REDES DE COMPUTADORAS
EC5751

USB

Seguridad y Nuevas Tecnologías

SEGURIDAD

Contenido

- Seguridad en la red
- Ataques Pasivos
- Ataques Activos
- Cifrado Convencional
- Algoritmos (DES y 3DES)
- Clave Publica
- Firma Digital
- RSA
- IPSec
- DNSSec

SEGURIDAD

- La **Seguridad de redes** son las políticas y acciones adoptadas para prevenir y monitorear accesos no autorizados, mal uso, modificación o la denegación de acceso a una red de computadoras , los recursos de acceso y/o los servicios que esta puede prestar.

SEGURIDAD

Ataques Pasivos

- Escucha de las transmisiones para obtener información
- Divulgación del contenido del mensaje
- Análisis de trafico:
  - Si se conoce la frecuencia y longitud de un mensaje (aunque este cifrado) se puede descubrir el contenido.
- Difíciles de detectar
- Se pueden Prevenir

SEGURIDAD

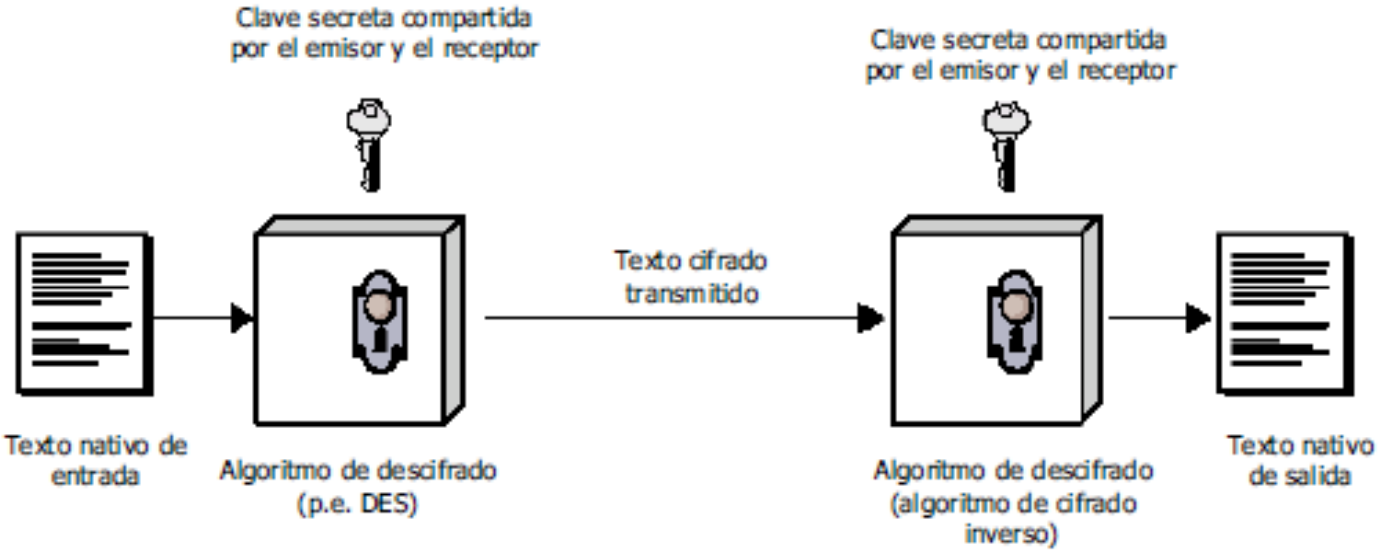
Ataques Activos

- Enmascaramiento
  - Una entidad pretende ser otra
- Repetición
- Modificación de los mensajes
- Denegación de un servicio (DDOS)
- Fácil de detectar
  - Por lo general la detección es disuasiva
- Difícil de Prevenir

SEGURIDAD

Cifrado Convencional (Criptografía Simétrica)

- Texto Nativo
- Algoritmo de Cifrado (Robusto y complicado)
- Clave Secreta (Intercambio “seguro”)
- Texto Cifrado
- Algoritmo de Descifrado



SEGURIDAD

Cifrado por Algoritmos:

•Procesan bloques de texto y productos de bloques de igual tamaño pero ya cifrados.

- •Principales Algoritmos:
  - •**DES (Data Encryption Estándar):** Aun usado fue el estándar en USA, creado en 1976 (Lucifer) y declarado inseguro en 1998, usa claves de 56 dígitos y maneja bloques de 64 bits.
    100 mil billones de claves posibles.
  - •**TDEA o 3DES (Triple Data Encryption Algorithm):** Estándar actual, creado en 1979 extensión mas segura de DES. claves de 168 dígitos (1, 2 o 3 claves DES) y bloques de hasta 256 bits. Por lo general se encripta con K1, desencripta con K2 y se vuelve a encriptar con K1. Otro esquema es posible

SEGURIDAD

AES—The Advanced Encryption Standard

- Creado por Rijmen y Daemen en 1997.
- Definido en 2001 como el estándar norteamericano.
- Utiliza cifrado simétrico por bloques.
- Soporta claves de 128, 192 y256 bits.
- Se diseño para ser implementado por Sw o por Hw.
- Existen procesadores comerciales (Intel y otros) que incluyeron en su diseño el algoritmo AES.

SEGURIDAD

Ataques al Cifrado Convencional:

•Criptoanálisis: Conociendo el algoritmo y con textos cifrados se trata de encontrar la clave original.

•Fuerza bruta: Se prueban todas las opciones posibles hasta encontrar la clave que genere el texto legible.

SEGURIDAD

Principal problema ¿Como se comparten las Claves?

- Resuelto en 1973 por Diffie-Hellman-Merkle
- Lado A selecciona la primera parte de la clave y se la entrega a B
- Un tercero C, selecciona la segunda parte de la clave y se la entrega a A y B.
- Se utiliza la clave original para cifrar y transmitir una nueva parte 1 y para A y B.
- Se genera la tercera parte de la clave y se transmite utilizando la primera clave entre A y B.

SEGURIDAD

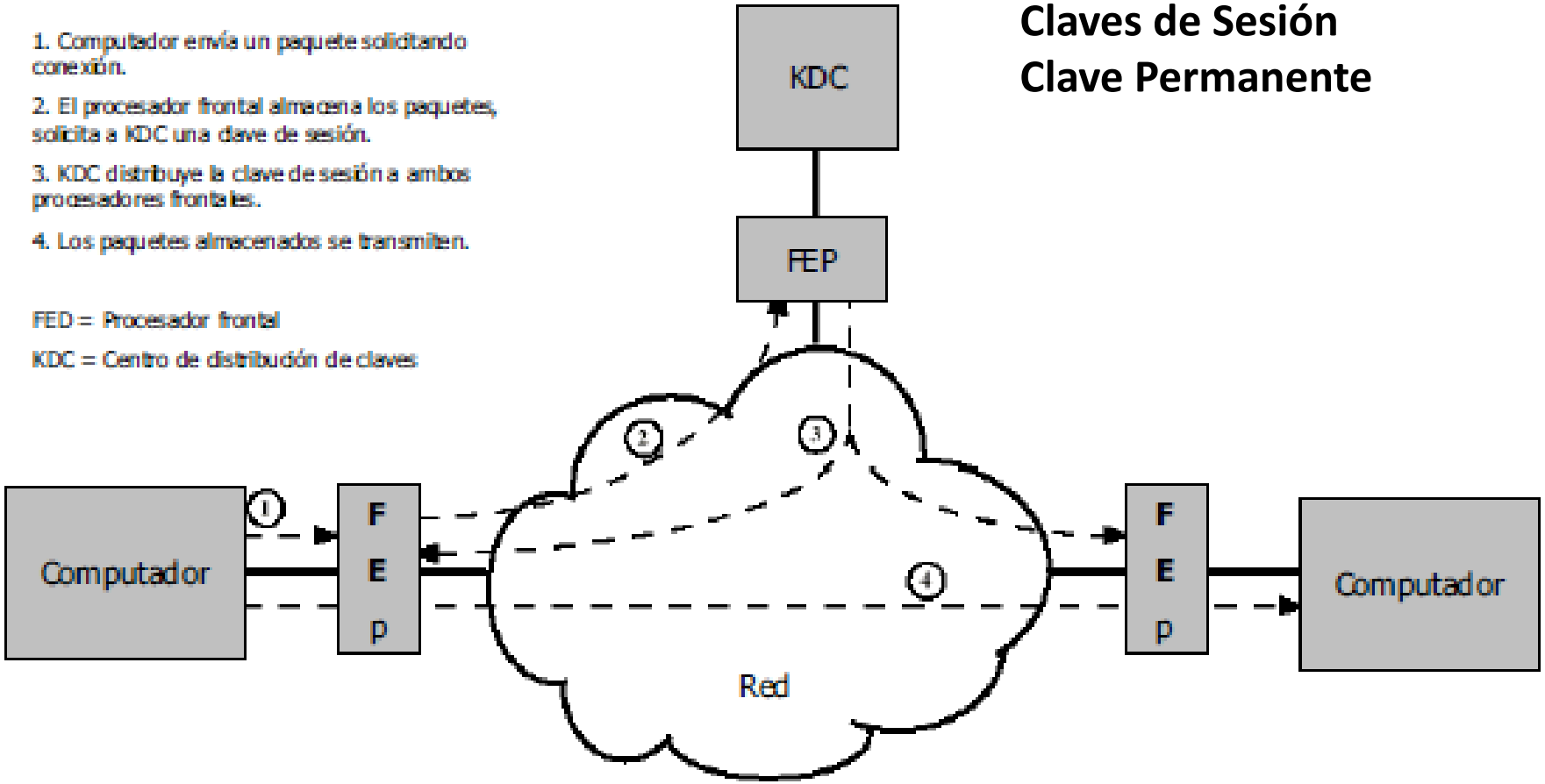
Envió Automático de Claves

1. Computador envía un paquete solicitando conexión.
2. El procesador frontal almacena los paquetes, solicita a KDC una dave de sesión.
3. KDC distribuye la clave de sesión a ambos procesadores frontales.
4. Los paquetes almacenados se transmiten.

FED = Procesador frontal

KDC = Centro de distribución de claves

Claves de Sesión
Clave Permanente



SEGURIDAD

Esquemas de protección adicionales:

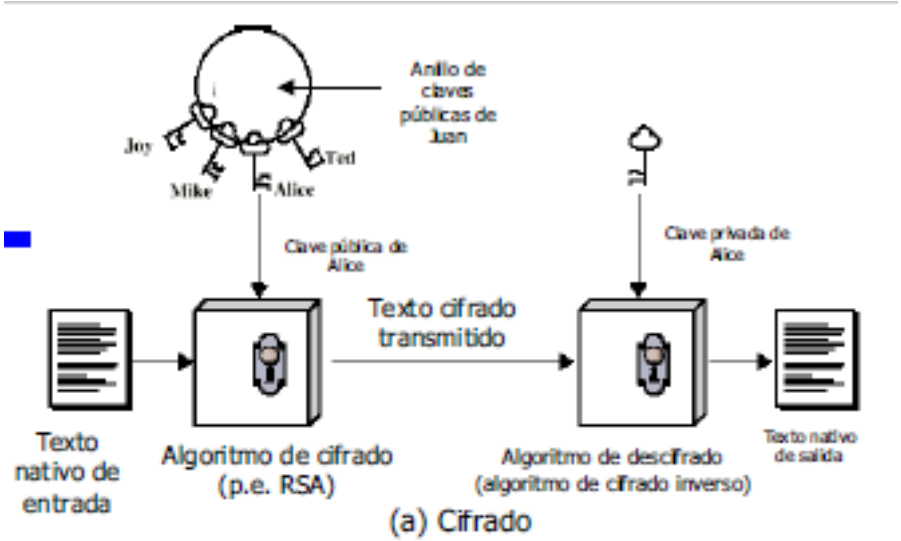
- **Relleno de trafico:**
  - Emite texto cifrado y aleatorio continuamente.
  - Cuando hay data la agrega e informa al destino.
  - Imposible determinar la cantidad de trafico.
- **Autentificación de mensajes:**
  - Protege de las agresiones Activas.
  - Emisor y receptor conocen las claves de cifrado.
  - Se valida origen, secuencia y destino.
- **Dispersión en un solo sentido:**
  - Como el destino espera el mensaje no hay clave.
  - Es rápido y solo hay una etiqueta resumen.

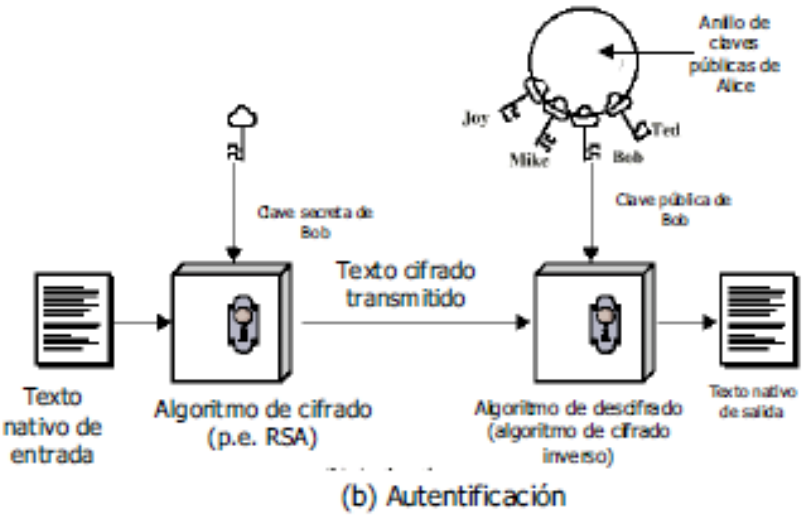
SEGURIDAD

Cifrado de clave Publica:

. Propuesto en 1975 por Diffie-Hellman-Merkle (descubierta en paralelo por Investigadores ingleses del GCHQ en 1973)

- Se basa en algoritmos matemáticos complejos.
- Claves Asimétricas: se usan dos claves independientes.
  - Publica, dominio general y se usa para cifrar.
  - Privada, la genera el usuario y se usa para descifrar.
- Es imposible conocer alguna de las claves conociendo la otra.





SEGURIDAD

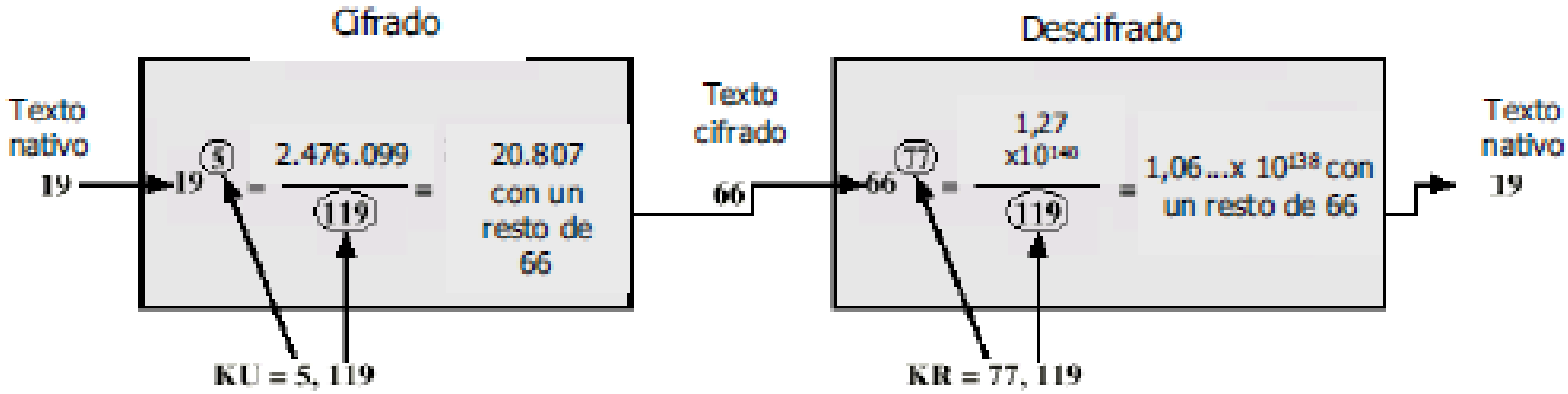
Cifrado de clave Publica: ejemplo

1. Ana redacta un mensaje
2. Ana cifra el mensaje con la **clave pública** de David
3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. David recibe el mensaje cifrado y lo descifra con su **clave privada**
5. David ya puede leer el mensaje original que le mandó Ana

SEGURIDAD

RSA – Rivest, Shamir y Adleman (1977)

- Algoritmo de criptografía mas usado a nivel mundial.
- Se utiliza para cifrar y firmar digitalmente.
- Las claves se basan en el producto de dos números primos muy grandes (Potencia de 300 o mas).
- Utiliza el esquema de clave publica y privada.



SEGURIDAD

Firma Digital:

- Basado en el principio de clave asimétrica.
- Emisor cifra la firma con su clave privada.
- Receptor descifra lo recibido con la clave publica del emisor.
- Se autentica al emisor ya que es el único que puede emitir ese cifrado.
- No se garantiza privacidad de los datos.

SEGURIDAD

Firma Digital: ejemplo

1. David redacta un mensaje
2. David firma digitalmente el mensaje con su **clave privada**
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la **clave pública** de David
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente

SEGURIDAD

PGP (Pretty Good Privacy)

- Desarrollado por Phil Zimmermann en 1991.
- Combina claves simétricas y asimétricas.
- El mensaje se comprime y codifica con una clave simétrica (DES,IDEA, triple DES) pero esta a su vez se codifica con una asimétrica (clave publica del receptor) y se envían juntos.
- Automáticamente es **firmado** digitalmente (clave privada del emisor).
- Se ha convertido en lo mas usado de internet por el publico (La especificación actual es la RFC 4880)

SEGURIDAD

Seguridad en IP

• **IPSec** (abreviatura de Internet Protocol Security) conjunto de protocolos cuya función garantizar autenticando y/o cifrando cada paquete IP.

• También incluye protocolos para el establecimiento de claves de cifrado.

• Permite:

  • Conectividad segura a través de Internet

  • Seguridad en el comercio electrónico

  • interconectar oficinas de empresas (intranet)

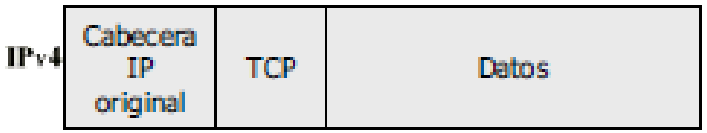
SEGURIDAD

Seguridad en IP

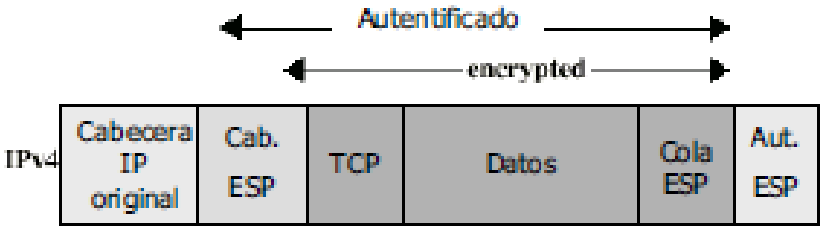
- Garantiza seguridad para IPv4 y IPv6.
- Normas RFC 2401,2402, 2406 y 2408.
- Maneja intercambio de claves.
- Encapsula en forma segura carga útil y encabezado.
- Se establece una “Asociación Segura” (SA) por cada sentido de viaje de la información.
- Hay dos modos de operación:
  - Transporte, solo se cifra la data
  - Túnel, se cifra data y encabezado

SEGURIDAD

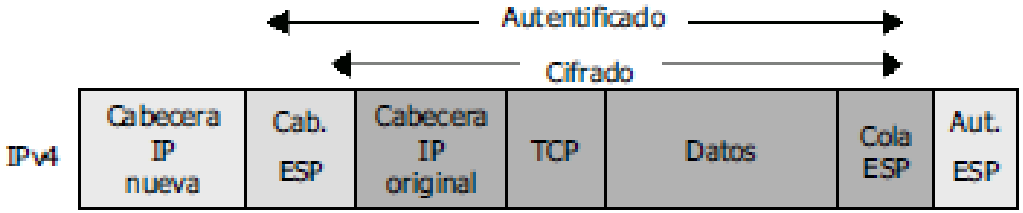
Seguridad en IP



(a) Paquete IP original



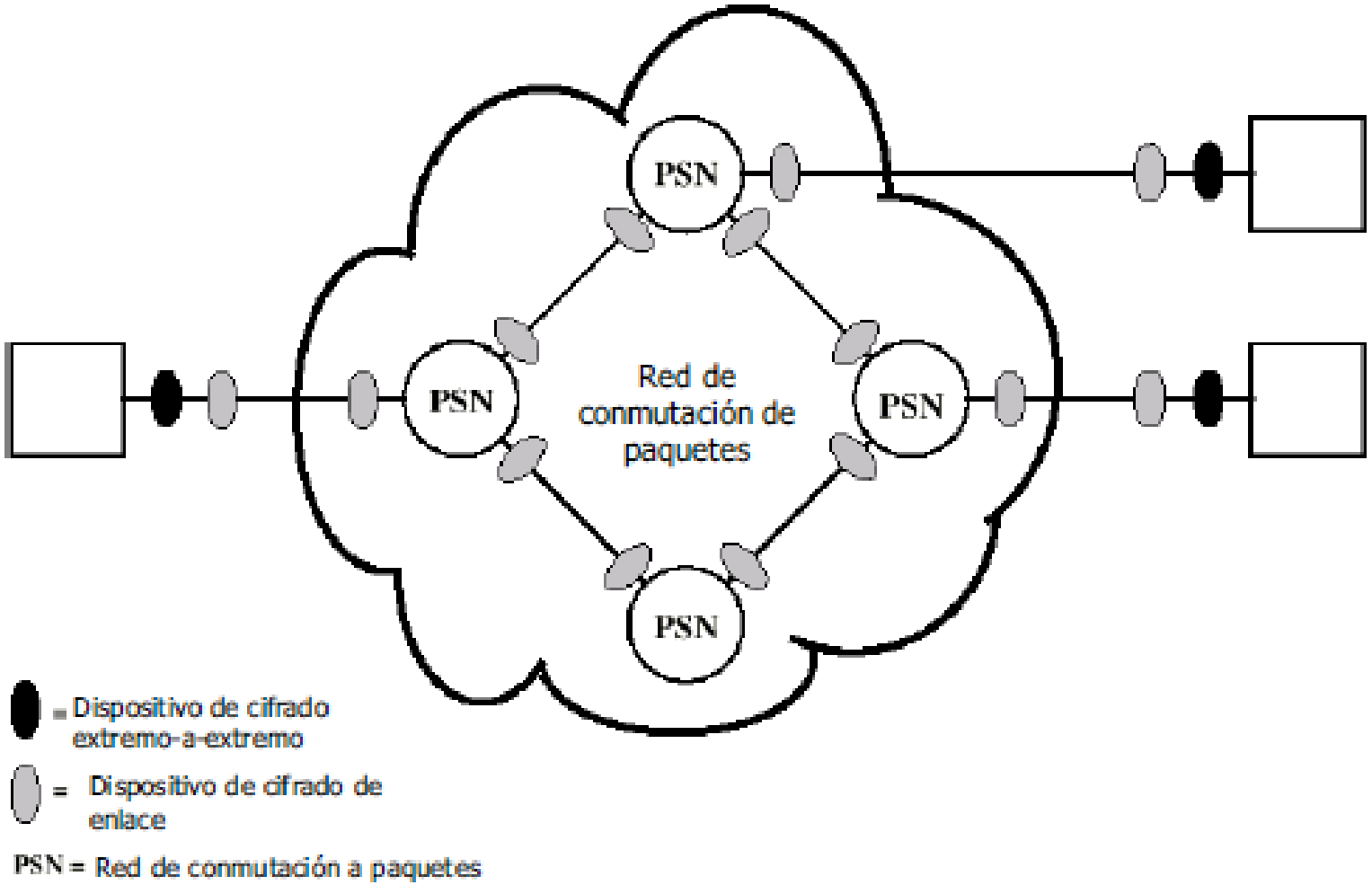
(b) Modo transporte



(c) Modo túnel

SEGURIDAD

Donde se colocan los codificadores de claves



SEGURIDAD

Cifrado de Enlace

- Cada enlace tiene un dispositivo de cifrado a ambos lados
- Todo el trafico se protege
- Alto nivel de seguridad en el enlace
- Requiere muchos dispositivos
- El mensaje se descifra en cada dispositivo, lo que lo hace vulnerable allí (si la red es publica esto es critico)

SEGURIDAD

Cifrado Extremo-Extremo

- El cifrado se hace en los dos sistemas finales
- Los datos cifrados se transmiten a través de la red
- Destino y origen comparten claves seguras (proceso Critico)
- Solo se cifra la data de usuario
- Modelo de trafico no seguro

SEGURIDAD

DNSSec - Domain Name System Security Extensions

• Se trata de un conjunto de extensiones al DNS que proporcionan a los clientes (o *resolvers*) la autenticación del origen de datos DNS, la negación autenticada de la existencia e integridad de datos, pero no disponibilidad o confidencialidad.

• No se cifran datos o peticiones, pero garantiza que la IP buscada es la correcta

• Si no se localiza una dirección, se valida y confirma su inexistencia.

SEGURIDAD

DNSSec - Domain Name System Security Extensions

- Lo bueno: realmente garantiza la seguridad del nombre buscado.
- Lo feo: el proceso de conversión a ella es lento y muchos proveedores no lo han iniciado.
- Lo malo: Su uso prácticamente triplica los recursos para el manejo de nombres.
- Se han creado muchos falsos rumores que retrasan su aplicación.

El Futuro

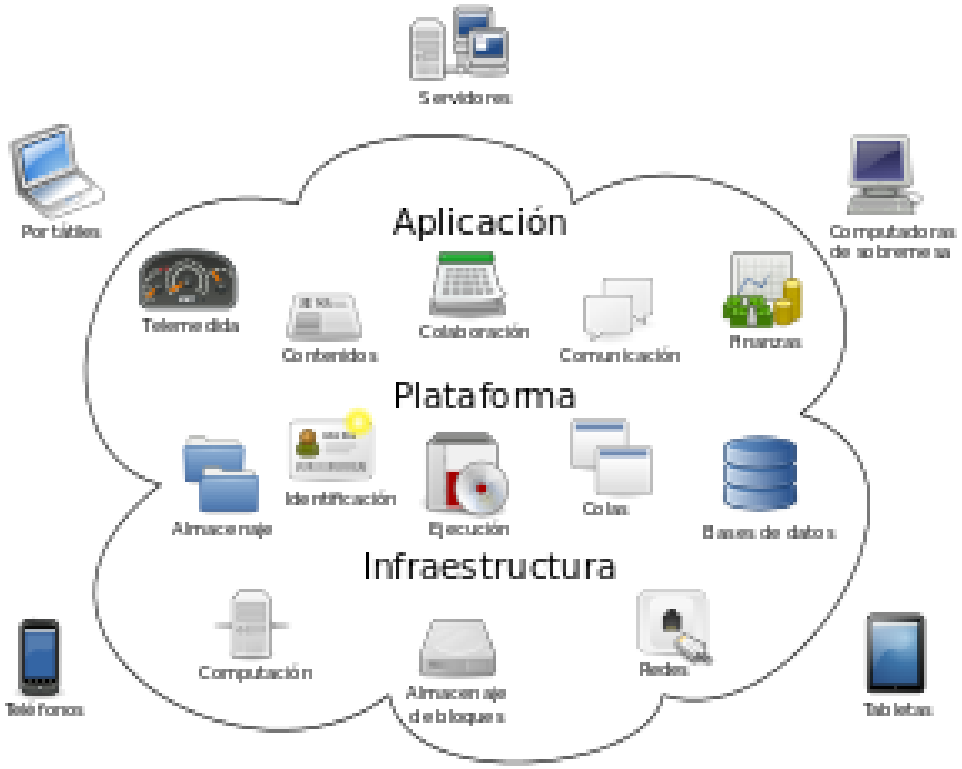
Contenido

- La Nube
- Big Data
- Internet de las Cosas
- SDN
- Seguridad Cuantica

El Futuro

La Nube (Cloud)

es un “paradigma” que permite ofrecer servicios de computación a través de una red, que usualmente es Internet



Computación en la nube

El Futuro

Big Data

Concepto que refiriere el almacenamiento de grandes cantidades de datos, y a los procedimientos usados para encontrar patrones repetitivos dentro de esos datos.

El Futuro

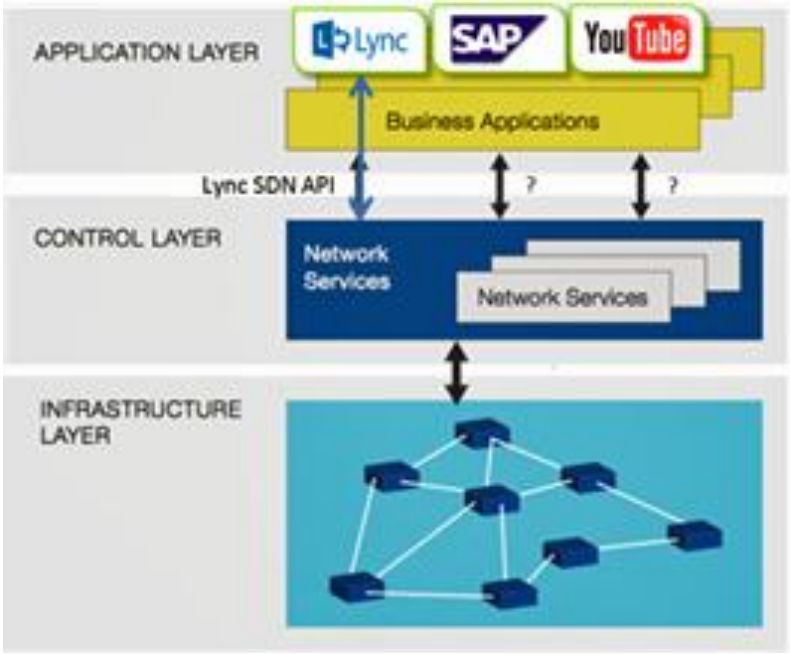
Internet de la cosas (IoT)

Se refiere a la interconexión digital de objetos cotidianos vía Internet (o alguna red).

El Futuro

Software Define Networks (SDN)

Redes definidas por software (SDN) son redes cuyo plano de control (software) es totalmente independiente del plano de datos (hardware), logrando con ello facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel.



El Futuro

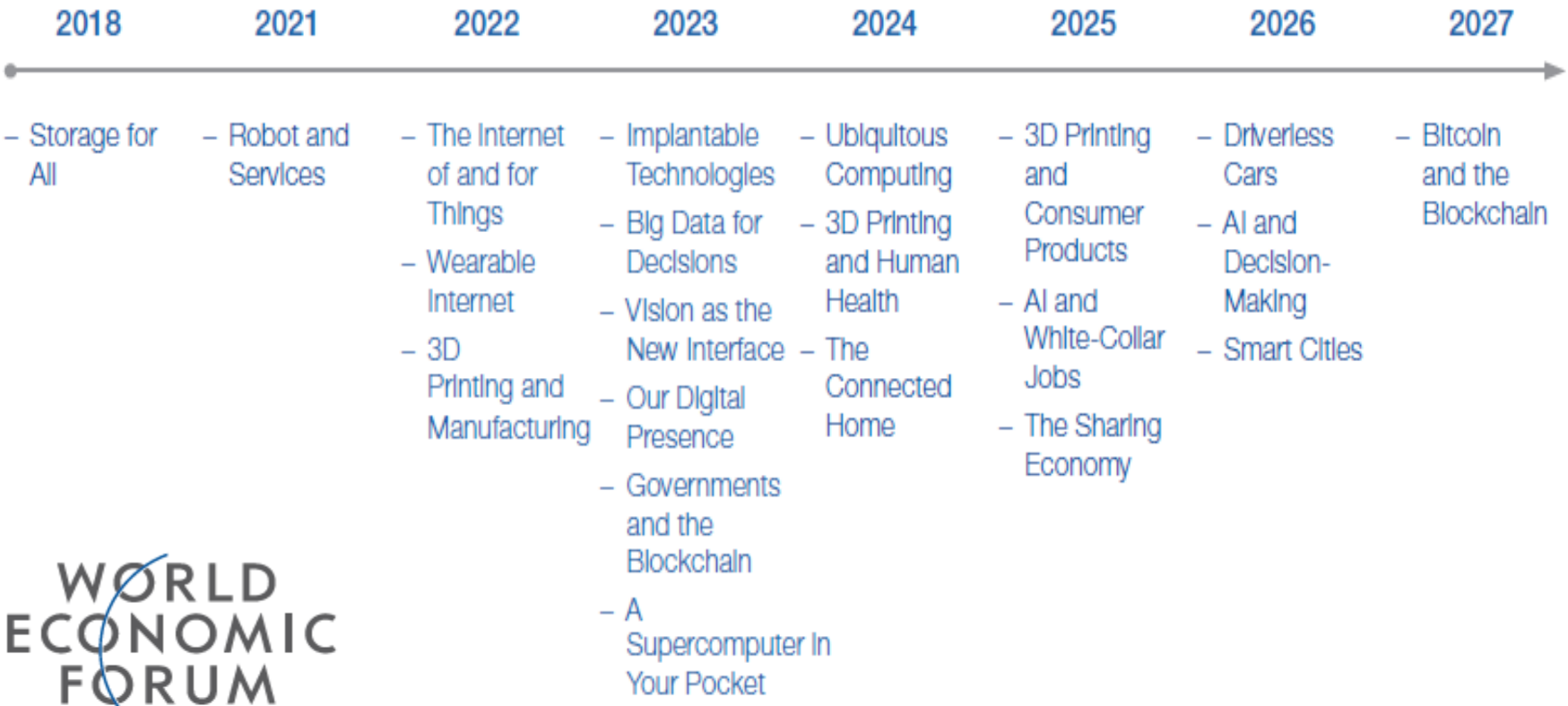
Seguridad Cuántica

- Ya hay dos protocolos:
  - BB84 de Bennet y Brassard, 1984 Angulo de rotación del fotón.
  - E91 de Artur Ekhert, 1991, pares de fotones enlazados.
- Se basa en transmitir fotones polarizados que representan 1's y 0's.
- BB84 operativo a nivel de laboratorio desde 1995 y hay productos en uso desde 2002 (restringidos en distancia).
- Permite detectar si esta siendo leída por terceros.
- Se considera indescifrable (pero en la historia de la criptografía que no lo ha sido?).

Cualquiera que pueda contemplar la mecánica cuántica sin sentir vértigo es que no la ha comprendido.

Niels Bohr

El Futuro



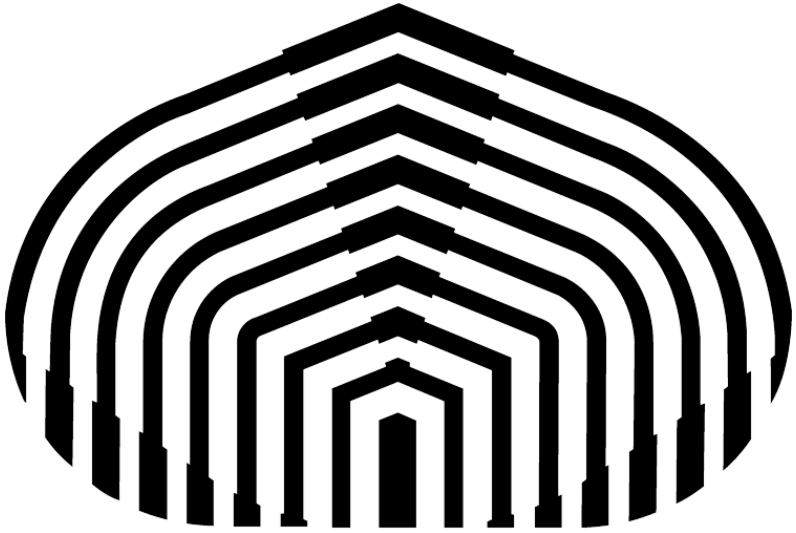
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Survey Report, September 2015

Bibliografía

- Stallings, W. Comunicaciones y Redes de computadoras , 6ta Edición. Prentice Hall.
- Tanenbaum. Redes de Computadores.
- Halsall, F. Data Communications, Computer Networks and Open Systems, Addison Wesley.



USB