9 (**Tema 21**)

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

**Introducción a la seguridad**

## 1 Introducción a la seguridad

- *El arte de la guerra nos enseña a confiar no en la posibilidad de que el enemigo no venga, sino en nuestra propia disponibilidad para recibirlo: no en la oportunidad de que no ataque, sino en el hecho de que hemos logrado que nuestra posición sea inexpugnable*

**El arte de la guerra, SUN TZU**

**Internet**

- Millones de equipos interconectados
- Intercambio de todo tipo de información
- Múltiples servicios disponibles





6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Introducción a la seguridad

## 1 Introducción a la seguridad<sub>2</sub>

- Enorme complejidad

The diagram illustrates a complex network topology titled "The Teledatacom™ Network". It shows a central IP Network node connected to various other components via different interfaces. These include:
 

- Signaling Gateways:** Signaling System 7 (SS7) and Media Server Part 1 (MSP1).
- Transport Elements:** Softswitch, Application Server, IMS/Media Server, Router, and IP PBX.
- Core Elements:** IP Network, GGSN, and Billing System.
- Data Protocol Interface:** IP over ATM (IPOA), IP over SONET/SDH (IPoSONET/SDH), and IP over Ethernet (IPoE).
- Access Elements:** Wi-Fi, Enterprise Network, SIP Client, IP PBX, and Residential Gateway.
- Customer Premises Equipment:** IP Client, SIP Client, and IP PBX.

 The network also includes optical networking (WDM, DWDM), wireless networks (BTS, Node B, Wimax/WBn Base Station), and various protocol stacks like SS7, S2, S2i, S2a, and S2p.

Delegación de confianza

5 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015 Universidad de Granada

Introducción a la seguridad

## 1 Introducción a la seguridad<sub>3</sub>

- Intercambio de bloques de datos (paquetes)
- En red local

The diagram illustrates a local area network (LAN) topology. At the top, two nodes labeled A and B are connected to a central "Bus" line. Below the bus, a "Concentrador (hub)/Comutador (switch)" is shown, which is connected to several "Estaciones" (stations). Arrows indicate the flow of data between the stations and the hub. The stations are represented by computer icons with yellow warning signs. A small inset image shows a person's face with a digital circuit overlay.

6 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015 Universidad de Granada

Introducción a la seguridad

## 1 Introducción a la seguridad 4

Extremo a extremo

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

7 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015

Universidad de Granada

Introducción a la seguridad ▶ Seguridad en comunicaciones

### 1.1 Seguridad en comunicaciones

Evolución de la **seguridad de la información**:

- de la **protección física y administrativa** (documentos físicos)
- a la **seguridad informática** (documentos informáticos)
- Las redes introducen un elemento adicional: protección de la información **en tránsito**

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

8 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015

Universidad de Granada

Introducción a la seguridad ▶ Seguridad en comunicaciones

## 1.1 Seguridad en comunicaciones<sub>2</sub>

- **Seguridad informática:** nombre genérico que se da al grupo de herramientas diseñadas para **proteger los datos y evitar la intrusión** de los hackers
- **Seguridad de la red:** medidas de seguridad para **proteger los datos durante su transmisión**
- **Seguridad de la internet:** medidas para proteger los datos durante su **transmisión a través de una internet**
  - Fronteras difusas
  - Se suele denominar seguridad de la red o **seguridad en comunicaciones**
  - Consiste en medidas para disuadir, prevenir, detectar y corregir las violaciones de seguridad involucradas en la transmisión de información

9 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

Introducción a la seguridad ▶ Seguridad en comunicaciones

## 1.1 Seguridad en comunicaciones<sub>3</sub>

- **Seguridad en comunicaciones:**
  - Simplicidad aparente – Gran complejidad real
  - Diseño preventivo de la propia seguridad
  - Complejidad del diseño de servicios acorde a contramedidas (servicios poco intuitivos)
  - Despliegue: ubicación física y lógica
  - Interdependencias: claves (gestión de) y protocolos
  - Fuertes motivaciones económicas (cibercrimen)
  - Usabilidad / usuarios

10 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes ▶ Arquitectura de seguridad OSI

## 2.1 Arquitectura de seguridad OSI

- Complejidad en la definición de los requisitos de seguridad
- **Recomendación X.800** (ITU-T): define un enfoque sistemático
  - Visión general abstracta centrada en los ataques a la seguridad, los mecanismos y los servicios de seguridad
- Definiciones (RFC 2828)
  - **Amenaza:** *posibilidad de violación de la seguridad*, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad.
  - **Ataque:** *asalto a la seguridad* del sistema derivado de una amenaza inteligente: es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema

11 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes ▶ Arquitectura de seguridad OSI

## 2.1 Arquitectura de seguridad OSI<sub>2</sub>

- **Ataque a la seguridad:**
  - cualquier **acción** que comprometa la seguridad de la información
- **Mecanismo de seguridad:**
  - un mecanismo designado para **detectar, prevenir o recuperarse** de un ataque a la seguridad
    - Ningún mecanismo posibilita todas las funcionalidades requeridas
    - Casi todos los mecanismos de seguridad usan **técnicas criptográficas**
- **Servicio de seguridad:**
  - un servicio que **mejora la seguridad** de los sistemas de procesamiento de datos y de las transferencias de información. Un servicio de seguridad hace uso de uno o más mecanismos de seguridad

12 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

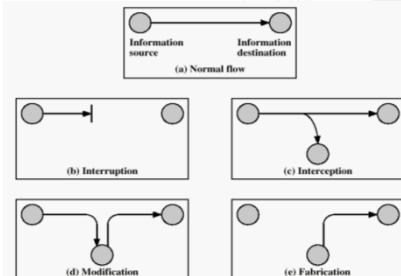
Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes ▶ Ataques a la seguridad

## 2.2 Ataques a la seguridad

 **Ataques a la seguridad**

- Tipos (X.800 y RFC2828)
  - Pasivos:** intentan conocer o hacer uso de información del sistema sin afectar a los recursos
  - Activos:** intentan alterar los recursos del sistema o afectar a su funcionamiento



Information source      Information destination

(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication

13

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

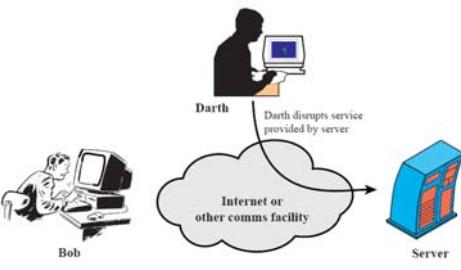
Fundamentos de seguridad en redes ▶ Ataques a la seguridad

## 2.1 Ataques a la seguridad <sub>2</sub>

 Cualquier acción que comprometa la seguridad de la información

Ataques	
Pasivos	Activos
Obtención de información	Análisis de tráfico
Modificación de mensajes	Suplantación de identidad
Repetición	Interrupción del servicio

- Ataques pasivos:** implican alguna observación del tráfico de datos, la trasmisión de datos, el objetivo es obtención de información



Darth

Darth disrupts service provided by server

Internet or other comms facility

Server

Bob

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

14

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad

**Definiciones:**

- **[X.800]** Servicio proporcionado por una capa de protocolo de sistemas abiertos de comunicaciones **que garantiza la seguridad adecuada** de los sistemas o de las transferencias de datos
- **[RFC2828]** Servicio de procesamiento o de comunicación proporcionado por un sistema para **dar un tipo especial de protección** a los recursos del sistema;
  - los servicios de seguridad **implementan políticas de seguridad y,**
  - son implementados, a su vez, **por mecanismos de seguridad**
- Previstos para contrarrestar los ataques la seguridad
- Replican funciones normalmente asociadas con los documentos físicos
  - Ej.: Firmas y fechas; protección frente a revelación, falsificación o destrucción; notariados o testificados; grabados o autorizados
- 5 categorías y 14 servicios en X.800

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

15

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad 2

<b>Confidencialidad/ privacidad</b> [↔ Cifrado (simétrico/asimétrico)]	<ul style="list-style-type: none"> <li>• <i>Protección de los datos frente a revelación no autorizada</i></li> </ul>
<b>Integridad</b> [↔ Funciones hash]	<ul style="list-style-type: none"> <li>• <i>Seguridad de que los datos recibidos son exactamente como los envió una entidad autorizada</i></li> </ul>
<b>Autenticación</b> [↔ Cifrado (simétrico/asimétrico)]	<ul style="list-style-type: none"> <li>• <i>Seguridad de que la entidad o entidades que se comunica/n son quien/es dice/n ser</i></li> </ul>
<b>Control de acceso</b>	<ul style="list-style-type: none"> <li>• <i>Prevención del uso no autorizado de una fuente</i></li> </ul>
<b>No repudio</b> [↔ Firma digital]	<ul style="list-style-type: none"> <li>• <i>Protección contra la negación, por parte de una de las entidades implicadas, de haber participado en toda o parte de la comunicación</i></li> </ul>
<b>Disponibilidad</b> [↔ ?]	<ul style="list-style-type: none"> <li>• <i>Protección de un sistema /servicio para asegurar su disponibilidad</i></li> </ul>

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

16

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad <sub>3</sub>

**Confidencialidad/privacidad**  
[↔ Cifrado (simétrico/asimétrico)]

- De la conexión
- No orientada a la conexión
- De campos seleccionados
- Del flujo de tráfico

**■ Protección de los datos frente a revelación no autorizada**

- Diferentes niveles de protección en función del contenido de una transmisión
- Protección del contenido de un solo mensaje, de un flujo de mensajes o de campos seleccionados de un mensaje.
- También protección frente a análisis de tráfico
  - Ocultación no sólo del mensaje sino también de la fuente, el destino, la frecuencia, la longitud, etc. de los mensajes

17

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad <sub>4</sub>

**Integridad**  
[↔ Funciones hash]

- De la conexión con recuperación
- De la conexión sin recuperación
- De la conexión de campos seleccionados
- No orientada a la conexión
- No orientada a la conexión de campos seleccionados

**■ Seguridad de que los datos recibidos son exactamente como los envió una entidad autorizada (sin modificación, inserción, omisión ni repetición)**

- Se puede aplicar a una serie de mensajes, a un solo mensaje a campos seleccionados de un mensaje
  - El nivel de protección es dependiente de ello
- Servicios con/sin recuperación: solo detección e informe o detección y recuperación de la integridad

18

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad 5

**Autenticación**  
[↔ Cifrado  
(simétrico/asimétrico)]

- De entidades origen y destino
- Del origen de los datos

 **Seguridad de que la entidad o entidades que se comunica/n son quien/es dice/n ser**

- En mensajes individuales basta con asegurar al receptor que el mensaje es de la fuente de que dice proceder
- En interacción continuada intervienen dos aspectos:
  - Inicio de la conexión: las dos entidades son auténticas (quienes dicen ser)
  - Protección frente a la intervención de la comunicación (man-in-the-middle)
- Dos tipos de autenticación: origen/destino y del origen de los datos

19

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016



Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad 6

**Control de acceso**

 **Prevención del uso no autorizado de una fuente**

- Quién puede tener acceso a una fuente
- En qué condiciones se puede producir el acceso
- Qué tienen permitido los que acceden a la fuente

20

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016



Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad 7

**No repudio** [↔ Firma digital]

- Origen
- Destino

 **Protección contra la negación, por parte de una de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación**

- Capacidad para demostrar la participación en la comunicación
- Capacidad para demostrar la generación de mensajes individuales por la parte contraria
- Suele requerir una tercera parte confiable

21

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes > Servicios de seguridad

## 2.3 Servicios de seguridad 8

**Disponibilidad** [↔ ¿?]

 **Protección de un sistema para asegurar su disponibilidad**

22

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Fundamentos de seguridad en redes > Servicios de seguridad

### 2.3 Servicios de seguridad <sub>9</sub>

Servicio	Obtención del contenido	Ánalysis de tráfico	Suplantación	Repetición	Modificación	Interrupción
Autenticación origen/destino						
Autenticación origen						
Control de acceso						
Confidencialidad		■				
Confidencialidad flujo de tráfico		■				
Integridad de los datos				■	■	
No repudio						
Disponibilidad						■

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

23

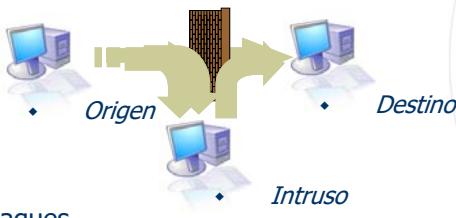
6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

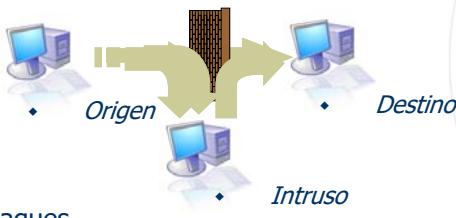
Universidad de Granada

Fundamentos de seguridad en redes > Servicios de seguridad

### 2.3 Servicios de seguridad <sub>10</sub>

 Ataques por sus **efectos** (en función de los servicios de seguridad)

- Finalidad de los equipos/sistemas: proporcionar información
- Ataques
  - Interrupción** (disponibilidad)
  - Intercepción** (confidencialidad)
  - Modificación** (integridad)
  - Fabricación** (autenticidad)



- Confidencialidad
- Integridad
- Autenticidad
- Disponibilidad
- No repudio

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

24

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Fundamentos de seguridad en redes ▶ Mecanismos de seguridad

## 2.4 Mecanismos de seguridad

**Mecanismos específicos**

- Cifrado
- Firma digital
- Control de acceso
- Integridad de los datos
- Intercambio de autenticación
- Relleno del tráfico
- Control de encaminamiento
- Notarización

**Mecanismos generales**

- Funcionalidad fiable
- Etiquetas de seguridad
- Detección de acciones
- Informe para la auditoría de seguridad
- Recuperación de la seguridad

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

25

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Fundamentos de seguridad en redes ▶ Mecanismos de seguridad

## 2.4 Mecanismos de seguridad<sub>2</sub>

Servicio	Cifrado	Firma digital	Control de acceso	Integridad de los datos	Intercambio de autenticación	Relleno del tráfico	Control de encaminamiento	Notarización
Autenticación origen/destino								
Autenticación origen	X							
Control de acceso			X					
Confidencialidad	X							
Confidencialidad flujo de tráfico					X	X		
Integridad de los datos	X			X				
No repudio		X						
Disponibilidad						X		

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

26

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Fundamentos de seguridad en redes ▶ Modelo de seguridad en redes

## 2.5 Modelo de seguridad en redes

**Elementos:**

- Mensaje, interlocutores, canal de información, protocolos de comunicación

Sender → Security-related transformation → Secret information → Secure message → Information Channel → Secure message → Security-related transformation → Secret information → Recipient

Trusted third party (e.g., arbiter, distributor of secret information)

Information Channel

Opponent

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

27

Universidad de Granada

Fundamentos de seguridad en redes ▶ Modelo de seguridad en redes

## 2.5 Modelo de seguridad en redes 2

**Elementos:**

- Transformación relacionada con la información
- Información secreta compartida entre los interlocutores

Sender → Security-related transformation → Secret information → Secure message → Information Channel → Secure message → Security-related transformation → Secret information → Recipient

Trusted third party (e.g., arbiter, distributor of secret information)

Information Channel

Opponent

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

28

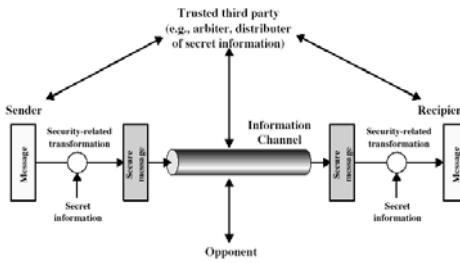
Universidad de Granada

Fundamentos de seguridad en redes ▶ Modelo de seguridad en redes

## 2.4 Modelo de seguridad en redes 3

 El uso del modelo requiere:

- El diseño de un **algoritmo** para llevar a cabo la **transformación** relacionada con la seguridad
- **Generar la información secreta** que deba ser usada con el algoritmo
- Desarrollar métodos para **distribuir y compartir** la información secreta
- Especificar un **protocolo** para los dos interlocutores que hagan uso del algoritmo de seguridad y la información secreta para obtener un servicio concreto de seguridad



Technologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

29

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red

## 3 Seguridad de los sistemas en red

 Terminología

- Conceptos básicos:
  - **Sistema seguro** → sistema fiable (en el sentido de los serv. seguridad)
  - **Amenaza** → posibilidad de violación de la seguridad
  - **Ataque** → atentado contra la seguridad (según serv. seguridad)
  - **Hacker (white hat)** → acción intrusiva
  - **Cracker (black hat)** → acción destructiva
  - **Pirata informático** → acción lucrativa
  - **Phreaker** → acción sobre sistema telefónico (fijo/móvil) y comunicaciones inalámbricas
- Metodologías relacionadas con ataques:
  - **Scanning** → rastreo/exploración
  - **Sniffing** → “olfateo”
  - **Spoofing** → suplantación
  - **Phising** → adquisición fraudulenta de información
  - **Flooding** → inundación

Technologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

30

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red

### 3 Seguridad de los sistemas en red<sub>2</sub>

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

ataque      defensa

- Herramientas involucradas en la seguridad:
  - **Malware** → software malicioso
  - **Virus** → software para inserción (y propagación) de código
  - **Gusano** → virus auto-ejecutable y auto-propagable
  - **Troyano** → puerta trasera (*backdoor*)
  - **Spyware** → recopilación de información (*p.e., cookies*)
  - **Dialer** → programa de tarificación adicional
  - **Rootkit** → ocultación de trazas de acciones
  - **Anti-{spyware,virus,troyano,...}** → software de lucha contra ataques
  - **Cortafuegos (firewall)** → filtro de tráfico
  - **Proxy** → dispositivo de paso intermedio
  - **VPN** → red privada virtual
  - **IDS** → detector de intrusiones
  - **Honey-{pots,nets}** → señuelos

31      6 - Seguridad en redes LAN y corporativas      Ver 1.1 - Enero 2015      Universidad de Granada

Seguridad de los sistemas en red

### 3 Seguridad de los sistemas en red<sub>3</sub>

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

- **Fallo de seguridad:** defecto en una aplicación software o un componente que, en las condiciones adecuadas, puede generar una vulnerabilidad
- **Vulnerabilidad:** conjunto de condiciones que permiten la violación de una política de seguridad implícita o explícita
- **Exploit:** software o técnica que utiliza una vulnerabilidad para violar una política de seguridad

32      6 - Seguridad en redes LAN y corporativas      Ver 1.1 - Enero 2015      Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Software malicioso

## Software malicioso

Programas dañinos (**malware**)

Programas dañinos						
Necesita programa anfitrión				Independiente		
Trampas	Bombas lógicas	Caballos de troya	Virus	Spyware	Gusano	Zombi

- Tienen como objetivo infiltrarse y atacar los sistemas
- Se aprovechan de vulnerabilidades en los sistemas, software y redes

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

33

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Software malicioso

## Software malicioso 2

Tipos de virus

Parásito	<ul style="list-style-type: none"> <li>Tipo tradicional</li> <li>Adjunto a archivos ejecutables</li> <li>Replicación al ejecutar</li> </ul>
Residente en memoria	<ul style="list-style-type: none"> <li>Alojado en memoria principal</li> <li>Parte de programa residente</li> </ul>
Sector de arranque	<ul style="list-style-type: none"> <li>Infecta registro de arranque</li> <li>Se extiende al arrancar el sistema</li> </ul>
Furtivo	<ul style="list-style-type: none"> <li>Diseño para evitar detección</li> </ul>
Polimórfico	<ul style="list-style-type: none"> <li>Capacidad de "mutar"</li> <li>No detectable mediante firmas</li> </ul>
Virus de macro	<ul style="list-style-type: none"> <li>Más abundantes actualmente</li> <li>Independientes de la plataforma</li> <li>Infección de documentos</li> </ul>

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

34

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

**Software malicioso** 3

The screenshot shows the Nuclear RAT 1.0 interface. It has a menu bar with Spy, Controls, Managers, Extras, Quick Menu, Languages, and About. Below the menu is a toolbar with icons for Connect, Connection Manager, Create Server, Share Server, and Check new version. The main window displays a list of connections under the heading 'Connections'. A sidebar on the left lists 'Virus', 'Gusanos', and 'Troya' with their respective descriptions.

**Virus**

- Reen
- Dest
- No a

**Gusanos**

- Capa
- Usan
- No p
- mem
- Cons

**Troya**

- Perr
- recabar información (espiar) o controlar remotamente la máquina anfitriona
- No necesariamente destructivo (ocultación)

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

© 2005-2014 - Jesús E. Díaz Verdejo

35

**Software malicioso** 4

The screenshot shows the Exploit Database website. It features a search bar at the top and a main content area with sections for 'Bombardeos lógicos', 'Exploits', and 'Rootkits'. To the right of the text blocks are two images: a black bomb with a USB cable and a cartoon illustration of a group of people climbing a flag.

**Bombas lógicas**

- Se activan al producirse un acontecimiento (fecha, combinación de teclas, condiciones técnicas)
- Permanecen ocultos hasta activarse

**Exploits**

- Software o fragmento de software destinado a aprovechar errores o vulnerabilidades en el software (o hardware)
- Vector de ataque

**Rootkits**

- Herramienta o grupo de herramientas cuya finalidad es esconderse a sí misma y a otros programas y archivos
- Acceso total al sistema (interposición)
- **Extremadamente peligrosos y difíciles de detectar/eliminar**

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

© 2005-2014 - Jesús E. Díaz Verdejo

36

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Software malicioso

## Software malicioso 5

**Backdoors**

- Permite evitar los mecanismos de seguridad en el acceso al sistema
- Entrada secreta

**Bots**

- Software que imita el comportamiento de un ser humano
- Recopilación de información / creación de cuentas / DoS

**Keyloggers**

- Registran las pulsaciones de tecla y las envían a través de Internet

**Hijackers (secuestradores)**

- Imposibilitan el acceso a datos/documentos/sistemas
- Se pide rescate
- (También redirección de peticiones)





Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

37

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Software malicioso

## Software malicioso 6

**Hoax**

En los próximos días, deben estar atentos: No abran ningún mensaje con un archivo anexo llamado "Invitación".

independientemente de quien se lo envíe. Es un virus que "abre" una antorcha olímpica que "quema" todo el disco duro C de la computadora. Este virus vendrá de una persona conocida que te tenía en su lista de direcciones. Es por eso que debes enviar este mail a todos tus contactos.

- No son virus ni tienen cap (por sí mismos)
- Mensajes de contenido falso: copias y enviarlas a contactos
- Recopilación de direcciones

**Dialers**

- Acceso a internet / llamadas

**Spyware**

- Recopilación de información sobre el sistema / actividades de usuario

**Adware**

- Publicidad intrusiva




Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

38

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Software malicioso

## Software malicioso 7

**Botnets**

- Redes de equipos que operan bajo el control de un equipo central
- **Extremadamente peligrosas**
- Amplia difusión

**Ingeniería social**

- Uso de psicología y "buenas maneras"

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

39

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas

**Delitos informáticos**

**Opera o que orden**

- No
- "Convoca a los intérpretes informáticos abusivamente"
- No

**FRAUDE INFORMATICO**

- Art. 255 CP
- "...utilizar telecomunicaciones ajenas..."
- Valiéndose de mecanismos instalados para realizar la defraudación.
- Alterando maliciosamente las indicaciones o aparatos contadores.
- Empleando cualesquiera otros medios clandestinos

**ESTAFAS INFORMATICAS**

- Art. 248 CP
- Transferencia patrimonial
  - Animo de lucro
  - Engaño bastante
  - Manipulación informática
- FABRICAR – POSEER – DISTRIBUIR

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

40

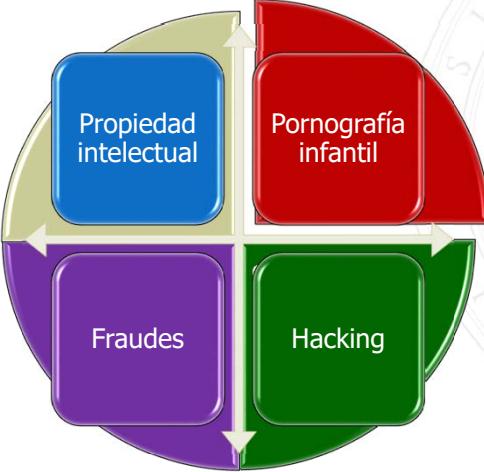
6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>2</sub>



**Tipología**

- Propiedad intelectual
- Pornografía infantil
- Fraudes
- Hacking

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

41

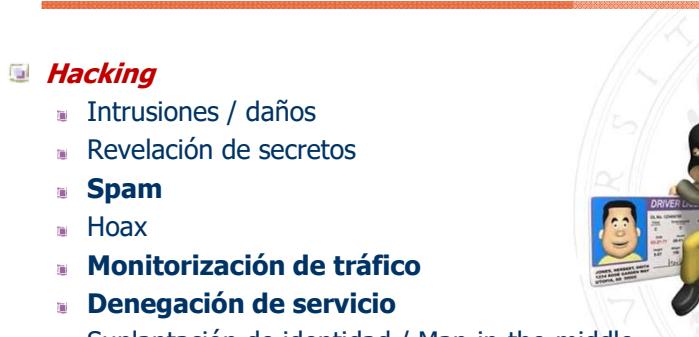
6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016



Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>3</sub>



**Hacking**

- Intrusiones / daños
- Revelación de secretos
- Spam**
- Hoax
- Monitorización de tráfico**
- Denegación de servicio**
- Suplantación de identidad / Man-in-the-middle





Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

42

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016



Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 4

**Spam**

- Correo no solicitado (correo basura)
- Fines normalmente publicitarios
- Se basan en el bajo coste de envío
- Saturación equipos/redes



All Mail  
Spam (254)  
Trash

43

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 5

**Monitorización de tráfico**

- Obtención de datos / análisis de tráfico
  - Navegación web, ubicación, etc.
- Habitualmente, creación de perfiles de usuario
  - Marketing / Publicidad dirigida
- Tema candente



6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>6</sub>

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

45

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>7</sub>

### Denegación de servicio

- Bloqueo de los servicios ofrecidos por un proveedor / servidor
  - Habitualmente mediante fuerza bruta

Distributed Denial of Service (DDoS) Attack

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

46

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>8</sub>

```

graph TD
    Fraudes[Fraudes] --- Social[Ingeniería social]
    Social --- Malware[Ingeniería técnica]
    Malware --- Fraudes
    Malware --- Skimming[• Malware  
• Hacking  
• Skimming]
    
```

**Fraudes**

- Engaños
- Suplantación identidad
- Habilidades sociales

**Ingeniería social**

- Malware
- Hacking
- Skimming

**Ingeniería técnica**

**UNCLE SCAM**

I WANT YOUR MONEY

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Universidad de Granada

47

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas <sub>9</sub>

```

graph LR
    Tipos[Tipos] --- Comercio[Comercio electrónico]
    Tipos --- Banca[Banca electrónica]
    Tipos --- Otros[Otros]
    
```

**Tipos**

**Comercio electrónico**

- Compras
- Premios
- Subastas

**Banca electrónica**

- Phising
- Pharming
- Man-in-the-middle

**Otros**

- Timos
- Loterías
- Donaciones
- ...

**Fraudes**

FREE MONEY

My Money went to NIGERIA and all I got was this lousy T-Shirt

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Universidad de Granada

48

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 10

**Compras**

CLIENTE                                  VENDEDOR

Ingeniería social (planificación)

**Fraudes**

CLIENTE                                  VENDEDOR

49

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 11

**Banca electrónica**

Phishing

SMShing

Robo de credenciales

Pharming

Man in the middle

**Fraudes**

Credit Card

John Smith  
1234 5678 9101 2345

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 12

Phishing

Fraudes

Diagrama que ilustra el ciclo del Phishing:

- Alojamiento de página → Retirada de dinero y envío
- Retirada de dinero y envío → Captación de mulas
- Captación de mulas → Obtención de claves
- Obtención de claves → Spam
- Spam → Alojamiento de página

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

51

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 13

Pharming

Fraudes

- Modificación DNS's
- Redireccionamiento
- Sitio duplicado
- Robo credenciales

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

52

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Prácticas maliciosas

## Prácticas maliciosas 14

**Man-in-the-middle**

Interceptación comunicaciones entre equipos

CLIENTE → BANCO ON-LINE

**Man-in-the-browser**

Fraudes

MANIPULACIÓN CREDENCIALES

INYECCIÓN CÓDIGO HTML

CLIENTE → NAVEGADOR → BANCO ON-LINE

53

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Fases de un ataque

## Fases de un ataque

1. Reconocimiento
  - Acceso / recopilación de información genérica o pública
2. Escaneado
  - Recopilación de información técnica
3. Acceso al equipo
  - Basado en aplicación o sistema operativo
    - Uso de vulnerabilidades
  - Basado en red (R2L)
4. Escalada de privilegios (U2R)
  - Adquisición de privilegios de administrador
5. Mantenimiento del acceso
  - Instalación de métodos de acceso alternativos
6. Ocultación
  - Evasión de mecanismos de detección y ocultación de pruebas

Reconocimiento

Escaneado

Acceso

Escalada de privilegios

Mantenimiento acceso

Ocultación

54

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Fases de un ataque

## Fases de un ataque 2



### Herramientas

- Mecanismos / conocimientos susceptibles de uso
  - Suplantación (*Spoofing*)
  - Acceso como administrador
  - Herramientas de DoS / DDoS
  - Software malicioso (*Malware*)
  - Ataques de contraseña (*password cracking*)
  - Acceso remoto
  - Explotación de vulnerabilidades de protocolos / sistemas (*exploits*)
  - Desbordamientos de buffer (*buffer overflows*)
  - Rootkits
  - Olfateadores (*Sniffers*)
  - Escaneadores (*Scanners*)
  - Acceso a la web
  - Manual de psicología
  - Paciencia

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

55

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Mitos

## Mitos de la seguridad en Internet



- **Privacidad** de las comunicaciones
- **Anonimato** (trazabilidad)
- Internet es **gratis**
- **5 mitos erróneos seguridad:**
  1. Es fácil detectar una computadora infectada.
  2. El email es la principal vía de infección.
  3. No se puede infectar una computadora sólo con visitar una página web.
  4. Los programas de intercambio de archivos son los grandes difusores de malware.
  5. Las páginas pornográficas son las más peligrosas

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

56

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red > Ataques y vulnerabilidades > Mitos

## Mitos sobre la seguridad 2

### Mitos (falsa sensación de seguridad)

- Tengo un software **antivirus**; eso es todo lo que necesito
- **No hay nada en mi ordenador** que pudiera querer un hacker
- Sólo los grandes servidores/grandes empresas son **objetivo** de los hackers
- Se necesita muchos **conocimientos tecnológicos** para ser un hacker
- **Mi proveedor** de Internet me da protección cuando estoy conectado
- Utilizo una **conexión telefónica**, no debo preocuparme
- Tengo un **Macintosh**
- Me siento seguro porque se que **hay un cortafuegos** que me protege de todo

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

57

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad

- Especificación de la filosofía y estructura de seguridad de una organización
- Finalidad
  - Planificación inversión y despliegue
  - Determinación de elementos sensibles y métodos de protección necesarios
  - Especificación de usos aceptables (lícitos) de los recursos computacionales
  - Especificación de derechos de acceso de los usuarios
  - Contrato de seguridad con los empleados
  - Instrucción de nuevos usuarios
- Coste / beneficio
- Revisiones periódicas
  - Detalles tecnológicos no incluidos en política
  - Aspectos legales

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

58

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad <sub>2</sub>

¿Qué debe considerar?

- Justificación de los gastos en seguridad
- Indicar el ámbito de actuación y los requisitos legales
- Especificar el personal relacionado con la seguridad, sus responsabilidades y su estructura
- Describir los comportamientos seguros que deben usarse (protocolos de uso de los recursos)
- Detallar los procedimientos para informar y gestionar las violaciones de seguridad
- Detallar los planes de contingencia y recuperación
- Plantillas disponibles (de pago y gratuitas)
  - <http://www.sans.org/resources/policies/#template>
  - [SANS Institute - The SANS Security Policy Project.htm](http://www.sans.org/resources/policies/#template)
  - [material\cleandeskpolicy-200808\\_01.doc](#)

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

59

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad <sub>3</sub>

Acciones divulgativas



**Not everything is as it seems**



**Trusting everything you see in an email is no different:**

- Microsoft is not giving \$1 million for forwarding the email
- Do not open any attachments you are not expecting, even if they are coming from someone you trust.
- Do not click on html links in suspicious looking emails
- Do not "unsubscribe" when you receive spam email
- Be suspicious of emails asking you to log into an account to "validate" your account, especially if it is a financial institution.

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

60

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad 4

Dan has left the office for the day, what did he forget to do?

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

61 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015 Universidad de Granada

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad 5

- Office keys should not be left out
- Sensitive FAX or call logs should be put away
- Passwords (pencil) should not be posted
- Portable media (CDs, flash drives) should not be left on the desk
- Laptop and cell phone should be kept secure
- Sensitive invoices should be put away
- Workstation screen should be locked
- Drinks should not be kept near workstations
- Documents and applications should be closed

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

62 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2015 Universidad de Granada

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad <sub>6</sub>



- Aspectos básicos:
  - Vulnerabilidades software
  - Gestión de *passwords*
  - Gestión de privilegios
  - Seguridad física
  - Uso de software desconocido
  - Educación usuarios
- Control de servicios:
  - Habilitación selectiva de servicios
  - Nivel de privilegios
  - Control de accesos
  - Análisis de vulnerabilidades
- Monitorización y rastreo

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

63

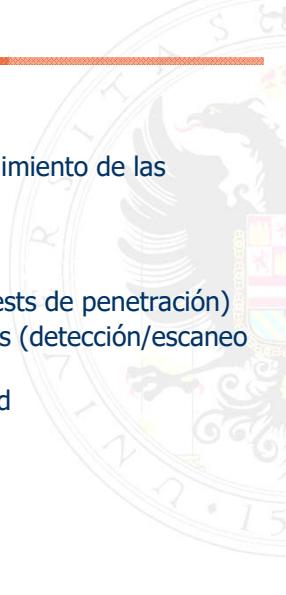
6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red > Gestión de la seguridad > Políticas de seguridad

## Políticas de seguridad <sub>7</sub>



- Auditorías de seguridad
  - Imprescindibles para garantizar el cumplimiento de las políticas de seguridad
  - Elementos:
    - Evaluación de riesgos
    - Comprobación de vulnerabilidades (tests de penetración)
    - Examen de vulnerabilidades conocidas (detección/escaneo de vulnerabilidades)
    - Verificación de la política de seguridad
  - Seguridad interna/externa

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

64

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

 Universidad de Granada

Seguridad de los sistemas en red > Despliegue de la seguridad

### 3.3 Despliegue de la seguridad

**Administración de la seguridad:**

- Arquitectura de seguridad de entornos de red:
  - Despliegue de los mecanismos de defensa en capas

1 <sup>a</sup> Capa	2 <sup>a</sup> Capa	3 <sup>a</sup> Capa
•Seguridad •periférica	•Autenticación	•Autorización
<b>Capa de seguridad de red</b>	<b>Prueba de identidad</b>	<b>Permisos basados en la identidad</b>
<ul style="list-style-type: none"> <li>➤ Comprobación de virus</li> <li>➤ Cortafuegos</li> <li>➤ Detección de intrusiones</li> <li>➤ Redes privadas virtuales</li> <li>➤ Protección de los servicios</li> </ul>	<ul style="list-style-type: none"> <li>➤ Usuario / clave</li> <li>➤ Sincronización de claves</li> <li>➤ Claves públicas</li> <li>➤ Testigos</li> <li>➤ Biométrica</li> </ul>	<ul style="list-style-type: none"> <li>➤ Permisos de usuario/grupo</li> <li>➤ Directorios de empresa</li> <li>➤ Administración de usuarios</li> <li>➤ Control de acceso basado en reglas</li> </ul>

65

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Despliegue de la seguridad

### 3.3 Despliegue de la seguridad 2

■ Capa 1 → **Seguridad periférica:**

```

graph TD
    SP[Seguridad periférica] --> SBBO[Seguridad basada en el ordenador]
    SP --> SBR[Seguridad basada en la red]
    SBBO --- CA[Corafuegos de acceso (local)]
    SBBO --- PS[Protección individual de los servicios]
    SBBO --- DV[Detcción de virus]
    SBR --- FA[Filtrado de acceso (Dir. Origen + puerto)(Wrappers)]
    SBR --- AS[Activación selectiva de servicios]
    SBR --- DV[Detención de vulnerabilidades]
    SBR --- O[Otros]
    CA --- FA
    CA --- AS
    CA --- DV
    CA --- O
    PS --- FA
    PS --- AS
    PS --- DV
    PS --- O
    DV --- FA
    DV --- AS
    DV --- DV
    DV --- O
  
```

66

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Despliegue de la seguridad

### 3.3 Despliegue de la seguridad

■ Capa 2 → **Autenticación:**

- Gestión de claves de acceso
- Testigos

■ Capa 3 → **Autorización:**

- Privilegios de los usuarios
- Administración de usuarios
- Control de acceso

■ Fases de la administración:

- **Prevención**
- **Detección**
- **Neutralización**

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

67 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Seguridad de los sistemas en red > Despliegue de la seguridad > Despliegue de redes

### 3.3 Despliegue de redes

■ Estructura básica de redes corporativas:

- **Zona pública:** *DMZ*
- **Zona privada:** *intranet*
- **Cortafuegos**
- **NAT**

Internet

• Acceso a Internet

• Router / cortafuegos de acceso

Zona pública (DMZ)

• Otros servicios

• WWW

• DNS, correo

• LAN pública

• Router / cortafuegos de intranet

• LAN privada

• Servicios intranet

• Estaciones de trabajo

Zona privada (intranet)

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

68 6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Seguridad de los sistemas en red ▶ Despliegue de la seguridad ▶ Despliegue de redes

# Despliegue de redes<sub>2</sub>

## Estructura jerárquica de redes corporativas:

Diagrama jerárquico de una red corporativa:

- Internet** se conecta a un **Router / cortafuegos de acceso**.
- Este router conecta a la **Red pública** y a la **Zona pública (DMZ)**.
- Red pública**:
  - Conectada a **Subred A** y **Subred B**, cada una con su propio **Router**.
  - Conectada a la **Zona pública (DMZ)** por un **Router**.
- Zona pública (DMZ)**:
  - Conectada a **Subred C** y **Router**.
  - Conectada a la **Red pública** por un **Router**.
- Router / cortafuegos de acceso** y **Router / cortafuegos de intranet** están conectados entre sí.
- Router / cortafuegos de intranet** conecta a la **Red pública** y a la **Zona privada (intranet)**.
- Zona privada (intranet)**:
  - Conectada a **Subred A**, **Subred B** y **Subred C**, cada una con su propio **Router**.

Tecnologías de red - **Curso 13/14**  
© 2005-2014 - Jesús E. Díaz Verdejo

69

6 - Seguridad en redes LAN y corporativas

Ver 1.1- Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

## 3.4 Seguridad perimetral

Elementos de monitoreo:

- Análisis
- Conversaciones
- Dominios
- Redes
- Ejemplos

Monitoreo:

WIRESHARK

Seguridad de los sistemas en red ▶ Seguridad perimetral

Seguridad de los sistemas en red > Seguridad perimetral > Cortafuegos

## Cortafuegos

- Filtrado selectivo de paquetes
  - En función de direcciones IP, puertos y/o aplicaciones
- Para establecer un cortafuegos se necesita (configuración mínima):
  - Un equipo con capacidad para actuar como enrutador
  - Dos interfaces de red
  - Desactivar el encaminamiento y reenvío IP
  - Conectar la red externa a uno de los interfaces
  - Conectar la red interna al otro interfaz
  - Instalar y configurar el software de cortafuegos
- De esta forma se obtienen dos redes que comparten un equipo

Red exterior ↔ Firewall ↔ Red Interior

6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

71

Seguridad de los sistemas en red > Seguridad perimetral > Cortafuegos

## Cortafuegos 2

- El equipo que actúa como cortafuegos puede acceder a las dos redes
  - Los ordenadores de la red exterior no pueden acceder directamente a los ordenadores de la interior y viceversa
  - En ambos casos es necesario acceder al cortafuegos
- Mejora en el nivel de seguridad:
  - Cualquier ataque a la red interior debe pasar primero por un ataque al cortafuegos
  - Es posible establecer varios criterios para permitir el paso de paquetes IP
- Un cortafuegos proporciona (habitualmente) tres funciones básicas:
  - **Filtrado**
  - **Enmascaramiento (NAT)**
  - **Estadísticas y trazas**

6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

72

Seguridad de los sistemas en red > Seguridad perimetral > Cortafuegos

## Cortafuegos 3

### Tipos de cortafuegos

- **Filtrado de paquetes**
  - Filtrado de paquetes TCP / UDP en función de combinaciones de direcciones origen/destino y puertos origen/destino
    - ◆ Independientes de la aplicación
  - Tipo más común
  - Limitaciones:
    - ◆ No se examina la carga útil
    - ◆ No se traza lo que le sucede al paquete tras atravesar el cortafuegos
- **Cortafuegos de sesión (stateful)**
  - Seguimiento de sesiones
- **Cortafuegos de aplicación**
  - Operan a nivel de aplicación proporcionando servicios de proxy para las aplicaciones
  - Ausencia de comunicación directa entre la aplicación y la red
  - Dependientes de la aplicación (un cortafuegos por aplicación)

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

73

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Seguridad de los sistemas en red > Seguridad perimetral > Cortafuegos

## Cortafuegos 4

### Filtros

- Determinan los paquetes que atraviesan el cortafuegos
- Hasta tres filtros:
  - Entrada (b)
  - Salida (b)
  - Retransmisión (f)
- Todo paquete desde el exterior al interior (o viceversa) debe atravesar los tres filtros
  - Los filtros de entrada protegen al propio cortafuegos
  - Los de salida limitan la conexión desde el cortafuegos hacia otras máquinas
  - Los de retransmisión limitan la actuación del cortafuegos como pasarela

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

74

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

## Cortafuegos – Ej. Outpost

**Outpost Firewall Pro (Service Mode) - configuración1.cfg**

Visor de registro de Outpost Firewall Pro

Hora de...	Nombre del proceso	Dirección	Protocolo	Dirección remota	Puerto remoto	Motivo
23:35:33	system	SALIENTE	UDP	192.168.1.255	NETBIOS_DGM	Permitir tráfico NetBIOS
23:35:33	system	ENTRANTE	UDP	192.168.1.4	NETBIOS_DGM	Allow local UDP connection
23:35:33	outlook.exe	SALIENTE	TCP	imap.ugr.es	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.ugr.es	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.telefonica...	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.telefonica...	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.telefonica...	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.telefonica...	IMAP	Microsoft Outlook IMAP co
23:35:33	outlook.exe	SALIENTE	TCP	imap.ugr.es	IMAP	Microsoft Outlook IMAP co
23:35:33	srvhost.exe	SALIENTE	UDP	80,59,61,250	DNS	General Host Process DNS
23:35:32	firefox.exe	ENTRANTE	TCP	localhost	30606	Allow local TCP connection
23:35:32	elrm.exe	ENTRANTE	TCP	localhost	1451	Eset NOD32 Service conn
23:35:32	elrm.exe	ENTRANTE	TCP	64.233.183.100	HTTP	Browser HTTP connection
23:35:32	svchost.exe	SALIENTE	UDP	80,59,61,250	DNS	Generic Host Process DNS
23:35:32	firefox.exe	SALIENTE	TCP	localhost	30606	Allow local TCP connection
23:35:32	elrm.exe	ENTRANTE	TCP	localhost	1452	Eset NOD32 Service conn
23:35:32	elrm.exe	ENTRANTE	TCP	51.ytimg.com	HTTP	Allow local TCP connection
23:35:32	elrm.exe	ENTRANTE	TCP	localhost	30606	Allow local TCP connection
23:35:32	elrm.exe	ENTRANTE	TCP	localhost	1441	Eset NOD32 Service conn
23:35:32	elrm.exe	ENTRANTE	TCP	localhost	1444	Eset NOD32 Service conn
23:35:32	firefox.exe	TCP	localhost	70006	Allow local TCP connection	

6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Tecnologías de red - Curso 13/14 © 2005-2014 - Jesús E. Díaz Verdejo

## IDS

**Seguridad perimetral:**  
■ Uso de cortafuegos  
→ insuficiente

Internet → Router / cortafuegos de acceso → LAN pública → Router / cortafuegos de intranet → LAN privada → Estaciones de trabajo

■ !Seguridad perimetral insuficiente!

6 - Seguridad en redes LAN y corporativas Ver 1.1 - Enero 2016 Universidad de Granada

Seguridad de los sistemas en red > Seguridad perimetral > IDS

## IDS<sub>2</sub>

**Detección de intrusiones:**

- Proceso de monitorizar los eventos en un equipo o red en busca de signos de intrusión
- Arte de detectar actividad inadecuada, incorrecta o anómala

**Sistema de detección de intrusiones**

- Autoexplicativo
  - Un administrador examinando trazas del sistema es un IDS
- Combinación de software y/o hardware que intenta realizar la detección de intrusiones
- **¿Intrusiones?**

77

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Seguridad perimetral > IDS

## IDS<sub>3</sub>

**Generación de alertas**

- Información en las alertas
- Número de alertas / severidad

**Diseño de un IDS**

- ¿Qué eventos son significativos?
- Técnicas a utilizar para la detección
  - Ocultación ataques
  - “0-day attacks”
  - Polimorfismo
- Rendimiento:
  - En términos de cantidad de **eventos procesados**
  - En términos de **capacidad de detección**
- Aspectos legales
- Punto de despliegue
- **iResposta!**
  - Intervención humana
  - Automatizada (utópica actualmente)

78

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Universidad de Granada

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

Seguridad de los sistemas en red > Seguridad perimetral > IDS

## IDS<sub>4</sub>

**Tipos**

- Múltiples clasificaciones posibles/propuestas
- Dos criterios (básicos):
  - Origen de la información
    - **HIDS:** *Host-based IDS*, información local del propio equipo
    - **NIDS:** *Network-based IDS*, información obtenida de la red (en tránsito)
  - Estrategia de análisis
    - Basados en **firmas**
      - ◆ Comparación con bases de datos de "firmas" de ataques conocidos
    - Basados en **anomalías**
      - ◆ Detección de comportamientos "sospechosos"
      - ◆ Capacidad teórica para detectar nuevos ataques

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

79

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Seguridad de los sistemas en red > Seguridad perimetral > IDS

## IDS<sub>5</sub>

**La mayoría de los IDS comerciales usan detección basada en firmas**

- Mecanismos de actualización remota de las firmas

**Ejemplos de sistemas:**

- SNORT
- VCC/Tripwire
- NetRanger, de Wheelgroup
- Real Secure, de ISS
- G-Server, de Gilian Technologies

**La mayoría de los cortafuegos/antivirus incorporan algún mecanismo de detección basada en firmas**

- TruPrevent de Panda, Outpost, etc.

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

80

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Seguridad de los sistemas en red > Seguridad perimetral > IDS

## SNORT

- SNORT es un IDS basado en red y en firmas de dominio público
  - <http://www.snort.org>
  - Ampliamente difundido
- 4 modos básicos de operación
  - Modo “sniffer”
  - Modo de captura de paquetes
  - Modo de detección de intrusiones
  - Modo “inline” (IPS)
- Prestaciones básicas
  - Ligero: ocupa poca memoria, incluye un mecanismo muy eficiente de emparejamiento de patrones
  - Operación en tiempo real
  - Respuesta activa correctiva
  - Totalmente modular y extensible (módulos adicionales de terceros)
  - Portabilidad



6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

81

## Conclusiones

- Lo que no sabes puede dañarte
- Los cortafuegos son sólo el inicio
- No todos los intrusos están fuera
- Las personas son el punto más débil
- Las claves son inseguras
- Ellos te pueden ver pero tú no los puedes ver
- El software es vulnerable
- Las opciones por defecto son peligrosas
- Se necesita un ladrón para atrapar a otro ladrón
- Los ataques son cada vez más fáciles de realizar
- La protección frente a virus es insuficiente
- El contenido activo es más activo de lo que se supone
- La criptografía más segura de ayer es la más insegura de hoy
- La puerta trasera está siempre abierta
- No hay ataque inofensivo
- La información es la mejor defensa

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2016

Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo

82

**Tecnologías de red - Curso 13/14  
© 2005-2014 - Jesús E. Díaz Verdejo**

## La evolución de la especie

BRINGING CIVILIZATION TO ITS KNEES...

The cartoon illustrates the 'evolution of civilization' through four panels:

- Goths:** A warrior with a horned helmet and a sword labeled 'HACK' is shown.
- Vandals:** A warrior with a sword labeled 'HACK HACK HACK' is shown.
- Huns:** A warrior with a sword labeled 'HACK HACK' is shown.
- Geeks:** A person with glasses and a computer monitor labeled 'HACK HACK HACK HACK' is shown.

**83**

6 - Seguridad en redes LAN y corporativas

Ver 1.1 - Enero 2015

Universidad de Granada

**Tecnologías de red  
Jesús Díaz Verdejo  
Dpto. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada**

## Fundamentos de criptografía

### Esquema

- Fundamentos de criptografía**
  - Introducción
  - Evolución histórica
  - Cifrado simétrico (o de clave privada)
  - Cifrado asimétrico (o de clave pública)
  - Autenticación de mensajes
  - Firmas digitales

**Apéndice. Fundamentos de criptografía en redes**

Universidad de Granada

**Introducción**

- **Criptografía**
  - proviene del griego *krypto* «oculto» y *graphos*, «escribir»
  - técnicas que permiten modificar un mensaje (en apariencia, no en contenido) para convertirlo en otro de manera que un usuario ajeno no pueda descifrarlo si no conoce la **clave** apropiada.

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

 Universidad  
de  
Granada

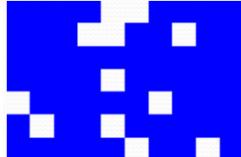
Apéndice. Fundamentos de criptografía en redes

**Introducción**  
**Ejemplos**

- Transposición
 

buenas tardes  
CVFÑBT UBSEFT
- Uso en esteganografía
 

T E A M A R E  
H A S T A E L  
F I N D E L  
M U N D O  
M I C O R A Z O N  
A Ñ O R A T U  
P R E S E N C I A




Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

 Universidad  
de  
Granada

Apéndice. Fundamentos de criptografía en redes

**Introducción**

■ Elementos del modelo de **cifrado simétrico**

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

■ **Principio de Kerckhoff:** Todos los algoritmos son públicos; sólo las claves deben ser secretas

■ Dos técnicas básicas: **transposición** y **sustitución**

Apéndice. Fundamentos de criptografía en redes

**Introducción**

**Cifrado por sustitución**

- Unidades de texto plano son **sustituidas** con texto cifrado siguiendo un sistema regular
  - las "unidades" pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros.
  - El receptor descifra el texto realizando la sustitución inversa.
- Cambio de cada letra o cada bit

a	b	c	d	e	f	g	h	i	j	k	l	m
Q	W	E	R	T	Y	U	I	O	P	A	S	D
n	o	p	q	r	s	t	u	v	w	x	y	z
F	G	H	J	K	L	Z	X	C	V	B	N	M

Texto plano      estecifradoesindestructible  
 Texto cifrado    TLZTEOYKQRGTLOFRTLZKXZOWST

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Introducción**

## Cifrado por transposición

- Las unidades del texto plano son cambiadas usando una **ordenación diferente** y normalmente bastante compleja
  - las unidades en sí mismas no son modificadas
- Ejemplo de cifrado por transposición

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Temática y Comunicaciones, Universidad de Granada

**Texto plano**  
please transfer one million dollar  
stom swiss bank accounts six two two

**Texto cifrado**  
AFLLSKSOSELAWAIAATOOSCTCLNMOMANT  
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

**Método de descifrado**

- Conocer el tipo de cifrado
- Conocer el número de columnas
- Reordenar las columnas

**MILLION DOLLARS**

**Apéndice. Fundamentos de criptografía en redes**

**Introducción**

## Criptoanálisis

- Ataques:** decodificación de mensajes sin disponer de la clave
  - Criptoanálisis:** explota las características del algoritmo para intentar deducir un texto nativo o la clave
    - Se puede disponer de conocimiento sobre características generales del texto nativo o incluso de pares de texto nativo y plano.
    - Compromiso de todos los mensajes (pasados, presentes y futuros) si se deduce la clave.
  - Fuerza bruta:** prueba de cada posible clave sobre texto cifrado hasta obtener un texto plano
- Un algoritmo de cifrado se considera seguro si es resistente al criptoanálisis y el tiempo empleado para un ataque de fuerza bruta es muy elevado
  - Evolución de las capacidades de cómputo -> debilidad de algoritmos

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Temática y Comunicaciones, Universidad de Granada

**Apéndice. Fundamentos de criptografía en redes**

**Evolución Histórica**

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

- Primer uso documentado de una cifra con propósitos militares: *La guerra de las Galias*, de Julio Cesar.
- Cifra de *sustitución monoalfabética* de tres lugares (ROT<sub>3</sub>).
 

a b c d e f g h i j k l m n ñ o p q r s t u v w x y z	D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C
---	---

 Texto llano **veni vidi vici**  
 Texto cifr. **YHQL YLGL YLFL**
- Conforme comienza a utilizarse la criptografía, nace la ciencia opuesta: el **criptoanálisis**.

**Escítala (griegos)**

**Apéndice. Fundamentos de criptografía en redes**

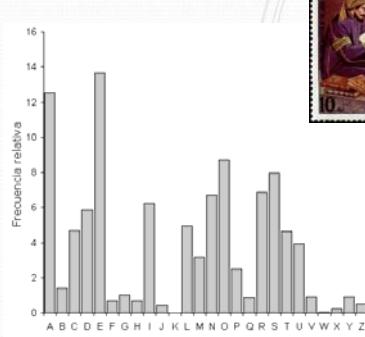



**Evolución Histórica**

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

- Descifrado: criptoanalistas árabes (Al Kindi).
- Amplio conocimiento estadístico, lingüístico y matemático.
  - Patrones lingüísticos, relaciones entre letras, análisis de frecuencia.
- Representando la freq. de las letras en el texto cifrado, y comparando con la distribución en el idioma original

**Apéndice. Fundamentos de criptografía en redes**




## Evolución Histórica

- Cifra de sustitución polialfabética (cifra Vigenère)

Tecnologías de red  
Jesús Díaz-Verdejo  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

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
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 A
B 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 A B
C C C D E 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 D E 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 E 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
F 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 F
G 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 F G
H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
Q Q R S 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 R S 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 S 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
T 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 T
U 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 T U
V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
X X Y Z 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 Y Z 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 Z 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

Leon Battista (s. XV).  
Blaise de Vigenère (s. XVI).

Clave      hielohielohielohi  
Texto Llano desvietropasalsur  
Texto cifr. KMWGLBVZDHAETGBZ

- s codificada como W, A y G.
- W codifica la s y la i.
- Inmune al análisis de frecuencia tradicional.

Apéndice. Fundamentos de criptografía en redes

## Evolución Histórica

- Descifrado: Friedrich Kasiski (1863).
- Descubrir la longitud de la clave a través de los *factores* de los espacios entre repeticiones.

Tecnologías de red  
Jesús Díaz-Verdejo  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Clave      KINGKINGKINGKINGKINGKING  
Texto Llano thesunandthemaninthemoon  
Texto cifr. DPRYEVNTNBUKWIAOXBUKWBT

Separación de 8 → factores 2 y 4.  
El M.C.D. será la longitud de la clave.  
Análisis de frecuencia a cada uno de los alfabetos.

Apéndice. Fundamentos de criptografía en redes

**Evolución Histórica**

Tecnologías de red  
Jesús Díaz Verdejo  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

- Solución: clave tan larga como el mensaje.
- Poco efectivo inventarse alguna → lista de palabras, letra de una canción, un verso ...
- Descifrado:

<b>Clave</b>	CANADABRAZILEGYPTCUBA	
<b>Texto Llano</b>	themeetingisatthedock	
<b>Texto cifr.</b>	VHRMHEUZNFQDEZRWFIDK	

- NUNCA reutilizar una clave.

Apéndice. Fundamentos de criptografía en redes

**Evolución Histórica**

Tecnologías de red  
Jesús Díaz Verdejo  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

- Mecanización de la criptografía
- Utilizada por los nazis en la II Guerra Mundial

Des... jewski, criptoanalista Polaco.  
etchley Park (sede GC&CS).

Apéndice. Fundamentos de criptografía en redes

## Cifrado simétrico

**■ Uso de la misma clave para cifrar y descifrar**

- La clave debe permanecer privada

**■ Elementos del modelo de cifrado simétrico**

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Temática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

## Cifrado simétrico Transmisión segura

- Requisitos para transmisión segura:
  - **Algoritmo de cifrado robusto:** el oponente debería ser incapaz de descifrar el texto o descubrir la clave incluso si poseyera varios textos cifrados junto a sus correspondientes textos planos
  - **Gestión de claves:** Emisor y receptor deben haber obtenido la clave de forma segura y ésta debe permanecer secreta
- Dos elementos a desarrollar/analizar:
  - Algoritmos de cifrado robustos
  - Mecanismos (protocolos) de distribución segura de claves
- Evolución algoritmos
  - DES ➤ 3DES ➤ RC5 ➤ AES ➤ Blowfish ➤ IDEA

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Temática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Cifrado simétrico**

## Algoritmos de cifrado

- **DES – Estándar de cifrado de datos**
  - Nace en enero de 1977 como estándar oficial de comunicaciones no secretas (gubernamental)
  - Clave de 56 bits ➤ Obsoleto
- Las partes principales del algoritmo son las siguientes:
  - fraccionamiento del texto en bloques de 64 bits (8 bytes),
  - permutación inicial de los bloques,
  - partición de los bloques en dos partes: izquierda y derecha, denominadas *I* y *D* respectivamente,
  - fases de permutación y de sustitución repetidas 16 veces (denominadas **rondas**),
  - reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Cifrado simétrico**

## Algoritmos de cifrado

- **3DES – Triple DES**
  - En 1979 nace una modificación de DES, Triple D
  - Repetición de DES tres veces con dos o tres claves únicas (longitud de 112 o 168 bits)
- $$C = E_{DES}^{k_3} \left( D_{DES}^{k_2} \left( E_{DES}^{k_1} (M) \right) \right)$$
- Modelo de encriptación
- Modelo de desencriptación

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Cifrado simétrico**

## Algoritmos de cifrado

- **AES – Advanced Encryption Standard**
  - Concurso para nuevo estándar en enero de 1997
  - Reglas del nuevo estándar:
    - El algoritmo debe ser un cifrado de bloques simétricos
    - Todo el diseño debe ser público
    - Deben soportarse las longitudes de claves de 128, 192 y 256 bits
    - Deben ser posibles las implementaciones tanto de SW como en HW
    - El algoritmo debe ser público o con licencia en términos no discriminatorios
  - Finalistas
    - Rijndael (de Joan Daemen y Vincent Rijmen, 86 votos)
    - Serpent (de Ross Anderson, Eli Biham y Lars Knudsen, 56 votos)
    - Twofish (de un equipo encabezado por Bruce Schneider, 31 votos)
    - RC6 (de los Laboratorios RSA, 23 votos)
    - MARS (de IBM, 13 votos)

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Cifrado simétrico**

## Algoritmos de cifrado

- Ejemplo de uso para clave de 128 bits
  - $2^{128} \approx 3 \times 10^{38}$  combinaciones diferentes
  - Operación en base a bloques de 128 bits (matriz cuadrada)
  - Almacenamiento en vector **estado**, que es modificado en cada etapa
- Operaciones de sustitución y transposición de bytes completos
- Elementos de partida

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

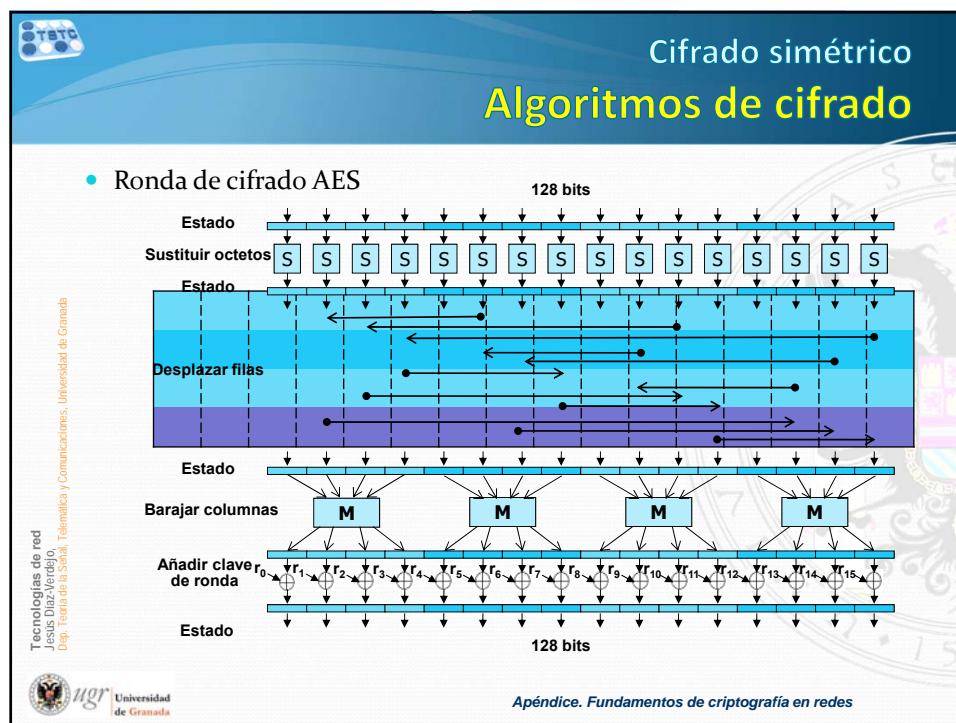
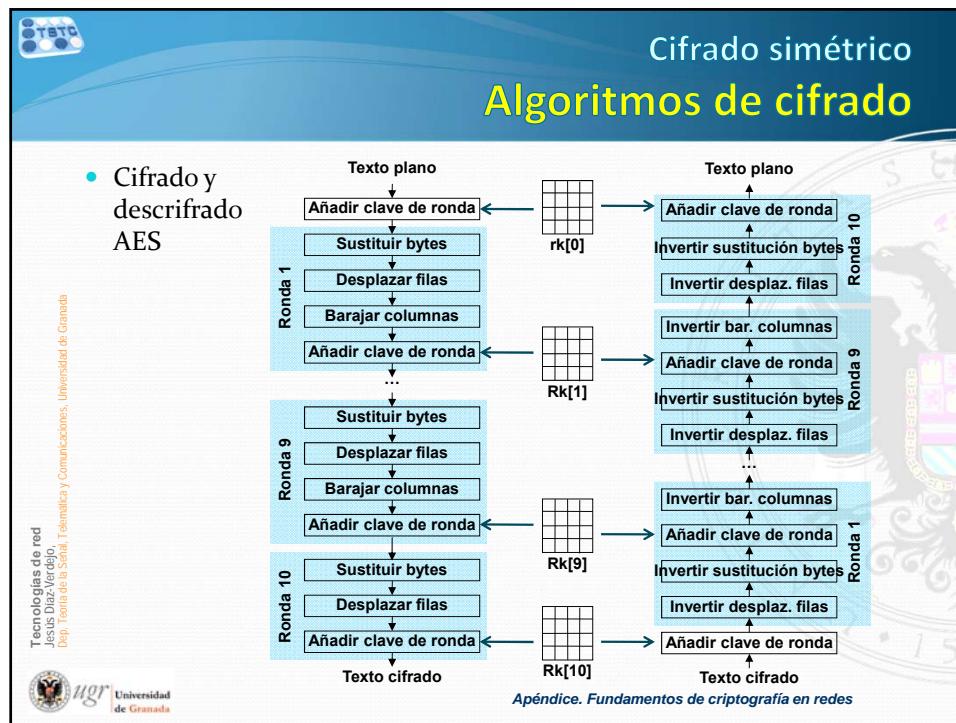
128 bits de texto plano

Clave de encriptación de 128 bits

rk[0] rk[1] rk[2] rk[3] rk[4] rk[5] rk[6] rk[7] rk[8] rk[9] rk[10]

ShiftRows

Apéndice. Fundamentos de criptografía en redes



**Cifrado simétrico**

## Algoritmos de cifrado

- Otros cifrados simétricos

Cifrado	Autor	Longitud de clave	Comentarios
Blowfish	Bruce Schneider	1 – 448 bits	Antiguo y lento
DES	IBM	56 bits	Muy débil
IDEA	Massey y Xuejia	128 bits	Bueno, pero patentado
RC4	Ronald Rivest	1 – 2048 bits	Algunas claves débiles
RC5	Ronald Rivers	128 – 256 bits	Bueno, pero patentado
Rijndael	Daemen y Rijmen	128 – 256 bits	La mejor opción
Serpent	Anderson, Biham	128 – 256 bits	Muy robusto
Triple DES	IBM	168 bits	Segunda mejor opción
Twofish	Bruce Schneider	128 – 256 bits	Muy robusto, muy utilizado

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

## Cifrado de Clave Pública

- Propuesto originalmente por Diffie, Hellman y Merkle.
- Supongamos que Alice quiere enviar un mensaje totalmente seguro a Bob:
  - Coge una caja fuerte, pone su candado y se la envía a Bob
  - Bob pone su propio candado y reenvía la caja fuerte a Alice
  - Alice quita el suyo y vuelve a reenviar la caja a Bob.
  - Finalmente Bob quita su candado, y puede leer el mensaje de forma segura.
- Enormes implicaciones: es posible intercambiar un mensaje seguro entre dos personas sin necesidad de intercambiar una clave.
- Funciones de una sola vía (aritmética modular)

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

## Cifrado de Clave Pública

- Claves de cifrado y descifrado diferentes

Tecnologías de red  
Jesús Díaz-Verdejo.  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

## Cifrado de Clave Pública

- Propiedades:

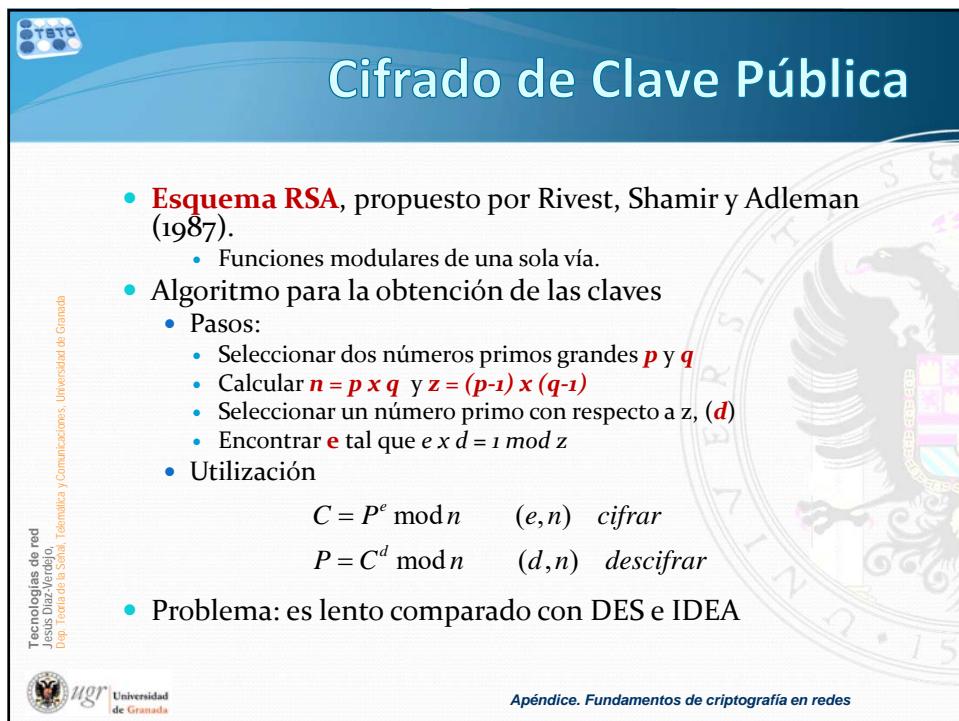
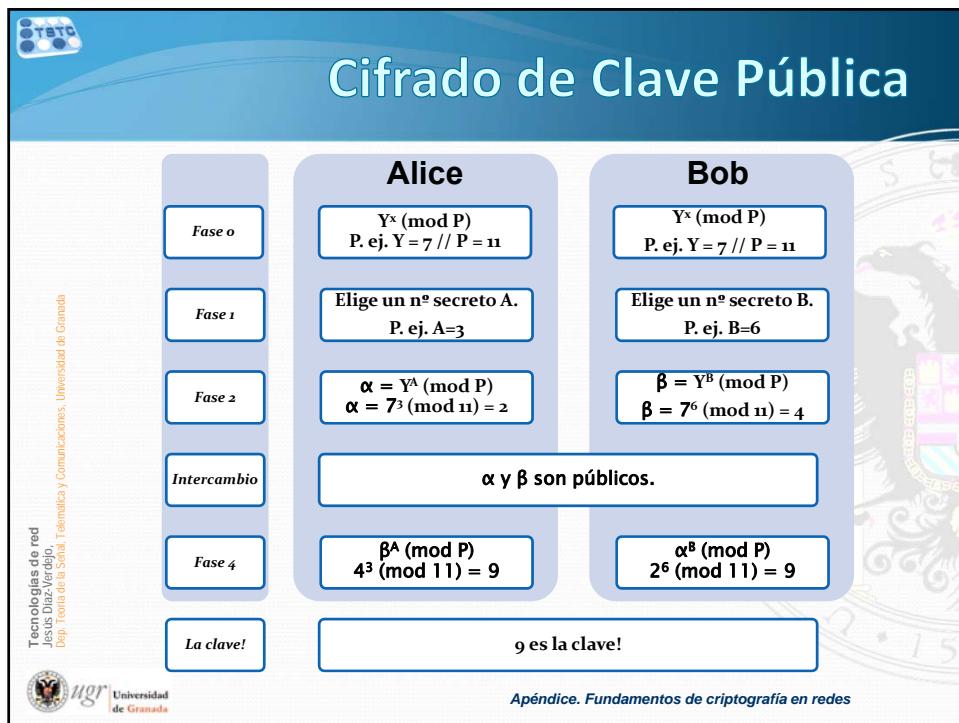
  - No es factible determinar la clave de descifrado a partir del algoritmo y la clave de cifrado
  - Cualquiera de las dos claves puede usarse para el cifrado y descifrado

- Uso:

  - Cada usuario genera un par de claves
  - Cada usuario publica una de las claves en un registro público (clave pública). La otra clave se mantiene secreta (clave privada)
  - Si Bob quiere mandar un mensaje privado a Alice, cifra con la clave pública de Alice.
  - Alice descifra con su clave privada. Sólo Alice puede descifrar.

Tecnologías de red  
Jesús Díaz-Verdejo.  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes



## Cifrado de Clave Pública

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

- Cifrador de bloque**, donde el texto llano ( $M$ ) y el cifrado ( $C$ ) son enteros entre 0 y  $n-1$ .

$$C = M^e \pmod{n}$$

$$M = C^d \pmod{n} = (M^e)^d \pmod{n} = M^{ed} \pmod{n}$$

- Las claves son:
  - Pública:  $KU = \{e, n\}$
  - Privada:  $KR = \{d, n\}$
- Requisitos:
  - Valores de  $e$ ,  $d$  y  $n$  tal que  $M^{ed} = M \pmod{n}$  para todo  $M < n$ .
  - Relativamente fácil calcular  $M^e$  y  $C^d$  para todo  $M < n$ .
  - Impracticable determinar  $d$  dados  $e$  y  $n$ .

Apéndice. Fundamentos de criptografía en redes

## Cifrado de Clave Pública

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Alice	
Fase 1	Elegir <b>p</b> y <b>q</b> primos enormes P. ej. $p = 17 // q = 11$
Fase 2	Calcular <b>n</b> = $p \times q$ $n = 187$
Fase 3	Calcular <b><math>\phi(n)</math></b> = $(p-1) \times (q-1)$ $\phi(n) = 160$
Fase 4	Seleccionar <b>e</b> (primo relativo y $< \phi$ ) P. ej. $e = 7$
Fase 5	Calcular <b>d</b> ( $< \phi$ y $d \cdot e \pmod{\phi} = 1$ ) $d = 23$
Cifrado	
Descifrado	$M = C^d \pmod{n}$ , entonces, si $C = 11$ $M = 11^{23} \pmod{187} = 88$

**KU = {e, n} = {7, 187}**  
**KR = {d, n} = {23, 187}**

**Bob**

$$C = M^e \pmod{n}, \text{ entonces, si } M = 88$$

$$C = 88^7 \pmod{187} = 11$$

Apéndice. Fundamentos de criptografía en redes

## Cifrado de Clave Pública

- Conceptos erróneos:
  - **Cifrado de clave pública más seguro que el de clave privada.**
    - Depende de la longitud de la clave y del esfuerzo computacional que requiera.
  - **Ha dejado obsoleto al cifrado de clave privada.**
    - Al contrario, pues necesita una carga computacional muy grande.
    - Esquemas híbridos: Clave pública para codificar la clave de sesión, y después clave privada.
- **Distribución de claves trivial comparado con la engorrosa negociación requerida en cifrado simétrico.**
  - Se necesita algún tipo de protocolo, y generalmente implica un agente central (tercera parte de confianza).

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

 Universidad  
de  
Granada

Apéndice. Fundamentos de criptografía en redes

## Distribución de claves y autenticación Cifrado Simétrico

- Proporciona **privacidad**
  - Ambas partes deben conocer la clave
  - Es necesario mantener la clave secreta
- Distribución de claves, posibilidades:
  - Bob selecciona y entrega físicamente la clave a Alice
  - Una tercera persona selecciona la clave y la entrega físicamente a ambos
  - Si Bob y Alice han usado una clave, intercambio de nueva clave cifrada con anterior
  - **Uso de conexiones cifradas con una tercera parte**
    - **Centro de distribución de claves (KDC)**

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

 Universidad  
de  
Granada

Apéndice. Fundamentos de criptografía en redes

**Distribución de claves y autenticación**  
**Cifrado Simétrico**

• Autenticación
 

- Verificación de la identidad del interlocutor

• Notación y funcionamiento básico:
 

- Protocolo de autentificación de dos vías más corto
- Escenario
  - Alicia y Bob
  - Trudy (intruso)

$X$  = identidad de  $X$   
 $R_X$  = random generado por  $X$   
 $K_{AB}(P)$  = texto  $P$  cifrado con clave secreta  $AB$

Diagrama de flujo:

```

graph LR
    Alice[Alice] -- 1 --> Bob[Bob]
    Bob -- 2 --> Alice
    Alice -- 3 --> Bob
  
```

Apéndice. Fundamentos de criptografía en redes

Tecnologías de red  
 Jesús Díaz Verdejo  
 Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

UGR Universidad de Granada

**Distribución de claves y autenticación**  
**Cifrado Simétrico**

• Vulnerabilidad: Ataque por reflexión

Diagrama de flujo:

```

graph LR
    Trudy[Trudy] -- 1 --> Bob[Bob]
    Bob -- 2 --> Trudy
    Trudy -- 3 --> Bob
    Bob -- 4 --> Trudy
    Trudy -- 5 --> Bob
  
```

• Solución: se necesita un centro de distribución de claves (KDC) en el que ambas partes confían

Diagrama de flujo:

```

graph LR
    Alice[Alice] -- 1 --> KDC[KDC]
    KDC -- 2 --> Bob[Bob]
  
```

Apéndice. Fundamentos de criptografía en redes

Tecnologías de red  
 Jesús Díaz Verdejo  
 Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

UGR Universidad de Granada

**Distribución de claves y autenticación  
Cifrado Simétrico**

• Uso de KDC
 

- Dos tipos de clave
  - Clave de sesión
  - Clave permanente

1. Host sends packet requesting connection  
2. Front end buffers packet; asks KDC for session key  
3. KDC distributes session key to both front ends  
4. Buffered packet transmitted

FEP = front end processor  
KDC = key distribution center

Alice knows R1  
Bob knows R1  
Alice, Bob communicate using shared session key R1

**Apéndice. Fundamentos de criptografía en redes**

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

UGR Universidad de Granada

**Distribución de claves y autenticación  
Cifrado Simétrico**

• Needham-Schoeder (1987)

• Otway-Rees (1987)

**Apéndice. Fundamentos de criptografía en redes**

Tecnologías de red  
Jesús Díaz-Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

UGR Universidad de Granada

**Distribución de claves y autenticación**

## Cifrado asimétrico

- La clave pública debe poder atribuirse a su usuario
- **Certificados de clave pública**
  - Constan de una clave pública más un identificador de usuario
  - Firmado por una tercera parte de confianza
    - **Autoridad de certificación (CA)**
  - Certificados ofrecidos (publicados) por el usuario
    - Verificados por CA a partir de la firma
- **Infraestructura de clave pública (PKI)**
  - Problemas de gestión / actualización
  - Listas negras

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Distribución de claves y autenticación**

## Cifrado asimétrico

- **Autenticación con clave pública**
  - Basado en RSA, con intercambio de retos y establecimiento de una clave secreta:
  - Debilidad: obtención de las claves públicas

```

graph LR
    Alice[Alice] -- 1 --> E_B["E_B(A, R_A)"]
    E_B --> Bob[Bob]
    Bob -- 2 --> E_A["E_A(R_A, R_B, K_S)"]
    E_A --> Alice
    Alice -- 3 --> K_S["K_S(R_B)"]
    K_S --> Bob
  
```

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Autenticación de mensajes**

- Protección contra ataques activos
  - Se puede usar criptografía de clave privada
- Elementos:
  - Verificación del contenido del mensaje
  - Verificación de la fuente
  - Temporización de los mensajes
  - Secuenciación de los mensajes
- **Autenticación mediante cifrado simétrico**
  - Uso de la clave privada en exclusiva por las partes (autenticación de las partes)
    - Sólo las partes pueden cifrar/describir
  - Inclusión de código de corrección de errores y marcas temporales y/o número de secuencia
    - Protección contra manipulación de los mensajes

Tecnologías de red  
Jesús Díaz Verdejo.  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Autenticación de mensajes**

- **Autenticación de mensajes sin cifrado de mensajes**
  - Generación de una etiqueta de autenticación que se incorpora al mensaje
    - Los mensajes no son cifrados
    - Sólo se cifra la etiqueta de autenticación
- **Código de autenticación de mensajes (MAC)**
  - Uso de clave secreta para generar un pequeño bloque de datos (compendio) en función del mensaje
    - “Huella digital” del mensaje

Tecnologías de red  
Jesús Díaz Verdejo.  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

## Autenticación de mensajes

**• Funciones de dispersión de un solo sentido**

- Funciones hash para obtención del compendio
- Resumen de longitud fija
- No se usa clave secreta para generar el compendio
- Cifrado del compendio

**• Funciones de dispersión seguras**

- Funciones hash con propiedades seleccionadas
- Ej. SHA-1
- Uso en firmas digitales

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

(a) Using conventional encryption: A message is encrypted with a key K. The ciphertext is decrypted with the same key K to obtain the original message, which is then compared with the received message.

(b) Using public-key encryption: A message is encrypted with a private key  $K_{private}$ . The ciphertext is decrypted with a public key  $K_{public}$  to obtain the original message, which is then compared with the received message.

(c) Using secret value: A message is combined with a secret value (represented by a box) and then hashed to produce a digest. The digest is compared with the received digest to verify the message's integrity.

## Firma digital

• Proporcionan integridad, autentificación y no repudio

• Firmar digitalmente significa que:

- El receptor autentifica al emisor
- El emisor no repudia la autoría del documento
- El receptor no puede falsificar el mensaje

• Aproximación simple: cifrado de todo el mensaje con clave privada

• Alternativa sin cifrado del mensaje

- MD5/SHA

Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada

Apéndice. Fundamentos de criptografía en redes

**Firma digital**

- Firma con clave secreta:

```

graph LR
    Alice[Alice] -- "A, K_A (B, R_A, t, P)" --> BB[BB]
    BB -- "K_B (A, R_A, t, P, K_BB (A, t, P))" --> Bob[Bob]
  
```

- Firma con clave pública:

Transmission line

Alice's computer	Transmission line	Bob's computer
Alice's private key, $D_A$ $P \xrightarrow{E_B} E_B(P)$	↓	Bob's private key, $D_B$ $E_B(D_A(P)) \xrightarrow{D_B} P$
$D_A(P)$		$D_B(E_B(D_A(P)))$
$E_B$		$D_B$

*Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada*

*Apéndice. Fundamentos de criptografía en redes*

**Firma digital**

- Uso en estándares de transmisión segura
  - PGP (Pretty Good Privacy)

MD5 → ZIP → IDEA → BASE64

- SET (Secure Electronic Transaction)

MD5 → RSA(A, B) → BASE64

*Tecnologías de red  
Jesús Díaz Verdejo,  
Dep. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada*

*Apéndice. Fundamentos de criptografía en redes*