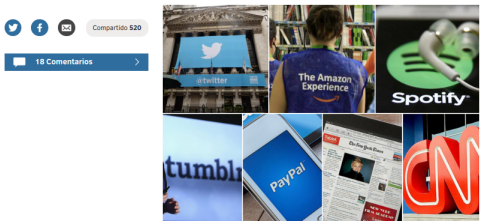
10.1. Amenazas de seguridad

- El usuario
- Programas maliciosos o malware
- Intruso
- Un siniestro (incendio, inundación, etc.)

Así se gestó el ciberataque más grave de los últimos 10 años



22/10/2016 14:10

Estados Unidos todavía se está recuperando del ciberataque perpretado este viernes y que dejó a millones de personas sin poder entrar en las webs más populares del mundo. Twitter, Spotify, Amazon, Reddit, Tumblr, PayPal, e incluso, las webs de medios tan importantes como 'The New York Times', 'Financial Times' o CNN, entre otros sufrieron una serie de ataques informáticos sucesivos que las dejaron K.O. durante horas.

Según la compañía, las primeras investigaciones apuntan a que el ataque provino de dispositivos conocidos como '**Internet of Things**' (interconexión digital de objetos cotidianos con Internet), tales como DVR, impresoras y otros aparatos conectados a la Red. Según la empresa Gartner, en 2020 habrá en el mundo aproximadamente 26.000 millones de dispositivos conectados.

http://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html

Virus: código escrito con la intención expresa de replicarse. Se adjunta a sí mismo a un programa o documento para propagarse de un equipo a otro. Puede dañar el hardware, el software o la información.

Gusano: se propagan sin necesidad de infectar ficheros y distribuye copias (posiblemente modificadas) de sí mismo por las redes.

Troyano: programa informático que parece ser útil pero que realmente provoca daños. No infecta ficheros ni se transmite solo.

Programa espía: se instala **furtivamente** en una computadora para recopilar información sobre las actividades realizadas en ella. No confundir con cookie

Bomba lógica: programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción.

Medidas:

- Antivirus y actualizaciones
- Desconfiar siempre
- Medidas antispam
- Programas: sólo los necesarios
- Ojo con algunas web

Hacker: experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware, etc.

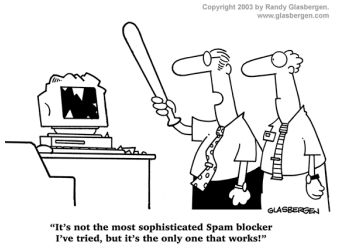
Cracker (CRiminal hACKER): persona que viola la seguridad de un sistema informático. La actividad es dañina e ilegal.

Defacer: alguien que cambia un sitio web sin permiso del administrador del sitio.

Trasher: busca en las papeleras información personal, de tarjetas de crédito, etc.

Phreaker (phone phreak): personas con conocimientos en teléfonos fijos y móviles. Desbloquean, clonan o programan móviles robados.

Phisher (fisher): intenta adivinar contraseñas llevando a sitios web falsos



Problemas de spam:

- Puerta de entrada de virus, troyanos, gusanos, phishing...
- Molestia y absorción de recursos

Medidas contra spam:

- No participar en cadenas de mail
- Usar campo CCO:
- No poner mail en webs ni dar dirección en cualquier parte
- Filtro anti-spam

http:www.10minutemail.com http:www.guerrillamail.com

Contraseñas

http://cert.inteco.es/Proteccion/Recomendaciones/Crear_una_contrasena_segura/

- La contraseña no debe contener el identificador o nombre de usuario de la cuenta, o cualquier otra información personal que sea fácil de averiguar (cumpleaños, nombres de hijos, conyuges, ...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (123456, qwerty...) No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.
- Se deben evitar contraseñas que contengan palabras existentes en algún idioma (por ejemplo Aguilanegra), uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en el diccionario y/o palabras de uso común.
- No se deben almacenar las contraseñas en un lugar público y al alcance de los demás.
- No compartir las contraseñas en Internet, por correo electrónico ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que te soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se trata de un fraude.

Contraseñas

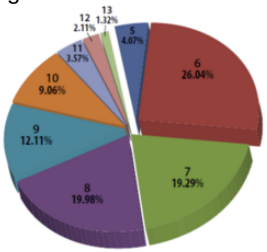
https://haveibeenpwned.com/

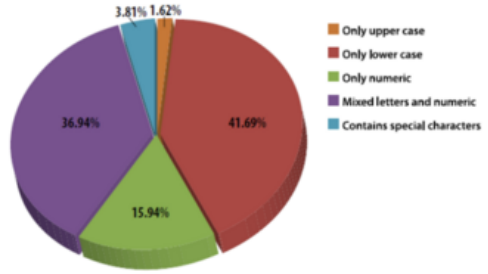
Incidente de seguridad en RockYou.com: 32.000.000 de contraseñas robadas en 2009

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Longitud:





Redes sociales

Identidad digital y derecho al olvido

Identidad digital: ¿quiénes somos en internet?

10.2. Seguridad en documentos y transacciones

Criptografía: del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida.

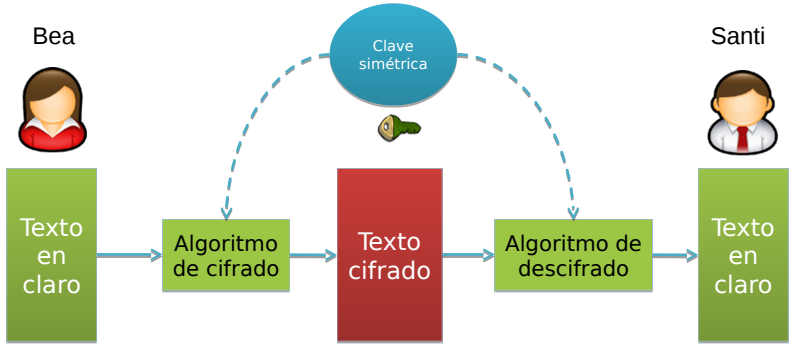
La criptografía se utiliza para enviar mensajes confidenciales o para almacenar información, y su propósito es que **sólo las personas autorizadas puedan entender el mensaje**.

CIFRAR **ENVIAR** **DESCIFRAR**

Problemas que resuelve la criptografía:

- **La privacidad**: la información solo puede ser leída por las personas autorizadas
- **La integridad**: la información no puede ser alterada en el transcurso del envío o el almacenamiento.
- **La autenticidad**: que se pueda confirmar la autoría del mensaje
- **El no rechazo**: que no se pueda negar la autoría de un mensaje enviado

Cifrado simétrico



- Bea cifra el mensaje con la clave.
- Santi descifra el mensaje utilizando la misma clave.

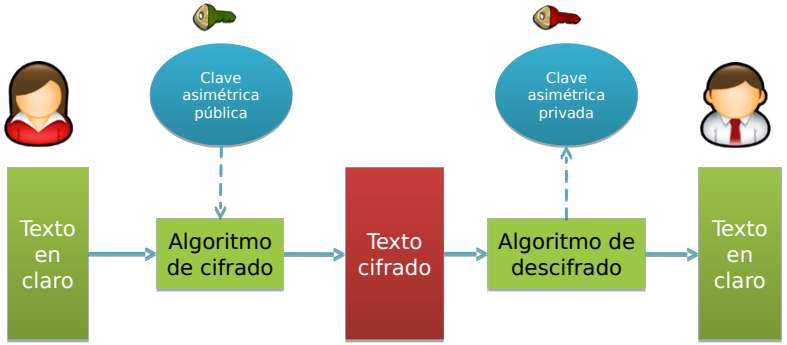
Ventajas del cifrado simétrico:

- El algoritmo es relativamente sencillo.
- La clave no tiene que ser muy grande para conseguir un cifrado seguro (256 bits).
- El texto cifrado puede considerarse compacto. (El texto cifrado es mayor que el texto claro, pero no mucho más)
- El algoritmo de cifrado es público.

Desventajas del cifrado simétrico:

- La clave sería un secreto compartido.
- Procedimiento para hacer llegar la clave al receptor.

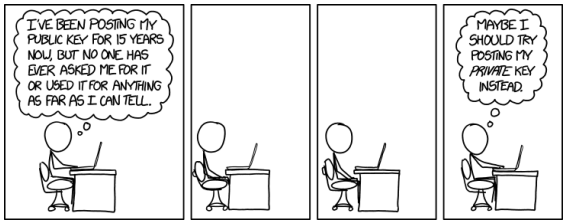
Cifrado asimétrico



- Bea cifra el mensaje con la clave pública de Santi
- Santi descifra el mensaje utilizando su clave privada.

Para firma digital se usa lo contrario:

- Bea firma el mensaje con su clave privada
- Santi comprueba la firma con la clave pública de Bea



Propiedades del cifrado asimétrico:

- La clave pública se corresponde sólo con una clave privada y la clave privada se corresponde sólo con una pública. Las dos claves forman un par biunívoco.
- La clave privada no se puede deducir a partir de la clave pública correspondiente.
- Una vez encriptado un mensaje con una clave pública no puede ser desencriptado más que con la clave privada correspondiente.
- La clave privada sólo la debe conocer el titular y debe controlarla adecuadamente.

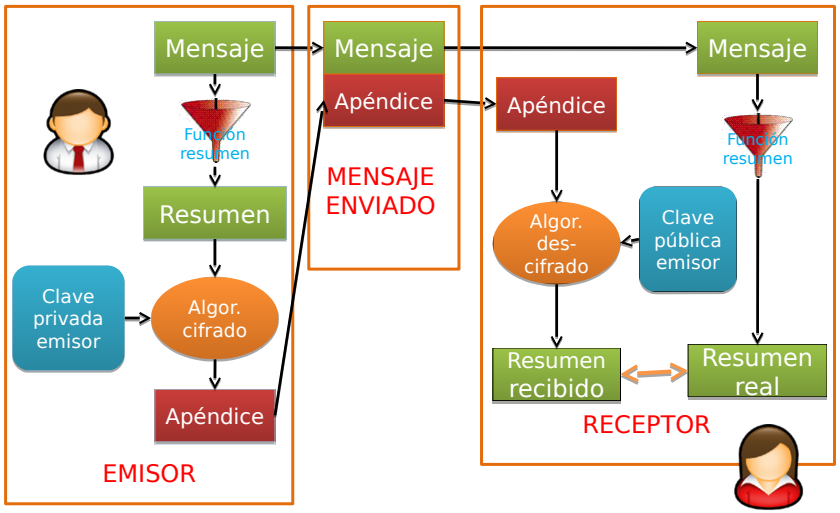
Ventajas del cifrado asimétrico:

- Al usar dos claves, una privada y otra pública: se puede enviar sin ningún problema la clave pública por cualquier medio.
- El algoritmo de cifrado y descifrado son públicos.

Desventajas del cifrado asimétrico:

- El algoritmo es relativamente complejo.
- La clave para conseguir un cifrado seguro tiene que ser relativamente grande (2048-4096 bits, 8192 para fines militares)
- El texto cifrado es poco compacto.

Firma digital



Condiciones para que los resúmenes coincidan:

- Las claves privada y pública usadas, tienen que pertenecer al mismo juego.
- El mensaje no pudo ser alterado.

Propiedades del apéndice:

- Cada apéndice se corresponde con un documento.
- El apéndice depende de la clave privada con la que se crea.
- Hay una relación biunívoca entre el mensaje y el apéndice de forma que en caso de modificar cualquier detalle del mensaje, deja de corresponderse con el apéndice, de esta forma se puede garantizar la integridad.

Certificado digital

Es un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora, dicho documento establece una relación entre un sujeto (persona física o jurídica) y su clave pública.

Componentes:

- Una clave pública
- La identidad del implicado: nombre y datos generales
- La firma privada de una entidad llamada Autoridad Certificadora que todos reconocen como tal y que válida la asociación de la clave pública en cuestión con la persona que dice ser.

Protocolo SSL

Es un protocolo seguro de Internet inventado por Netscape, que sirve para cualquier tipo de comunicación vía Internet.

Incluye las siguientes funciones:

- Fragmentación
- Compresión
- Autentificación
- Integridad
- Confidencialidad