TEMA 8
SEGURIDAD

- Dos planteamientos diferentes:
  - Seguridad de los datos: está referida a la integridad y autenticidad de los datos que transitan a través de redes de comunicaciones.
  - Seguridad de las redes: está referida a la protección de dispositivos y redes privadas en general ante ataques externos orientados a su corrupción o captura de datos internos, así como a la destrucción de los servicios que dichas redes ofrecen a Internet.

8.1. SEGURIDAD DE LOS DATOS

- Conjunto de conceptos y protocolos para asegurar la confidencialidad de la información que viaja por las redes.
- Inicialmente los datos estaban orientados a correo electrónico y compartición de impresoras y documentos. Ahora las redes transmiten datos de millones de personas que realizan transacciones bancarias, compras, declaraciones de impuestos etc.
- Los problemas de seguridad de los datos se pueden dividir en:
  - Secreto: información accesible solo para entes autorizados.
  - Validación de la identificación: identificación del ente autorizado
  - No repudio (firmas): que la información sea la original del emisor.
  - Control de la integridad: los recursos de un computador solo sea modificable por entes autorizados
- En el tema de seguridad de los datos, cada capa puede contribuir, pero la validación de la identificación y el no repudio solo se controla desde la capa de aplicación.
- Tipos de ataques:
  - Ataque pasivo: son escuchas y monitorizaciones sin modificación de los datos. Dificil de detectar, pues no modifican los mensajes. La solución es la prevención.
  - Ataque activo: modificación del flujo de datos o creación de flujos falsos.

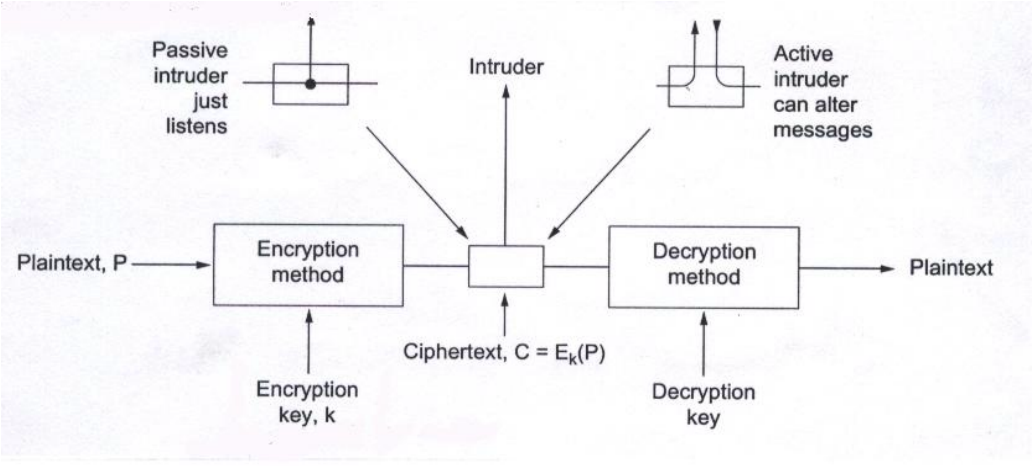


Fig 8.1

8.1.1. Cifrado tradicional o convencional

- Es el cifrado mas utilizado
- El método general de cifrado es conocido, es decir, el algorítmo de cifrado es público.
- El secreto real es la clave, y su longitud es un aspecto importante del diseño. Cuanto mayor sea la clave, mayor será el factor de trabajo (tiempo) para cescifrar el mensaje. Para descifrar las claves hay dos procedimientos:
  - Criptoanálisis ("arte" de descifrar): se suele disponer de alguna información previa del mensaje, del mensaje cifrado y de las características del algoritmo.
  - Fuerza bruta: comprobar todas las claves posibles. En claves de 32 bits, se localiza esta en máquinas modernas en unos minutos. Claves de 128 bits son necesarios billones de años.
- Dos tipos genéricos de cifrados (algoritmos):
  - Cifrado por sustitución: sustitución monoalfabética.
  - Cifrado por transposición y transformación: reordenación alfabética.

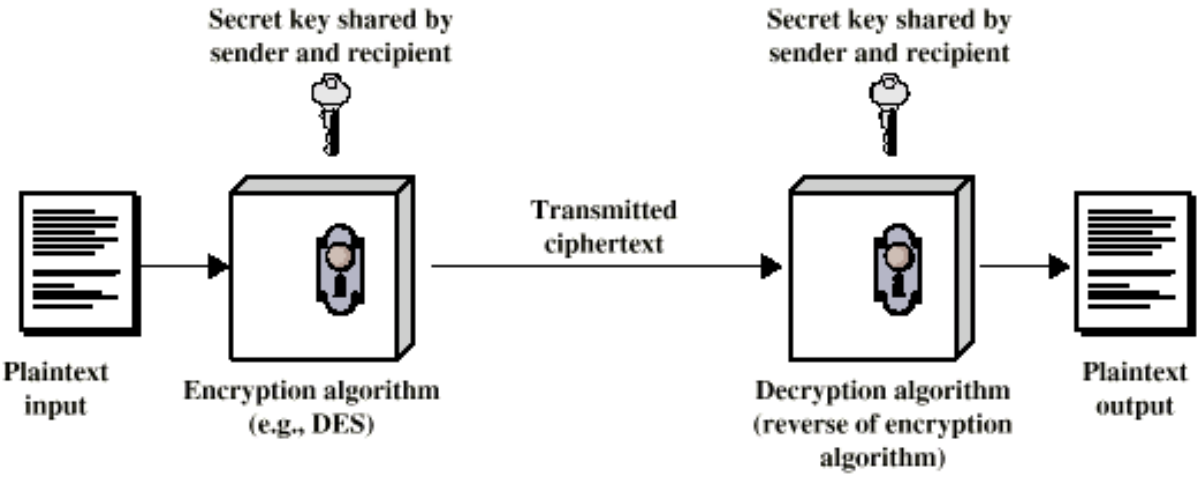


Fig. 8.2

8.1.2. Cifrado Moderno

- Se basa en las mismas ideas que el cifrado tradicional (sustitución y transposición), pero con un algoritmo tan complicado y rebuscado que el criptoanálisis será inocuo contra él.
- Las transposiciones y sustituciones se pueden implementar con circuitos sencillos.
- La potencia real se hace aparente cuando ponemos en cascada una serie de cajas para formar un cifrado de producto.

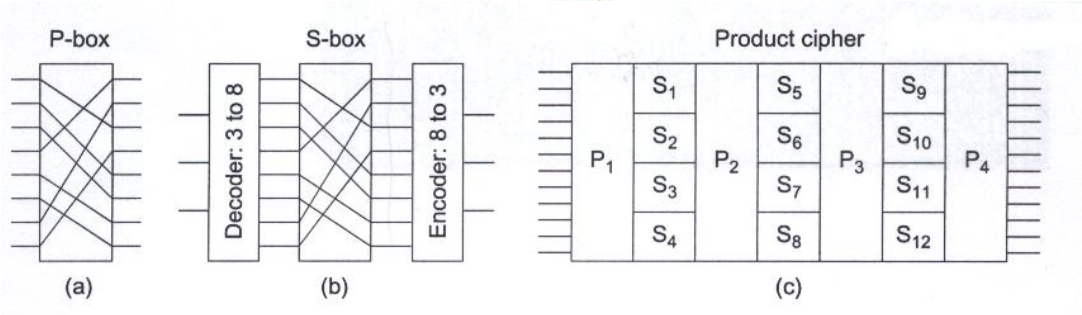


Fig. 8.3

- Como ejemplo la figura 8.2 indica cajas tipo P (transposición) y tipo S (sustitución). El apartado (a) indica una transposición normal, el apartado (b) hace una conversión binaria → decimal (8 cifras), una transposición y una deconversión. Si la entrada es 01234567:
  - (a) sale 36071245
  - (b) sale 24506713
  - (c) ?????

- Algorítmo DES (Data Encription Standart)
  - Es un algorítmo moderno por etapas. Utiliza el algorítmo DEA.

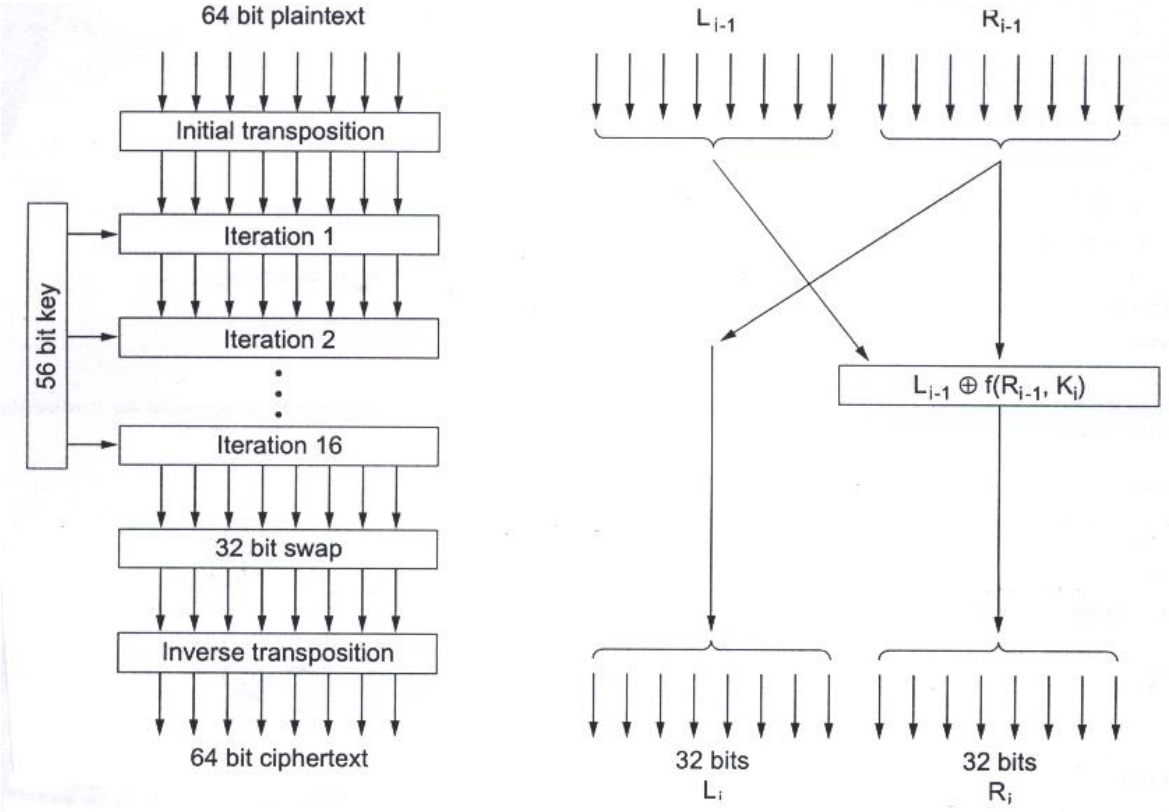


Fig. 8.4

- Fue desarrollado por IBM y adoptado por el gobierno de EE.UU. Este hecho trajo mucha controversia, pues diversos estudios indican que puede ser descifrado con muchas máquinas pequeñas.
- En 1998 con una máquina de 250.000 dólares fue descifrada la clave en menos de 3 días y se declaró muerto para agencias. Sigue utilizándose en corporaciones que no necesitan muy alta seguridad de sus datos.
- Tras él se utilizó el DES por etapas (DES triple) y otros algorítmos.

8.1.3 Dispositivos de cifrado:

- Cifrado de enlace: solo en Wan's privadas. Se usa para cifrar las cabeceras de direccionamiento. Es vulnerable en los nodos, pues estos tienen que descifrar el paquete para leer la cabecera de direccionamiento y poder encaminarlo. Es caro pues hay que poner dispositivos en cada enlace.
- Cifrado extremo a extremo: el proceso de cifrado-descifrado se realiza en los sistemas finales. El destino comparte una clave con el origen, por lo que puede descifrar el mensaje.

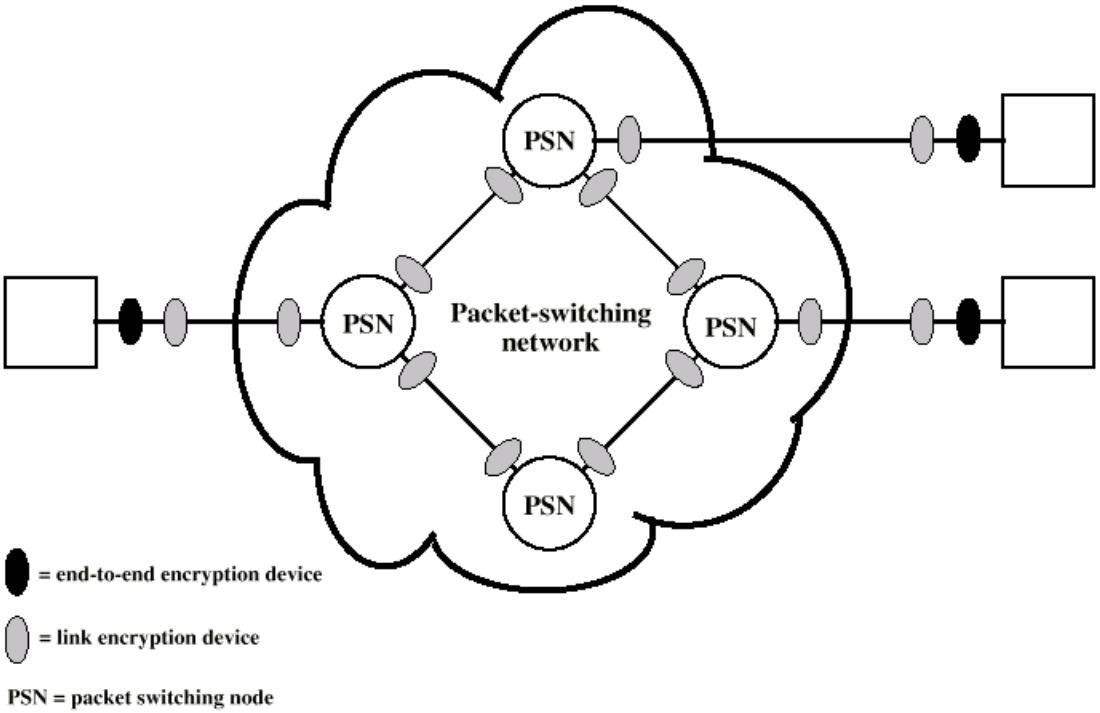


Fig. 8.5

8.1.4. Distribución de Claves

- Este es un problema crítico, pues en el cifrado tradicional y moderno, las claves las conocen tanto el emisor como el receptor. El problema está en la distribución de la clave.
- En la distribución de claves entre un computador A y otro B hay cuatro opciones:
  - A puede seleccionar una clave y entregarla directamente a B.
  - Una tercera parte neutra selecciona la clave y la entrega directamente a A y a B.

- Si A y B ya han tenido comunicación cifrada, se usa la clave previa para la transmisión de la clave nueva
- Si A y B tienen conexión cifrada a C, C es quien entrega la clave a A y a B.

- La última solución es la mas óptima en caso de distribución de claves entre muchos computadores y en caso en que se distribuyan claves con bastante frecuencia.
- La implementación es como sigue:
  - Inicialmente hay que distinguir entre dos tipos de claves:
    - Clave de sesión: clave que se usa durante una conexión lógica entre los computadores A y B.
    - Clave permanente: clave que se utiliza entre el computador A o B y el computador C. Se usa con el objetivo de distribuir claves de sesión.

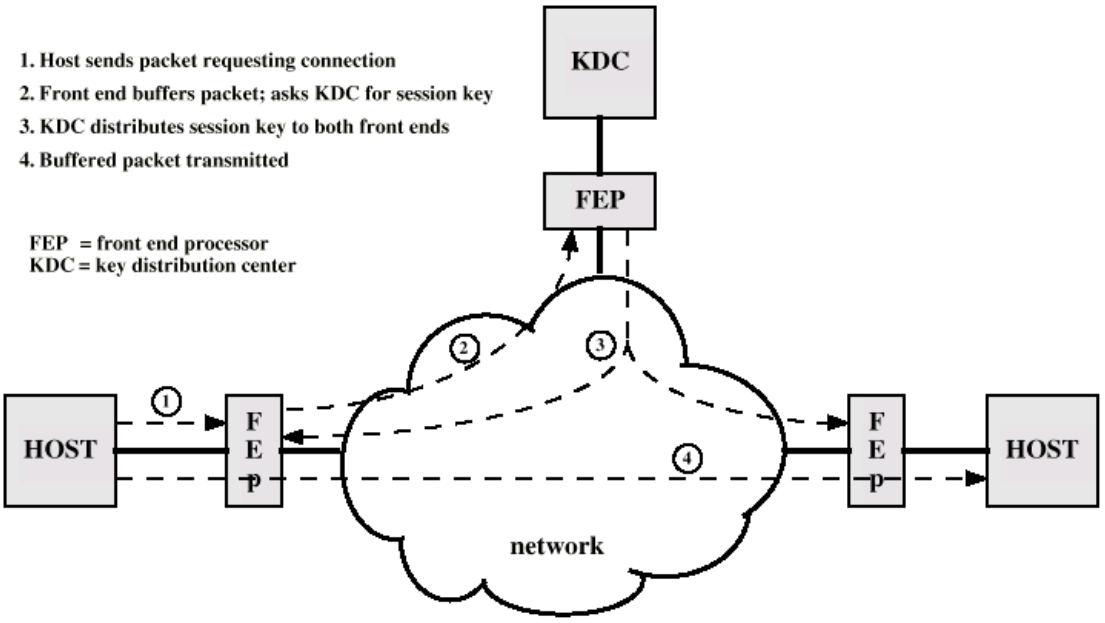


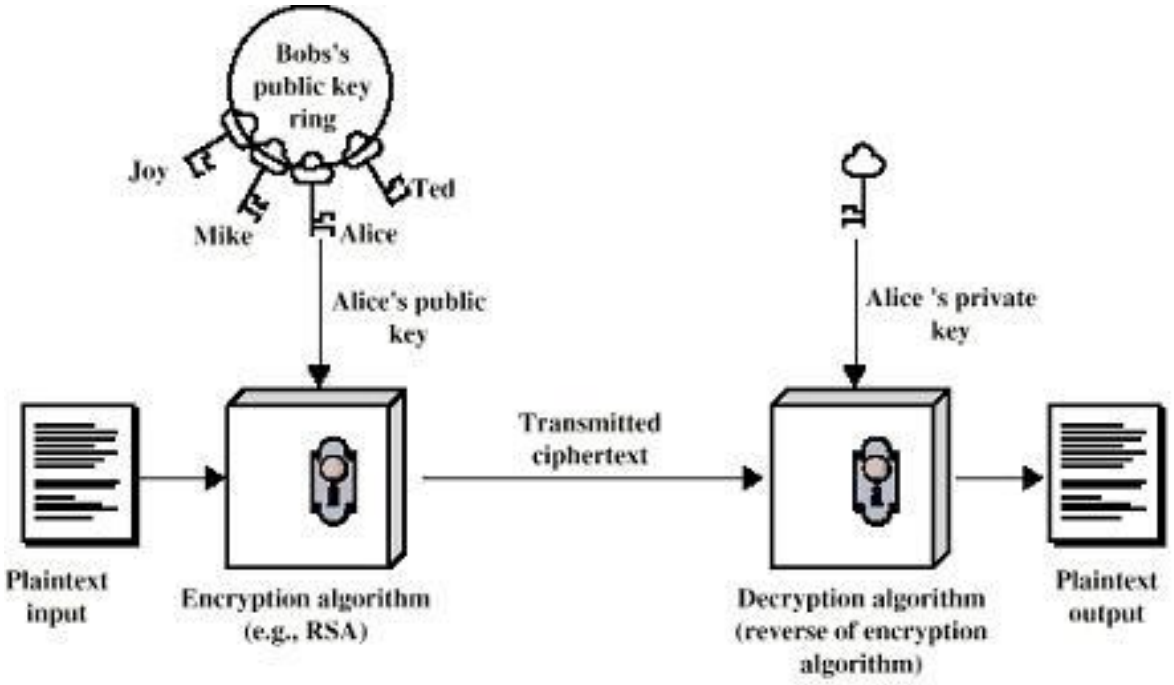
Fig. 8.6

- KDC o CDC: Centro de distribución de claves. Es el que proporciona claves de sesión a los computadores autorizados.
- FEP o PF: Procesador Frontal. Realiza el cifrado extremo a extremo y obtiene las claves de sesión en representación del host. Actualmente suele ser una capa de software dentro del host.
- A envia un paquete a C solicitando conexión a B. El procesador frontal (implementa el algoritmo) almacena los paquetes hasta que se establezca la conexión.
- Si el CDC aprueba la solicitud de conexión, genera una clave de sesión y la entrega a los dos hosts.
- El PF emisor libera los paquetes y se establece la comunicación cifrada con la clave de sesión dada por el CDC entre los dos hosts.

8.1.5. Algorítmos de clave pública. PKI

- Surgieron por la problemática de distribución de claves. El problema no es solo de distribución de la clave sino además de almacenamiento de la misma.
- Surgieron en 1976 en la Universidad de Stanford (Diffie y Hellman) y supuso una revolución en la criptografía en sus miles de años de historia.
- Están fundamentados en el hecho de que las claves de cifrado (D) y de descifrado (E) sean diferentes y tienen que cumplir 3 requisitos:
  - D(E(P))=P.
  - Es excesivamente dificil deducir D de E.
  - D no puede descifrarse si el intruso puede cifrar textos planos.

- Ejemplo de funcionamiento:
  - Ana quiere recibir mensajes secretos, para ello genera dos claves, Ea y Da, que cumplen los requisitos anteriores. El algorítmo y la clave Ea se hacen públicos. Sólo la clave Da permanece privada.
  - Juan quiere enviar un mensaje P cifrado a Ana. Coge la clave Ea y le aplica el algorítmo público al texto a enviar Ea(P).
  - Como solo Ana dispone de la clave Da, aplica el algorítmo y descifra el mensaje. Da(Ea(P)) = P

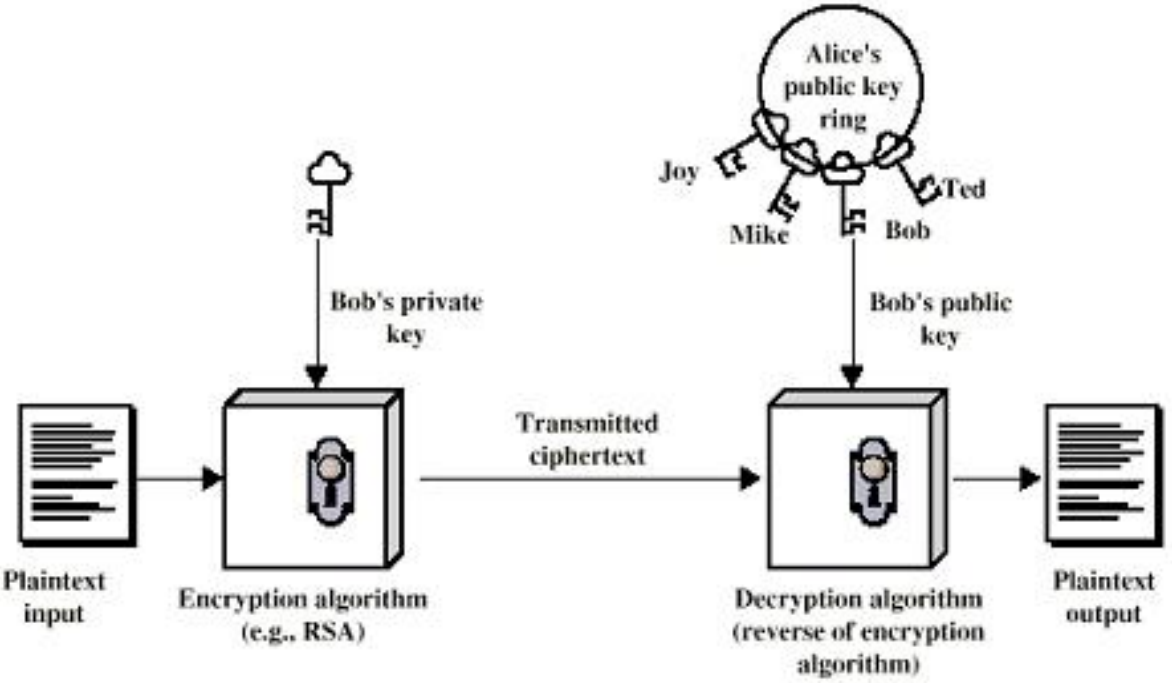


- Algorítmo RSA (Rivest, Shamir, Adleman)
  - Está basado en prinicipios matemáticos de la teoría de números.
  - Selección de claves:
    - Seleccionar dos números primos grandes, p y q (generalmente mayores de 10^{100}).
    - Calcular n=p*q, z=(p-1)*(q-1)
    - Encontrar e tal que e*d=1 mod z (e / e*d = 1 + m*z
      m Entero)

- Cifrado y descifrado.
  - Se divide el mensaje en bloques de tamaño k bits, donde $2^k<n$.
  - Calculamos:
    - $C=P^e \bmod n$ C=mensaje cifrado, P=mensaje original
    - $P=C^d \bmod n$
    - Así, la clave pública es (e,n) y la clave privada es (d,n).

- La seguridad del método se basa en la dificultad de factorizar números grandes. La factorización de un número de 200 dígitos puede requerir con máquinas actuales (2002) 400 millones de años.
- Se utiliza en las áreas de privacidad, distribución de claves y autentificación (firma electrónica)
- No es mejor un sistema de clave simétrica con respecto a uno de clave pública en lo que se refiere al criptoanálisis.

- Firmas digitales (Firma electrónica)
  - Aplicación directa de algorítmos de clave pública
  - El mensaje se autentifica en términos de la fuente e integridad de los datos.
  - El mensaje no está protegido contra escuchas, sino contra falsificación, pues cualquiera puede descifrar el mensaje con clave pública.



  - Funcionamiento básico:
    - Juan quiere enviar un mensaje autentificado para Ana.

- Juan encripta el mensaje con su clave privada. Solo él puede encriptarlo de esa forma
- Ana recibe el mensaje y utiliza la clave pública de Juan para desencriptarlo. Siel resultado es legible, tiene la certeza de que ha sido Juan quien lo ha enviado.

- Infraestructuras de clave públicas PKI
  - Sistema requerido para proveer cifrado de clave pública y servicios de firma digital.
  - Cada vez mas usados
  - Sirve para dar esos servicios a múltiples aplicaciones actuales, correo-e, formularios Web, etc
  - En general se utiliza un sistema de entidades certificadoras jerárquico o peer-to-peer.

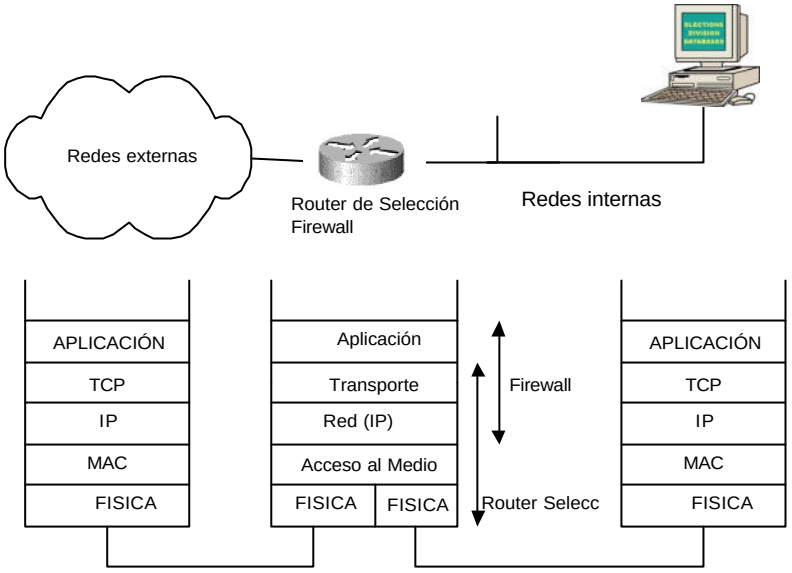
8.2. SEGURIDAD DE LAS REDES

- Zona de riesgo: todas las redes y máquinas a las que es posible acceder directamente a través de una red externa (internet).
- La seguridad de la zona de riesgo, se hace sobre la red, pues hacerla sobre todos los hosts es arduo y poco fiable.
- Política de seguridad: el conjunto de intereses de seguridad a os que está sujeta una red. (que guardar, que auditar, que proteger, cuanto cuesta, etc). Dos políticas diferentes en términos genéricos:
  - Todo lo que no está explicitamente prohibido está permitido. Política liberal, mas arriesgada y con auditorías contínuas para ser realmente efectiva como política de seguridad.
  - Todo lo que no está explicitamente permitido está prohibido. Política conservadora.
- Hay un RFC que trata el tema: RFC 1244.
- Arquitectura de seguridad: dispositivos tanto hardware como software implementados para establecer la política de seguridad. Normalmente son Firewalls (hardware o software). Proporciona un control y auditoría del acceso a los diferentes servicios de la red, habilitando un mecanismo que permita o bloquee de modo selectivo el tráfico entre las redes internas y externas.
- La seguridad está centrada en la entrada a las redes privadas y no a la salida de las mismas, estando no obstante ambas muy ligadas e implemntandose soluciones conjuntas.

8.2.1. Firewalls

- El concepto de firewall es bastante genérico, resumiendose en dos tipos.
  - Routers de selección: disponen de capacidad de seleccionar paquetes basándose en criterios como el protocolo, el puerto, dirección, campos de control etc. Se suelen fabricar en conjunto hardware-firmware y abarcan las 3 capas inferiores del modelo TCP/IP. A nivel Software están para Linux (LRP) “iptables, ipchains, ipfwadmin”. Normalmente lo que vienen de fábrica, no tienen posibilidad de auditoria.

- Gateways de Firewall: dejan subir los paquetes de la capa de transporte hasta la de aplicación para disponer de mas información. Suelen ser proxys y proporcionan mecanismos para requerir autentificación.



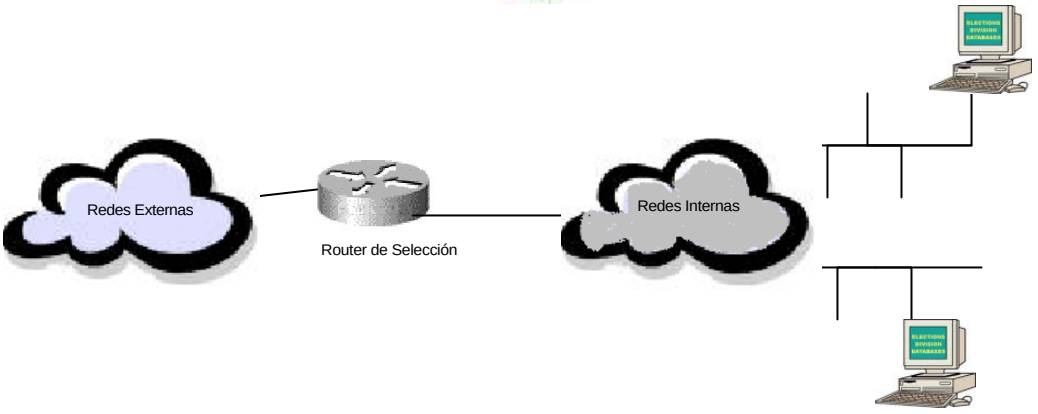
8.2.2. Arquitecturas básicas de seguridad.

- Bastion host: equipo identificado por el administrador como punto crítico de seguridad. Requiere politicas de seguridad de sistema específicas, como:
  - Eliminar cuentas de usuario superfluas.
  - Eliminar demonios de apertura de puertos superfluos.
  - Activar auditorias (logs).
  - Desactivar las funciones de reenvio TCP/IP.
  - Revisiones frecuentes y actualizaciones y parcheos.

  Suelen ser equipos con algún tipo de servicio a las redes externas (Servidores Web, de aplicaciones, ftp, o incluso el propio firewall, etc.).

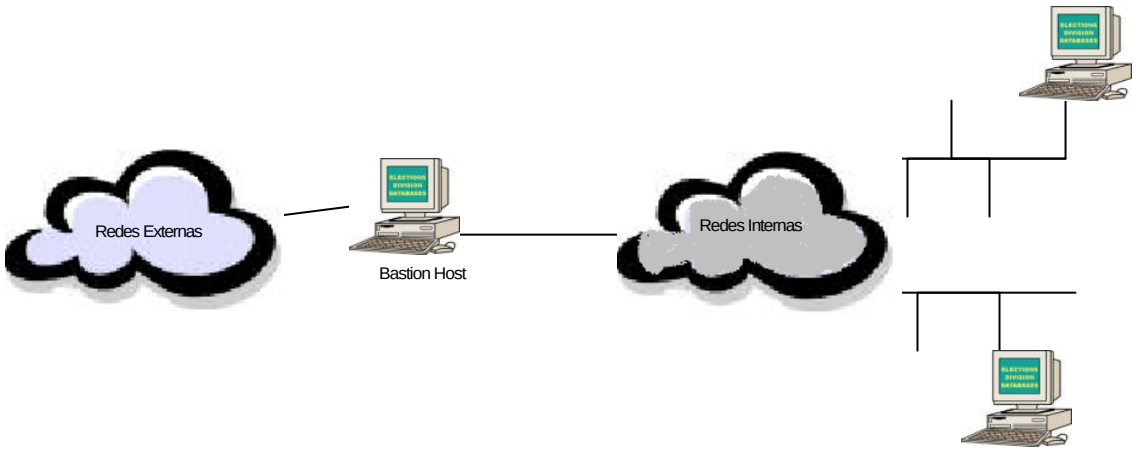
- DMZ (De-Militarized Zone ozona desmilitarizada): zona entre un router de selección y una red interna que tiene equipos no considerados críticos.
- Todas las arquitecturas están fundamentadas en las consecuencias que tendría un fallo en la seguridad.
- Algunas arquitecturas:

  - Solo router de selección:



En esta configuración, los paquetes son filtrados a nivel de las tres capas inferiores del conjunto TCP/IP. En caso de "destrucción" del router, sería muy dificil de descubrir y toda la red privada quedaría al descubierto.

- Solo Bastion Host



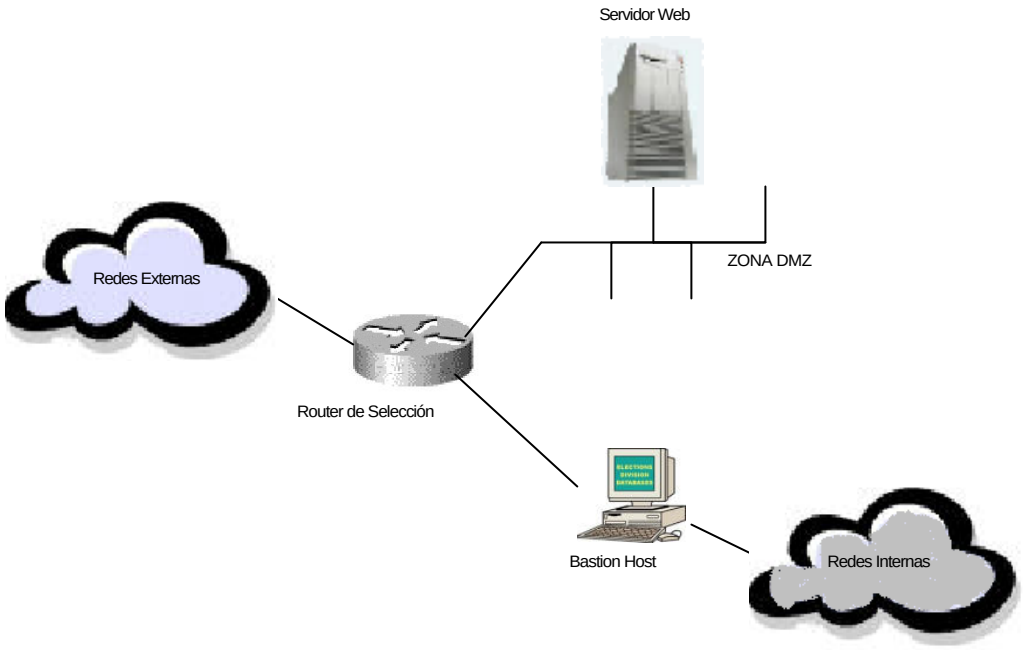
Las posibilidades son mayores:

Se puede hacer que sea un firewall de aplicación, permitiendo el acceso a solo algunas aplicaciones, o habilitar un acceso muy protegido desde el cual se pueda ver la red exterior.

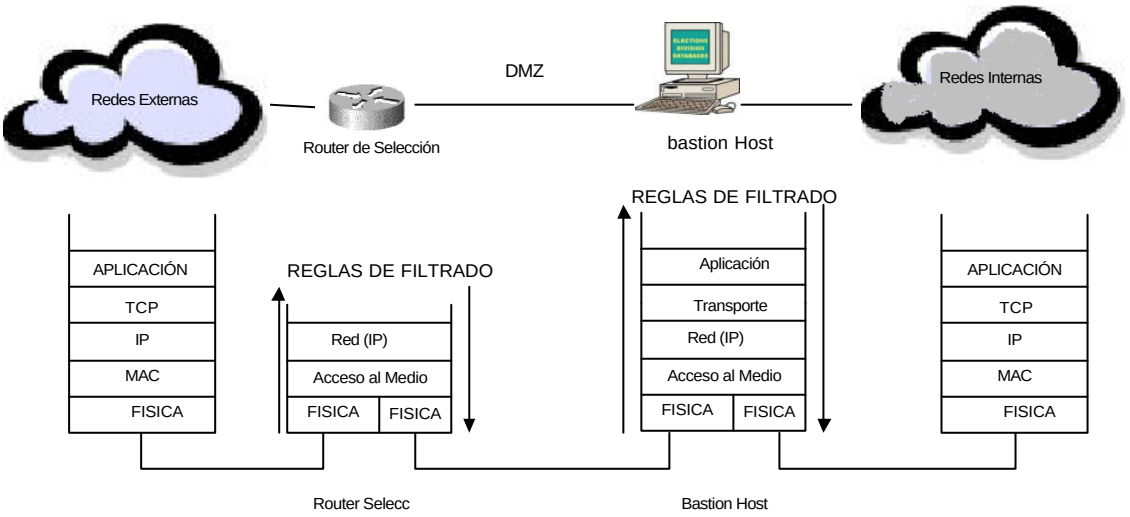
Permite mantener log's de las acciones que se están acometiendo, pudiendo tomar medidas oportunas. Se desabilita el IP_forwarding.

Si se ataca tiene consecuencias parecidas al router de selección.

- Router de selección y Bastion Host. Zona DMZ



Solución mejor que las anteriores, dejando una zona menos restringida para el acceso pues sirve al público en general y zona de acceso restringido para aplicaciones y servicios internos. Un esquema de capas sería:



Bibliografía:

Stallings, comunicaciones y redes de computadores.
A. Tannenbaum, Redes de Computadoras
Charlie Scott, Virtual Private Networks.
http://www.cisco.com