



Tema 6

Seguridad en el Comercio Electrónico



Ing. Carlos David Montellano Barriga



Contenido

- ❧ ¿Qué es Seguridad?
- ❧ Problemas de Seguridad en el Comercio Electrónico
- ❧ Criptografía
 - ❧ Criptografía simétrica
 - ❧ Cifrado de clave pública
 - ❧ Firma digital
 - ❧ Funciones 'hash'
 - ❧ Firmas digitales y funciones 'hash'
 - ❧ Sobres digitales
- ❧ Certificados digitales e Infraestructura de Clave Pública (PKI)
 - ❧ Tarjeta criptográfica
 - ❧ Pretty Good Privacy (PGP)
- ❧ Protección de los canales de comunicación
- ❧ Secure Sockets Layer (SSL)
- ❧ Redes privadas virtuales (VPN)
- ❧ Protección de las redes
 - ❧ Cortafuegos
 - ❧ Servidores 'proxy'



¿Qué es Seguridad?

- ❧ La seguridad de computadoras es la protección de activos contra el **acceso, uso, alteración o destrucción** no autorizados.
- ❧ Prevención, Detección y Respuesta contra acciones no autorizadas



Clasificación de la seguridad en computadoras



∞ Confidencialidad

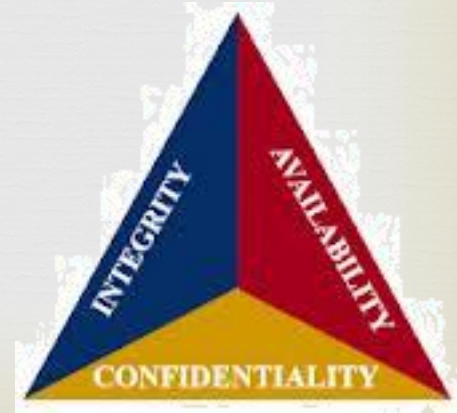
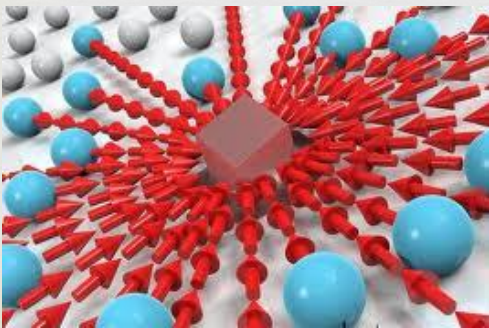
∞ Se relaciona con la protección contra la revelación no autorizada de datos y la garantía de la autenticidad de la fuente de datos

∞ Integridad

∞ Se refiere a evitar la modificación no autorizada

∞ Necesidad (también conocida *como negación del servicio*).

∞ Evita el retraso o negación (remoción) de datos



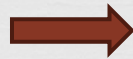
Los problemas de seguridad en el comercio electrónico

⌘ Tecnológicos



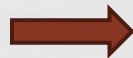
Podemos realizar transacciones más protegidas que con cualquier otra forma de comunicación

⌘ Legales



Hay un amplio desarrollo legal en la Estados Unidos, en la Union Europea y otros países sobre firmas electrónicas, etc

⌘ Psicológicos



Las encuestas y el acelerado aumento del volumen de transacciones electrónicas muestra que las barreras psicológicas han caído.

Aspectos tecnológicos

Seguridad en el almacenamiento de datos

❧ Frente a destrucción

- ❧ Catástrofes
- ❧ Problemas Físicos

❧ Frente a intrusos

- ❧ Personas
- ❧ Amenazas Lógicas



Seguridad en la transmisión de los datos

❧ Autenticación

❧ Integridad

❧ Confidencialidad

❧ No repudio

Criptografía



Griego κρύπτω *krypto* = oculto

- ⊙ El cifrado es el proceso de **transformar un mensaje** de forma que no pueda ser leído por nadie más que el remitente y el destinatario



- ⊙ La criptografía permite proteger:
 - a) la información almacenada
 - b) la transmisión de dicha información

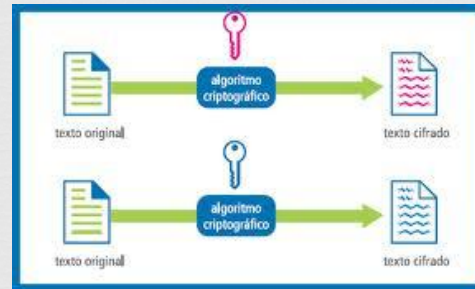
¿Que podemos obtener mediante criptografía?

- Integridad del mensaje
- No repudio
- Autenticación
 - Es decir, verifica la identidad de la persona (o máquina) que envía el mensaje
- Confidencialidad



Criptografía simétrica

- Transformación de datos en otros cifrados se lleva a cabo usando algún tipo de **clave**



cifrado por
sustitución



Reemplazar una letra por otra diferente

Ej: si usamos la clave “la letra más dos”, la palabra “Hola” se transformaría en “Jqnc”

cifrado por
transposición



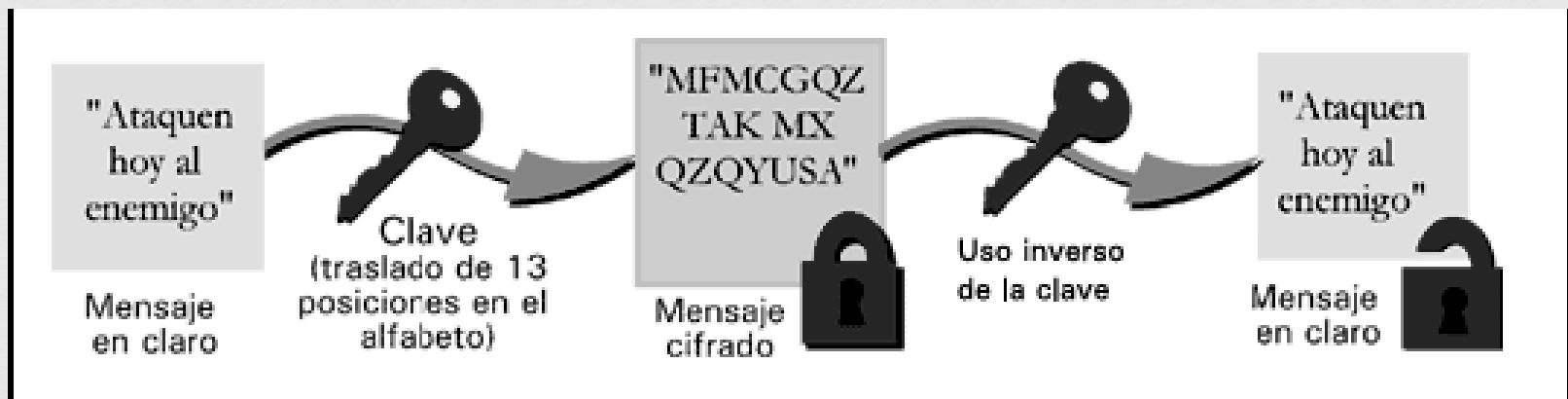
Cambiar el orden de dos letras de la misma palabra

Ej. notas en orden inverso
“Hola” se transformaría “aloH”

Algunos Métodos
simples

Criptografía simétrica

- ❧ Para descifrar estos mensajes, el receptor tiene que aplicar sobre el mensaje cifrado la **misma clave** que empleó el emisor para cifrar el mensaje original



Criptografía simétrica



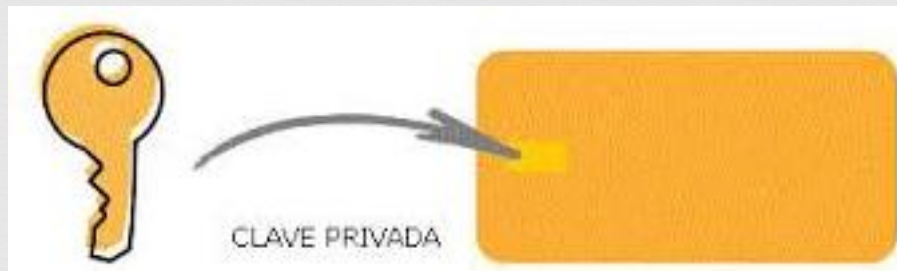
Problema: ¿cómo se envía la clave en sí?



Inconvenientes

❧ Requiere que ambas partes **compartan la clave**

❧ ¿Cómo se envían ésta de forma segura?



❧ Además, necesitaríamos una clave secreta para cada una de las partes con las que tratásemos

Una nota histórica la maquina Enigma

- Se usó mucho durante la Segunda Guerra Mundial
 - Cada día, la máquina generaba una nueva clave que usaba tanto sustitución como transposición de caracteres, mediante un dispositivo mecánico con una determinada configuración.
 - Al ser la configuración de todas las máquinas del mundo la misma, la comunicación era segura (en un día no había tiempo para averiguar la clave utilizada)
 - Después de un proceso largo y de mucho trabajo, con la captura de algunas de las máquinas los libros de códigos por parte de los aliados, éstos pudieron llegar a comprender su funcionamiento y, con ello, descifrar los mensajes alemanes



Alan Turing



Cifrado digital

- Claves usadas actualmente para codificar mensajes son digitales
 - Ej: multiplicar el mensaje a enviar por un número binario de 8 bits
 - resultado sería el mensaje cifrado y el número la clave necesaria para descifrar el mensaje



- La seguridad, depende de la longitud de la clave

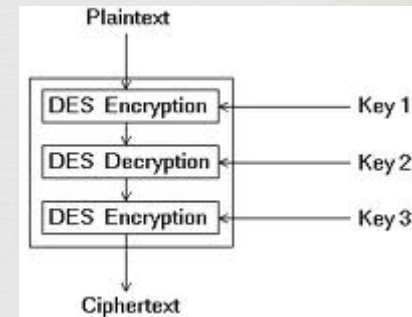
Función de cifrado debe ser conocida por todos, para que pueda usarse en un entorno de comercio electrónico

Claves utilizadas son de 56, 128, 256 ó incluso 512 bits

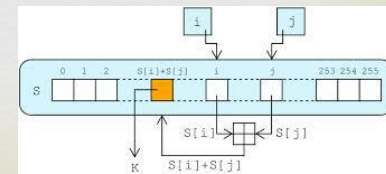
Se calcula que todas las computadoras del mundo, juntas, necesitarían 10 años para averiguar una clave de 512 bits

Algunos ejemplos

- El sistema de cifrado simétrico más usado en Internet hoy día es el DES (Data Encryption Standard)
 - Desarrollado por la Agencia de Seguridad Nacional (NSA) e IBM en los 50
 - Usa una clave de 56 bits
 - Para lidiar con las computadoras actuales se utiliza lo que se conoce como Triple DES (Cifrar el mensaje tres veces con otras tantas claves)



- RC2, RC4 y RC5, con claves de hasta 2048 bits
- El algoritmo IDEA, la base de PGP (128 bits)



Criptografía de clave pública

En 1976, Whitfield Diffie y Martin Hellman inventaron un modo totalmente nuevo de cifrar mensajes, denominado criptografía de clave pública



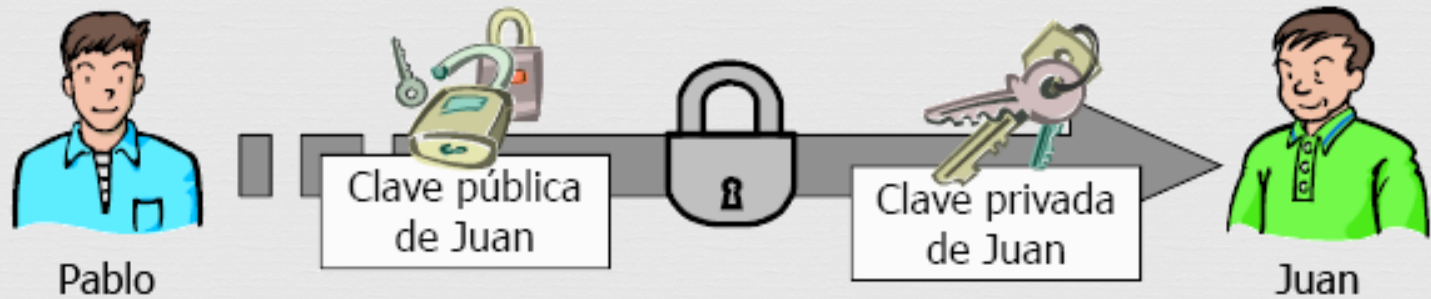
Resuelve el problema del intercambio de claves

Cada persona tendrá dos claves digitales relacionadas matemáticamente

- Una pública y otra privada
- Ambas sirven para cifrar y descifrar
- Lo que se cifra con una sólo se podrá descifrar con la otra
- Las funciones matemáticas usadas para generar las claves garantizan que no se puede averiguar una clave a partir de la otra (se usan claves de 128, 256 o 512 bits)

$$c \equiv m^e \pmod{n}$$

Ejemplo



- ❧ Pablo le envía un mensaje a Juan cifrado con la clave pública de éste
- ❧ Ese mensaje sólo podrá ser descifrado por Juan, mediante su clave privada

¿Qué se consigue?



- ⦿ Se garantiza la **confidencialidad** del mensaje, sin los inconvenientes del cifrado simétrico
- ⦿ Pero descuida los otros aspectos de la seguridad:
 - ✧ No hay garantía de que el emisor sea quien dice ser (**autenticación**)
 - ✧ Por tanto, éste podría negar haber enviado el mensaje (no repudio)
 - ✧ Y tampoco garantiza que el mensaje no haya sido alterado durante la transmisión (integridad)

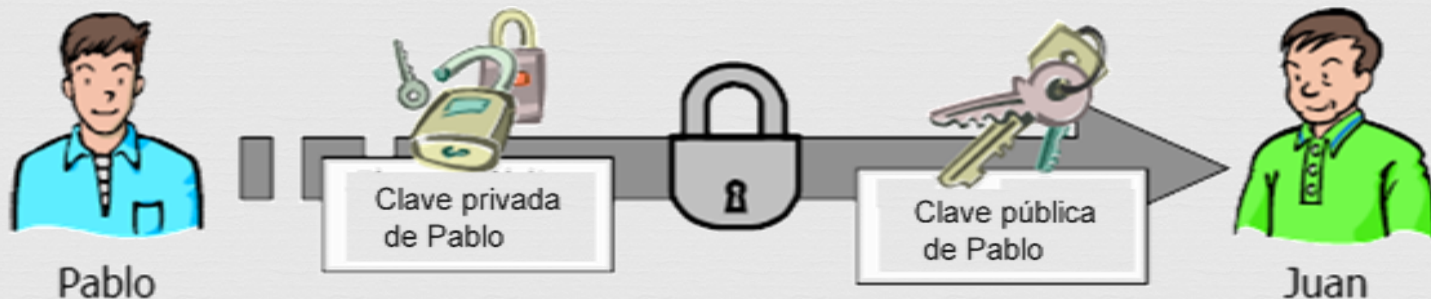
Firma digital



- ⦿ Al igual que la firma manuscrita tradicional, permite identificar a la persona que, en este caso, está realizando una transacción electrónica
- ⦿ Consigue:
 - ✧ Autenticación
 - Permite identificar al emisor, certificando es quien dice ser, es decir, que no se trata de ningún impostor
 - ✧ No repudio
 - Esta firma compromete al emisor, actuando como prueba

¿En qué consiste?

- ❧ Proceso inverso al de la clave pública
- ❧ Emisor cifra el mensaje original empleando su clave privada
 - ❧ El receptor, para descifrarlo, usará la clave pública del emisor



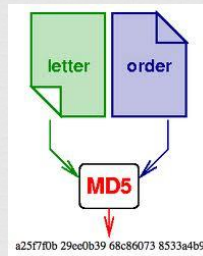
- ❧ Naturalmente, hay que usarlo en combinación con la clave pública
 - ❧ Para seguir garantizando la confidencialidad

Funciones 'hash'

- Integridad

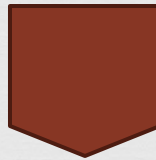
 - Que el mensaje no sea alterado durante su transmisión

- Esto se logra con las funciones 'hash'



 - Algoritmo que se aplica sobre el mensaje y produce un número de longitud fija que es un “resumen” de aquél

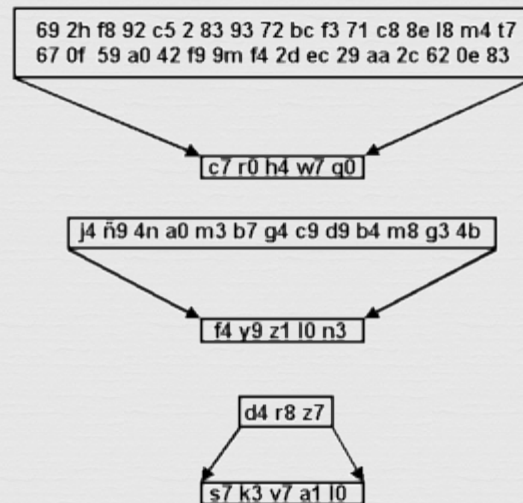
Carlos David Montellano



77d5ded6997600dbbeab1357781356bf

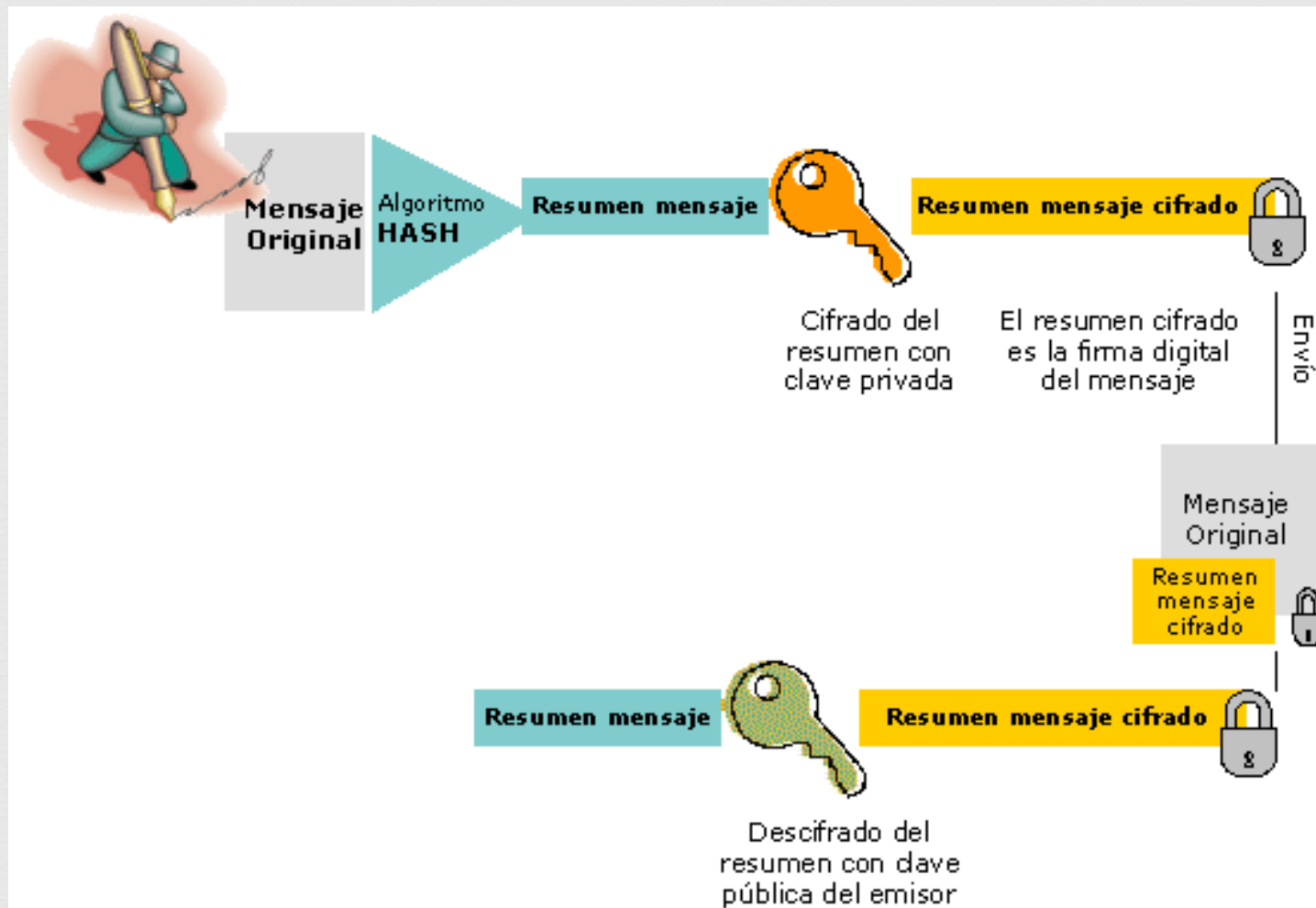
Funciones Hash

✧ Hay funciones estándar, como MD4 y MD5, que producen números de 128 y 160 bits respectivamente



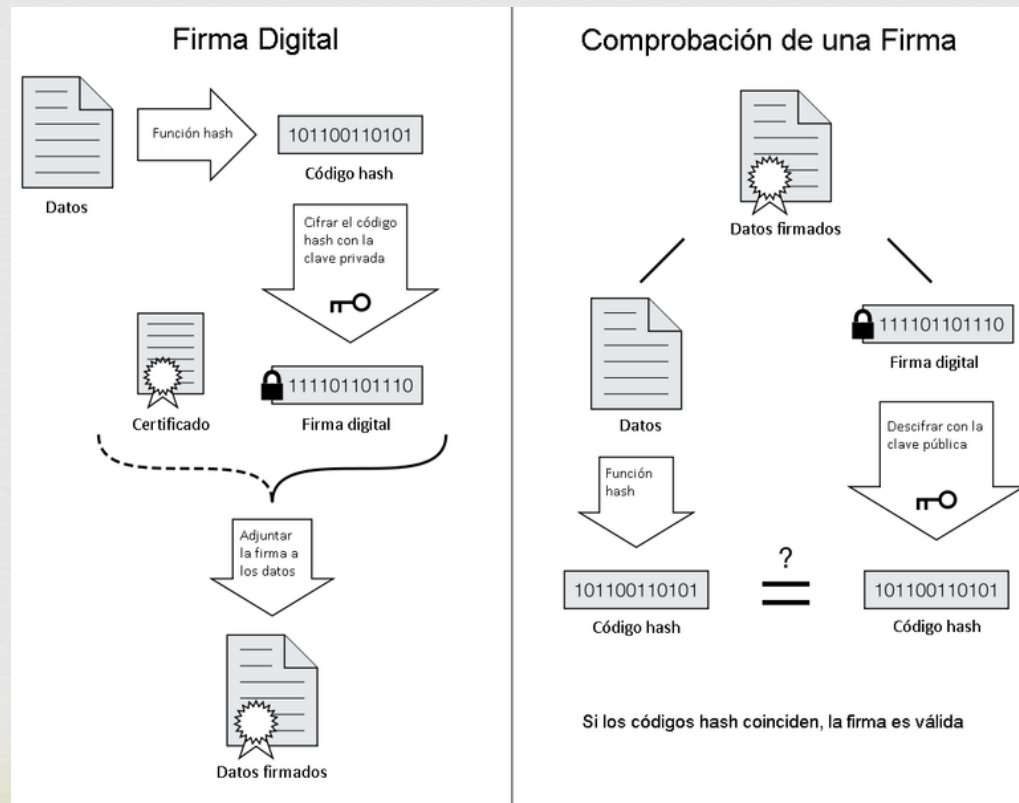
✧ El algoritmo SHA1

Como Funciona

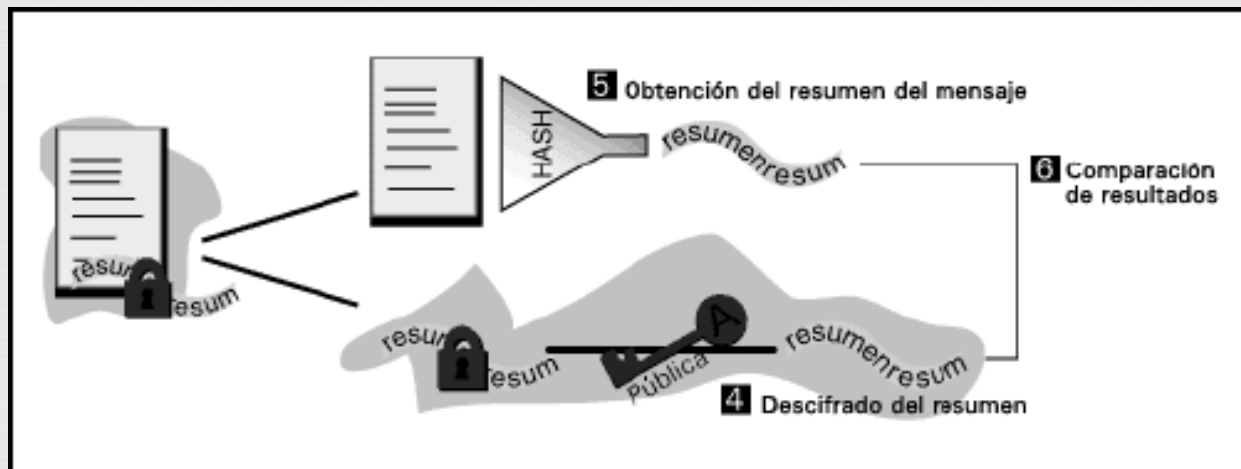


Firmas digitales y funciones 'hash'

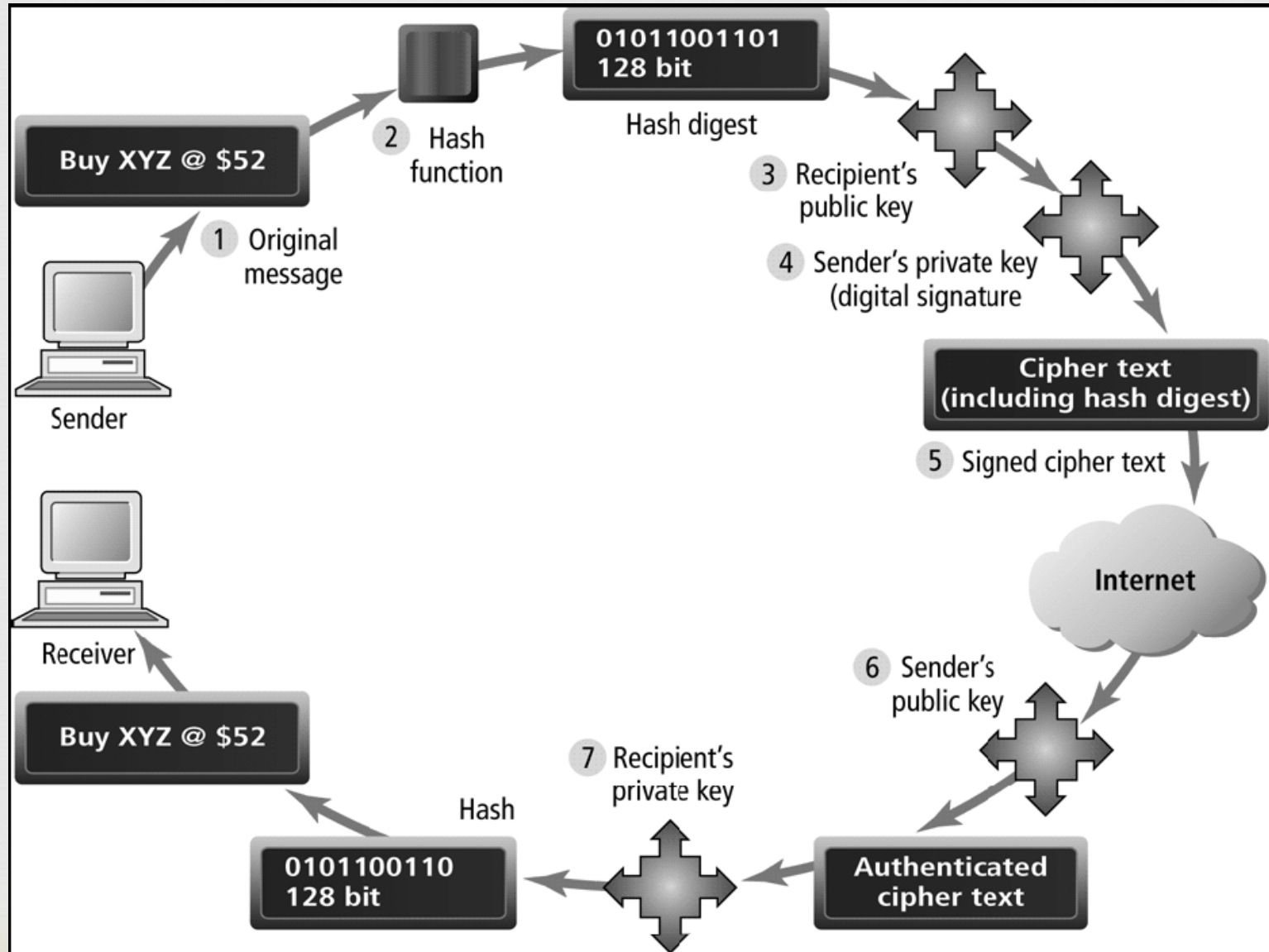
- ❧ Usadas conjuntamente, las firmas digitales son incluso “más únicas” que las manuscritas
- ❧ No sólo permiten identificar a un individuo, sino que la firma será única para cada documento concreto que éste firme



¿Cómo funciona?



❧ Para lograr todos los aspectos de seguridad (salvo el de privacidad), se usará conjuntamente criptografía de clave pública, funciones 'hash' y firmas digitales



Sobres digitales



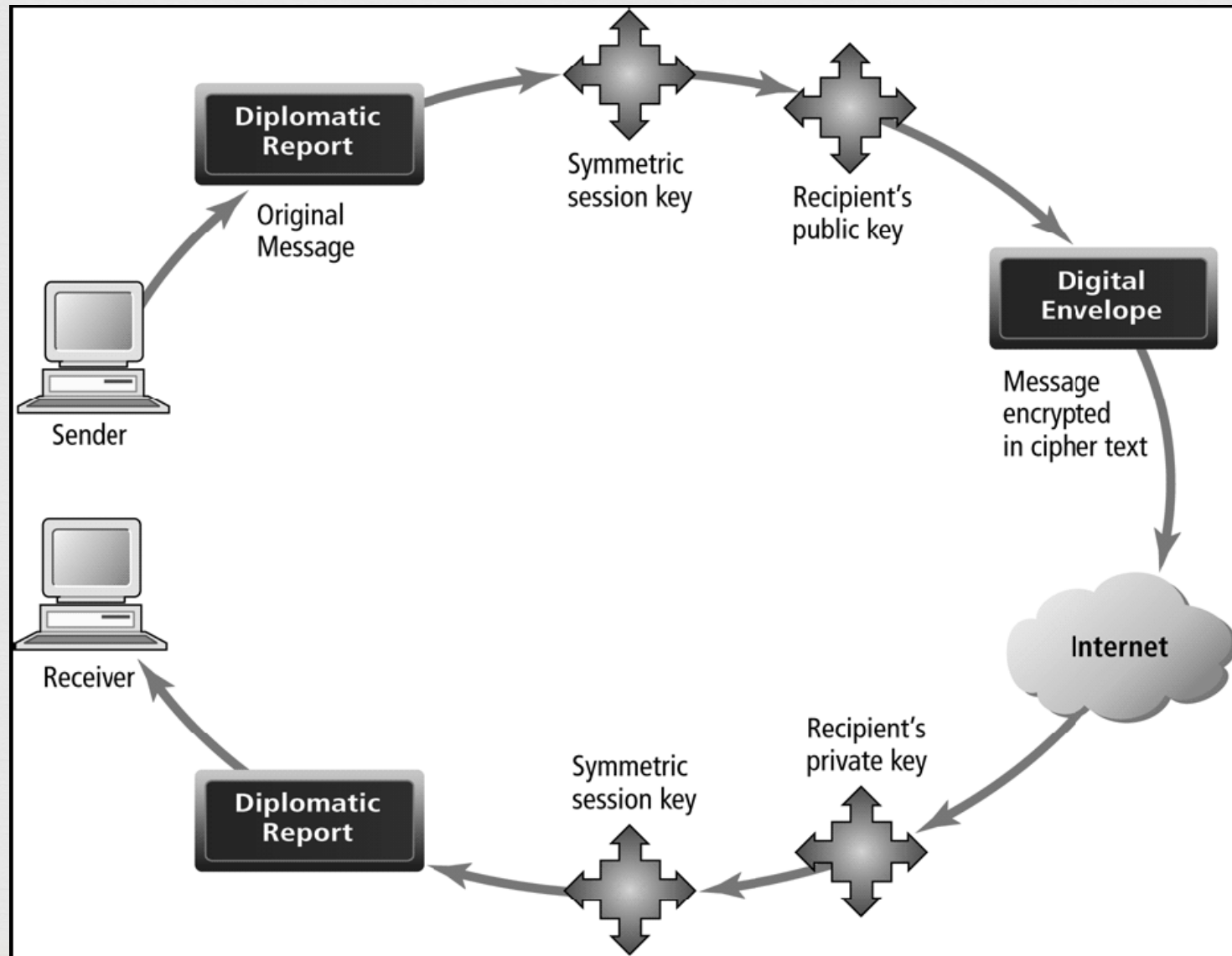
- ⦿ La criptografía de clave pública es computacionalmente lenta
 - ✎ Si usamos claves de 128 o 256 bits para cifrar un documento grande puede tardar bastante
- ⦿ La criptografía de clave simétrica es rápida pero tiene el problema del envío de la clave
- ⦿ Una solución intermedia

es usar criptografía simétrica para cifrar documentos grandes

enviar la clave cifrada mediante criptografía de clave pública

Es lo que se conoce como sobre digital

Ejemplo de sobre digital



Certificados digitales e Infraestructura de Clave Pública (PKI)

- ⊙ Aún queda un problema que solucionar
 - ✧ Efectivamente, sabemos que el documento recibido ha sido firmado, pero...
- ⊙ ... ¿cómo sabemos que el poseedor de dicha firma electrónica es quien dice ser?
 - ✧ Necesitamos algo similar al Carne de Identidad en el mundo real
- ⊙ Para eso están las llamadas autoridades de certificación
 - ✧ Garantizan la asociación entre una persona física y su clave pública



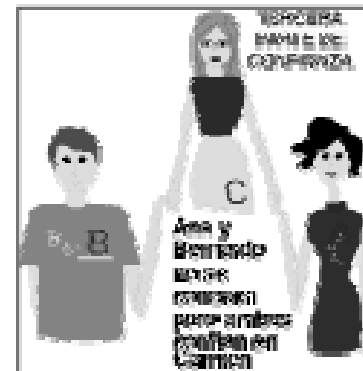
Certificados digitales

- Un certificado digital es un documento digital emitido por una autoridad de certificación (CA)
- Contiene:
 - El nombre de la persona o empresa
 - Su clave pública
 - Un número de serie del certificado
 - Una fecha de caducidad
 - La fecha de expedición
 - La firma digital de la autoridad de certificación
 - El nombre de la CA cifrado usando la clave privada de ésta



Autoridades de Certificación

- Institución de confianza que garantiza que la clave pública se corresponde con tal o cual persona
- Son lo que se denomina terceras partes de confianza (TTP, Trusted Third Party)



es fundamental en cualquier entorno de clave pública de tamaño considerable

mejor forma de permitir la distribución de los claves públicas (o certificados digitales) es que algún agente en quien todos los usuarios confíen se encargue de su publicación

en algún repositorio al que todos los usuarios tengan acceso.

Ejemplos de CA

- ⊙ En EEUU, empresas privadas como VeriSign y agencias del gobierno como el U. S. Postal Service

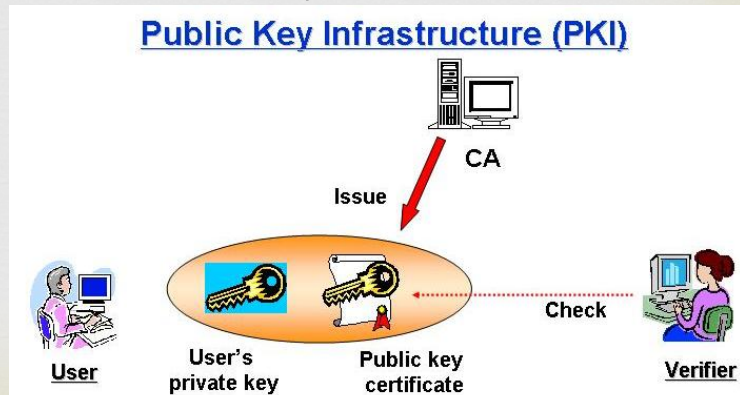


- ⊙ En España tenemos, por ejemplo, la Agencia Tributaria y la Seguridad Social
 - En ambos casos es, en última instancia, la Fábrica Nacional de Moneda y Timbre (FNMT) la emisora de los certificados



Infraestructura de clave pública

- ☞ Una Infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública
- ☞ Las PKI están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:
 - Autoridad de Certificación
 - Autoridad de Registro
 - Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital



Tarjeta criptográfica

- ❧ Sería otra posibilidad para tener nuestro certificado de usuario
- ❧ En vez de en un fichero en disco



Pretty Good Privacy (PGP)

- ❧ Programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet
- ❧ Podemos obtener un par de claves, pública y privada, en el sitio Web de Pretty Good Privacy www.pgpi.org
- ❧ Nos permite cifrar los mensajes así como identificarnos (nosotros y el destinatario)



El problema de la criptografía

Mayor problema es que se basan en una clave privada



cuya custodia es responsable el usuario



Es frecuente que esté almacenada en un PC sin la seguridad suficiente, en un disquete, etc.



normalmente las leyes nos hacen totalmente responsables de nuestra clave privada



No podremos reclamar lo que se haga con ella

Protección de los canales de comunicación

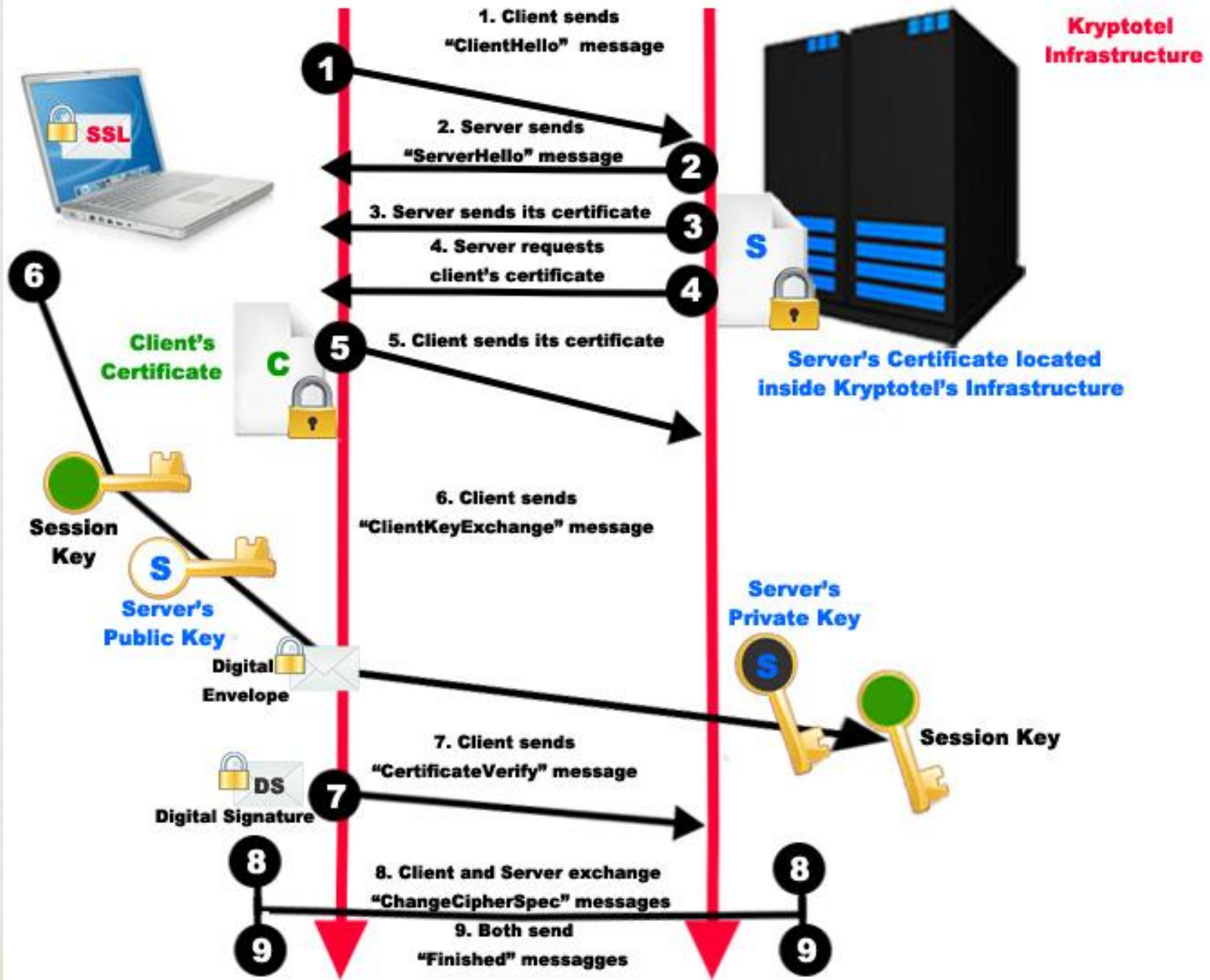




Secure Sockets Layer (SSL)

- ⦿ Protocolo que opera entre las capas de Transporte y Aplicación de TCP/IP y protege la comunicación entre el cliente y el servidor
 - ✧ Hace uso de técnicas como el cifrado de mensajes y las firmas digitales
- ⦿ Una sesión segura es aquella en la que tanto el propio URL del documento solicitado como el documento en sí, contenido de formularios y 'cookies' intercambiadas están cifradas
- ⦿ El cliente genera una clave de sesión simétrica

Funcionamiento SSL



Ejemplo de conexión SSL



← → ↻ Banco Nacional de Bolivia S.A. [BO] https://www.bnb.com.bo/bnbnetplus/login.aspx

BNB 1872 BANCO NACIONAL DE BOLIVIA

BNB Net+


Bienvenido a BNB Net +

- Está ingresando a un sitio seguro, certificado por [VeriSign](#).
- Verifique que la dirección de su navegador sea <https://www.bnb.com.bo/>.
- El banco nunca le pedirá que introduzca o digite a la vez todas las coordenadas de su tarjeta de coordenadas "Clave Maestra".
- Por favor revise los Consejos de Seguridad [aquí](#).
- La Clave es el PIN para el primer ingreso a BNB Net +. Posteriormente será la Clave para BNB Net + definida por usted.
- El banco nunca le pedirá información confidencial de sus cuentas o de sus tarjetas (contraseñas, claves secretas, números PIN, nombre de usuario) ni de sus datos personales, ya sea por correo electrónico, por teléfono o por otra forma de comunicación similar. Si usted recibe un mensaje pidiendo información confidencial o llamado raro, inusual o sospechoso o si alguien le solicita información por los medios antes mencionados, por favor absténgase de hacerlo y comunique esa situación al banco.



Usuario:
(Identificador de Acceso a Web)

Escriba las letras y números tal como se muestran en la siguiente imagen. No se distingue entre mayúsculas y minúsculas.



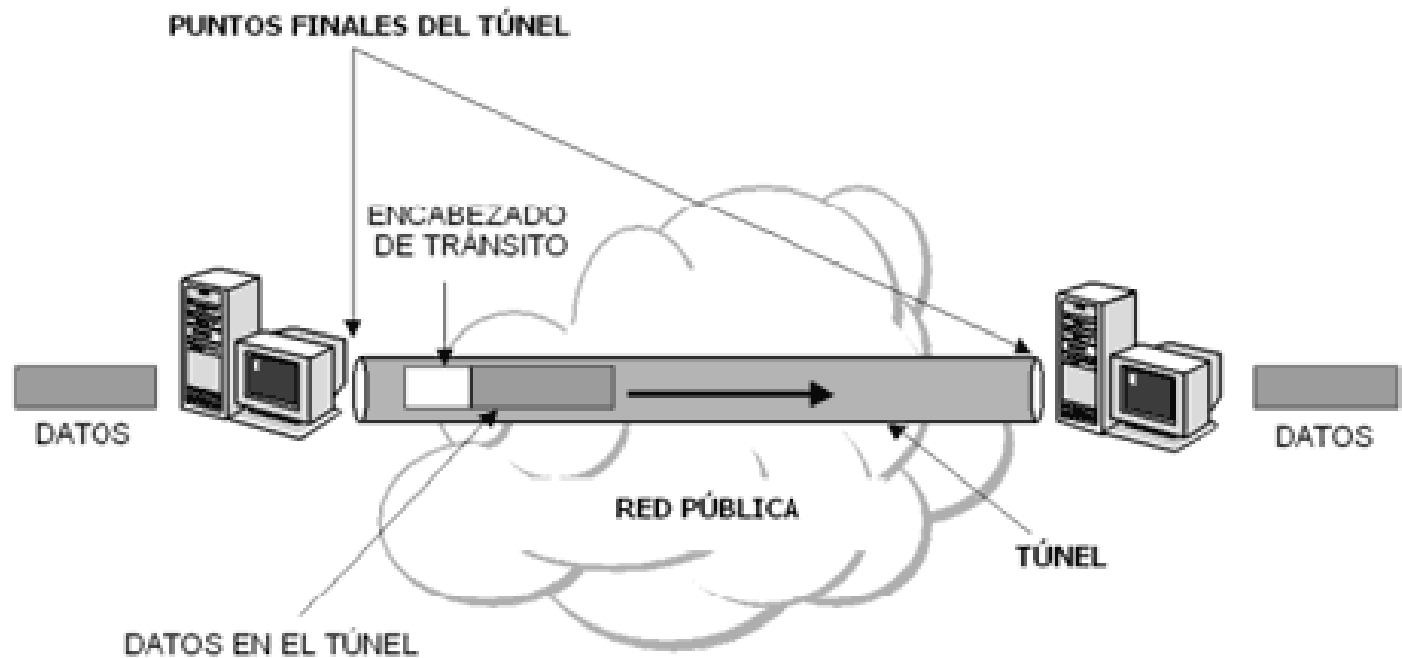
Enviar Manual Demo Limpiar

Redes privadas virtuales (VPN)

- ⦿ Permiten acceder a la red privada de la empresa a través de Internet, de forma segura
 - ✎ Un túnel representa un circuito virtual dedicado entre dos puntos
 - Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel
 - El protocolo encapsulará esos datos, cifrados, sobre IP
- ⦿ Protocolos: PPTP (Point-to-Point Tunneling Protocol), IPSec, etcétera



Redes privadas virtuales (VPN)



Protección de las redes



Lo último que nos queda por ver es cómo se
pueden proteger las redes en sí.



Firewalls (Cortafuegos)

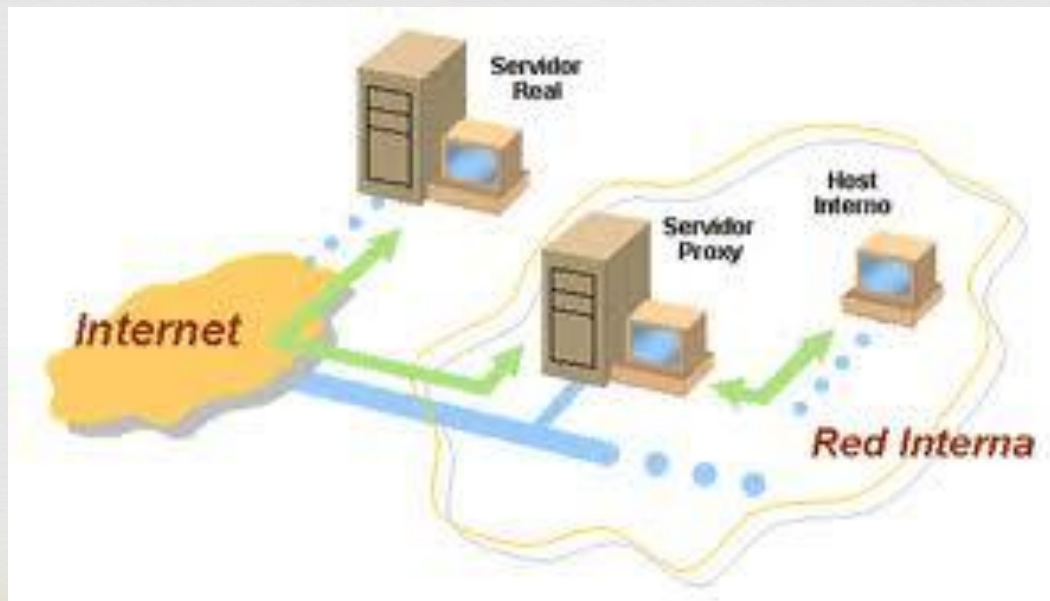
- ⦿ Evitan acceso de los clientes remotos a la red privada de la empresa
- ⌘ Pueden ser dispositivos hardware o software
- ⌘ Filtran todos los mensajes entrantes



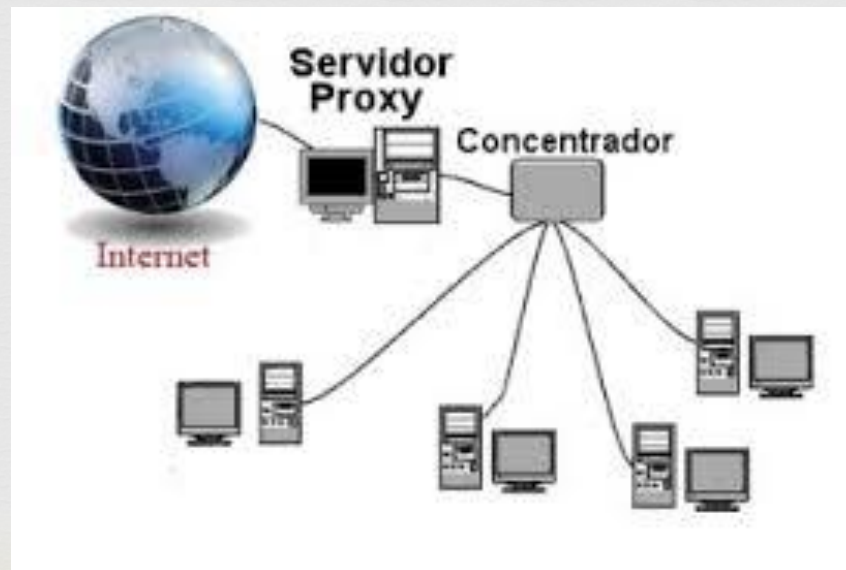
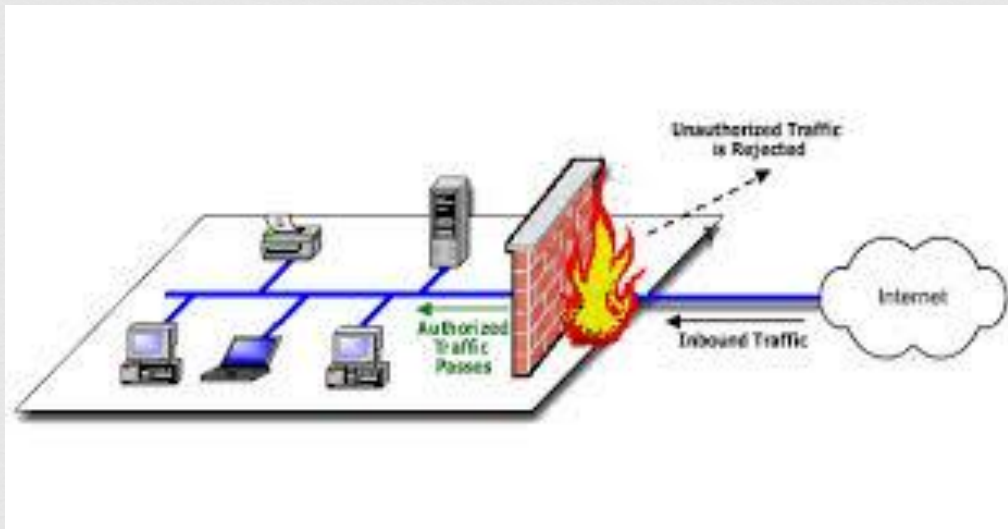
- Examinan paquetes ven si se dirigen a un puerto prohibido, o si provienen de una dirección IP no autorizada
- Todo ello configurado por el administrador de la red
- También el filtrado depende de la aplicación solicitada, en vez de el destino u origen del mensaje
- Telnet, FTP, HTTP, POP3...

Servidores 'proxy'

- ❧ Controlan el acceso desde la red interna a Internet
- ❧ Son la pasarela de acceso a Internet
- ❧ Suelen tener dos (o más) tarjetas de red
- ❧ Pueden ofrecer otros servicios, como NAT (Network Address Translation)



Cortafuegos y servidores 'proxy'



Consideraciones finales



En resumen

- En general, los riesgos para el consumidor en el comercio electrónico no son mayores que en el comercio tradicional
- Para los comerciantes sí son mayores
 - Perderían la mercancía vendida y el dinero (que tendrían que devolver al banco)
- Como siempre, la seguridad no es absoluta
 - Cualquier sistema de seguridad puede vulnerarse si se invierten los suficientes recursos en ello

En resumen

- Es necesario usar las tecnologías vistas para proporcionar un entorno seguro de comercio electrónico
- No obstante, la tecnología por sí sola no es suficiente
- Hacen falta una serie de leyes que persigan los delitos cometidos y permitan castigar a los culpables
- Por último, al igual que el comercio tradicional, es necesario que el consumidor adopte precauciones
- Que mire él mismo por su seguridad, con sentido común