Fibernet

Cifrado de comunicaciones ópticas

1. ¿Por qué cifrar los enlaces ópticos?
2. Descripción de un sistema criptográfico
3. Soluciones de cifrado de **Fibernet**

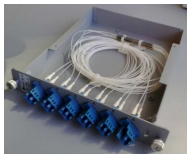
¿Por qué cifrar los enlaces ópticos?

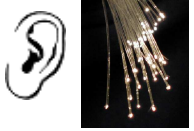
FiberNet

¿Se pueden espiar los datos de una fibra óptica?

- ✓ En general, podemos pensar que la fibra es más segura que las conexiones eléctricas cableadas o, especialmente, radiadas.
  - La radiación electromagnética es más fácilmente "espiable"
  - Las fibras suelen localizarse en sitios poco accesibles (enterradas, etc.)

- ✓ Pero las fibras también pueden ser "pinchadas"
  - Insertando *splitters* (normalmente en puntos de conexión)
  - Incluso sin llegar a cortar la comunicación



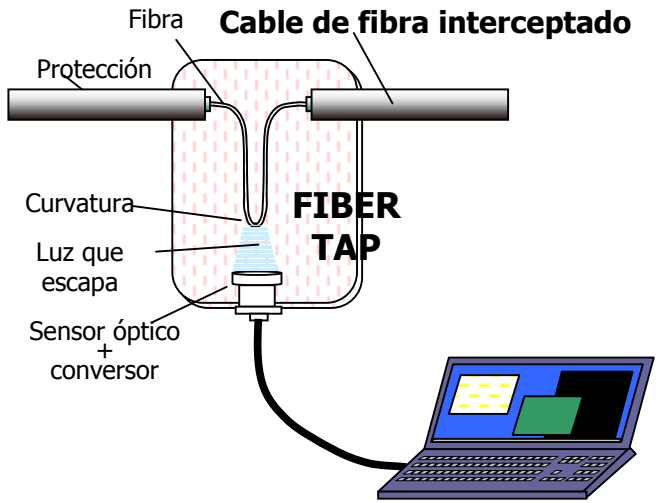


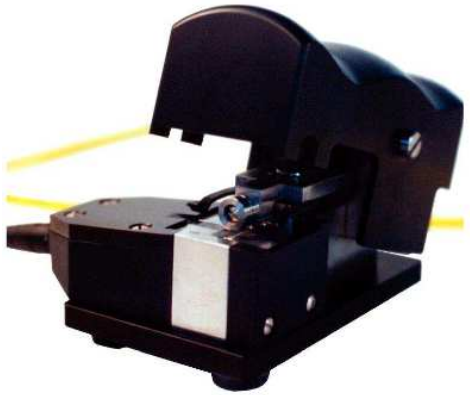
FiberNet

Espiar sin cortar la comunicación

Se basa en hacer que una pequeña porción de luz escape de la fibra

- ✓ Basta extraer un pequeño porcentaje de la potencia de señal
- ✓ Por ejemplo, mediante una doblez en la fibra





- ✓ Existen múltiples dispositivos comerciales, disponibles a un coste no prohibitivo, capaces de extraer señal de la fibra de esta manera

FiberNet

Potencial de la fibra como fuente de información

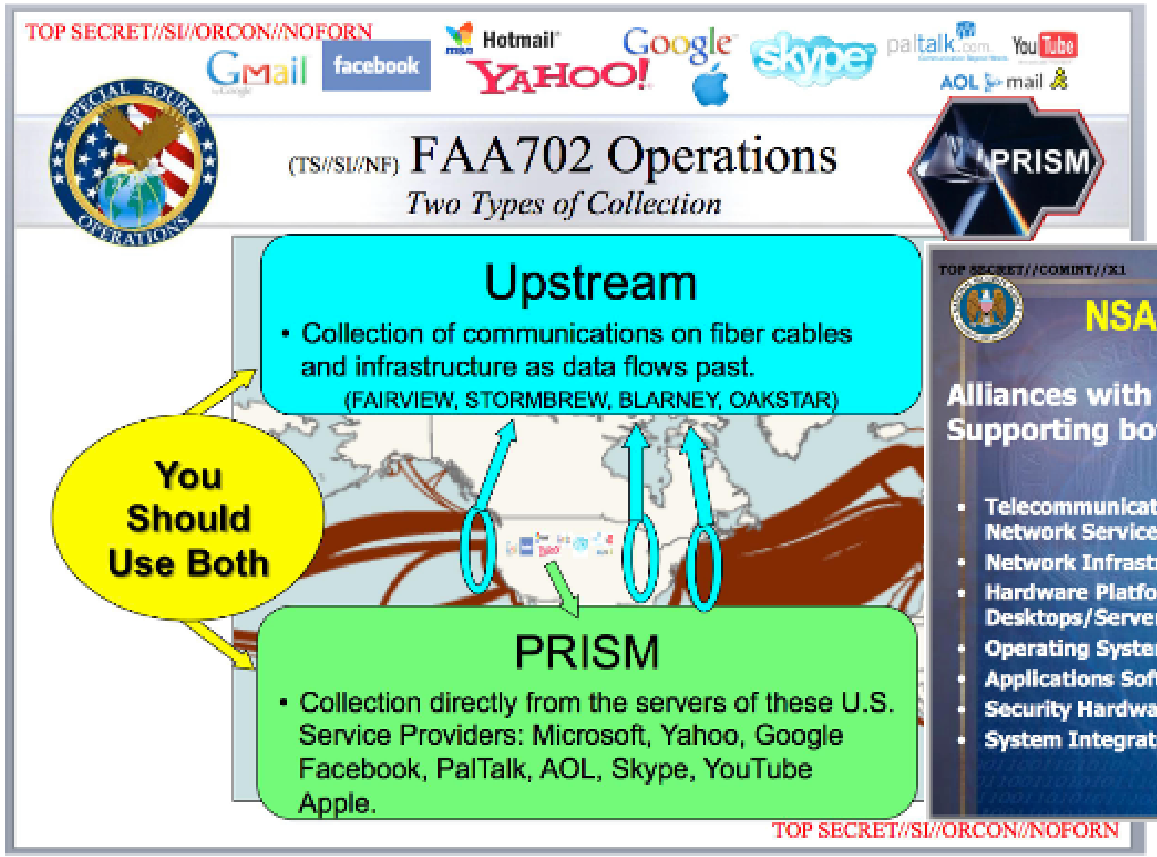
- ✓ La cantidad de datos y su concentración resultan tentadores
- ✓ Existe la tecnología y los interesados tienen amplios recursos

Se puede incluso pagar el uso de costosos submarinos para interceptar comunicaciones.

Ejemplo: en 2005 la prensa hablaba del submarino USS Jimmy Carter (> 3000 M$), especulándose sobre su dedicación al espionaje de comunicaciones

- ✓ No es, en absoluto, algo nuevo

Los archivos del ex-agente de la CIA Edward Snowden no sólo revelaron que el espionaje de la fibra se hace, sino también que incluso se cuenta con cierta ayuda ...



¿Cómo proteger la fibra?

Ante estas amenazas se pueden hacer tres cosas:

- ✓ Velar por la **seguridad física** de las instalaciones
  Recintos controlados, empalmes antes que conectores, etc.

- ✓ **Detectar posibles manipulaciones** no deseadas de la fibra
  Uso de equipos capaces de detectar cortes, variaciones de atenuación, etc.

  ⇨ Producto ***Fibersec*** de **Fibernet**

- ✓ **Cifrar los datos** que la fibra porta

  ⇨ Gama de ***tarjetas con cifrado*** de **Fibernet**

Lo ideal es aplicar todas estas medidas; a continuación se comentará el **CIFRADO**.

FiberNet

¿Cómo cifrar los datos?

Hay tecnologías muy extendidas en la industria para cifrar extremo a extremo

- ✓ Ej.: IPSEC - Protección de comunicaciones IP (cifrado, protección de integridad, autenticación), aplicable en general o para determinadas comunicaciones.

Soluciones buenas si se aplican correctamente, pero:

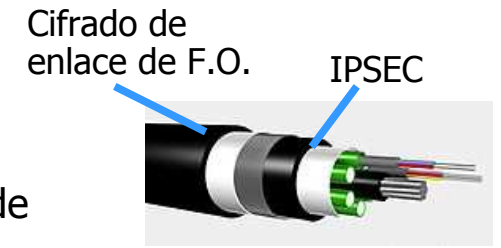
- ✓ No están libres de vulnerabilidades si hay descuidos en su aplicación.
  - Hay constancia de ataques con éxito (ej.: revelaciones de Snowden)
  - P.ej. IPSEC es una tecnología muy compleja, con múltiples opciones de configuración, con implementaciones variadas (según el sistema operativo, etc.) y con muchos atacantes. Se requiere una alta experiencia.
- ✓ Pueden reforzarse añadiendo protección en el tramo físico menos seguro: el que recorre la fibra.

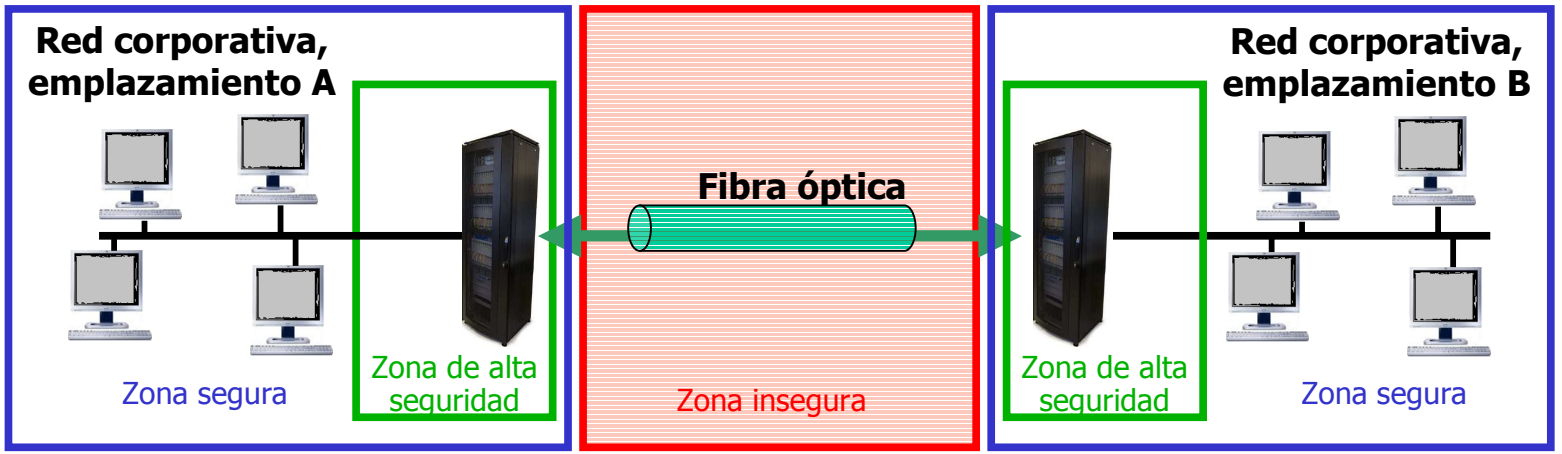
Por otra parte, un cifrado hardware del enlace de fibra no consume recursos de los equipos existentes ni introduce latencias perceptibles.

FiberNet

Seguridad reforzada

Igual que un cable de fibra emplea múltiples capas protectoras, presentes o no según el tramo del recorrido, también podemos dotar a nuestro esquema de seguridad de varias capas.





Cifrado de Fibra

IPSEC …

Descripción de un sistema criptográfico

FiberNet

Objetivo: proteger los datos en la fibra óptica → Criptografía Pero... ¿qué es?

- ✓ La idea central es la de ***ocultar la información*** a personas u organizaciones no autorizadas ("cifrado" o "encriptación").

  R.A.E: "*Arte de escribir con clave secreta o de un modo enigmático*".

- ✓ Más cosas a considerar: **autenticación de interlocutores**, **gestión de claves**, etc. Así, la criptografía se refiere al conjunto de técnicas para garantizar ***comunicaciones seguras*** en presencia de posibles "adversarios".

  Wikipedia (ES): "*Algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican*".

  Wikipedia (EN): "*The practice and study of techniques for secure communication in the presence of third parties (called adversaries)*".

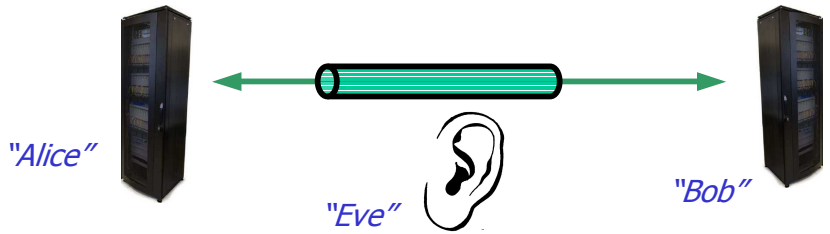
Un sistema de seguridad sólo es tan fuerte como el más débil de sus elementos

FiberNet

Amenazas a las que enfrentarnos

Protección:

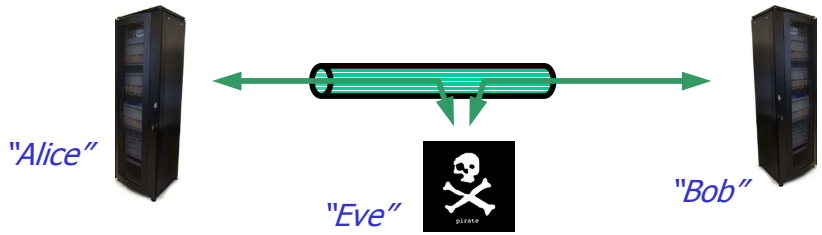
1. Escuchas indebidas



Cifrado

(o "encriptación")

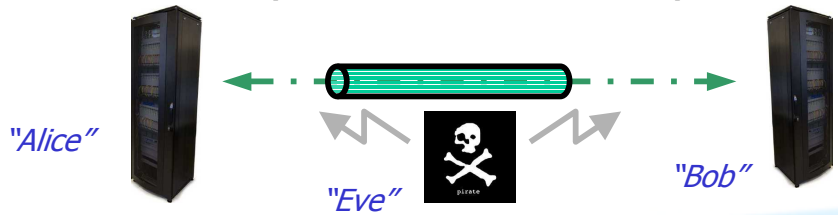
2. Suplantación ("man in the middle")



Autenticación

(o "autentificación")

3. Ataques al servicio (*DoS, Denial of Service*)



Filtrado de puertos, etc.

(De menor interés en enlaces punto a punto)

FiberNet

La importancia de usar tecnología bien conocida

Al contrario de lo que pudiera parecer, el conocimiento del sistema no lo pone en peligro, sino que da más garantías sobre su eficacia.

- ✓ Algoritmos complejos, pueden esconder debilidades o incluso características malintencionadas.
- ✓ Amplia comunidad de expertos en criptografía, dedicados a analizar algoritmos, contrastarlos con teorías matemáticas, atacarlos para comprobar su grado de seguridad, etc.

Principio de Kerckhoffs*: La seguridad de un sistema criptográfico debe depender sólo de la confidencialidad de la clave, no de la del algoritmo.*

National Institute of Standards and Technology

NIST National Institute of Standards and Technology U.S. Department of Commerce

Internet Engineering Task Force

IETF

Cifrado de Fibernet

- ✓ A continuación se comentará un enfoque de Fibernet al problema del cifrado de un enlace de fibra.
- ✓ Se trata de una solución hardware.
- ✓ El cifrado se efectúa en la capa de enlace.
- ✓ Se aplica a diversos protocolos de comunicaciones.

FiberNet

¿Qué algoritmo de cifrado utilizar para proteger los datos en la fibra?

Cifrado simétrico

- ✓ Se utiliza la misma clave para cifrar y para descifrar
- ✓ Más rápido, típico para comunicación de datos a alta velocidad
- ✓ Ej.: DES, Triple DES, AES

⇒ Adecuado para los **datos** de una comunicación sobre **fibra óptica**.

Cifrado asimétrico

- ✓ Algoritmos de clave pública y clave privada
- ✓ Cada agente cifra con la clave pública de su interlocutor y el resultado sólo puede descifrarse con la clave privada.
- ✓ Potente y facilita el problema de la distribución de las claves, pero ...
- ✓ .. más complejo y lento, demasiado lento para comunicaciones a alta velocidad (a menudo aplicado en autenticación)
- ✓ Ej.: RSA

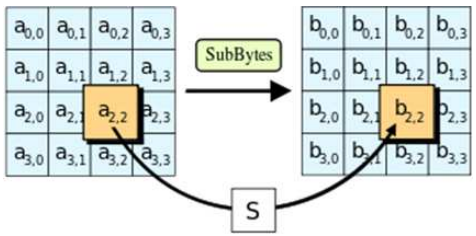
FiberNet

Cifradores de bloque

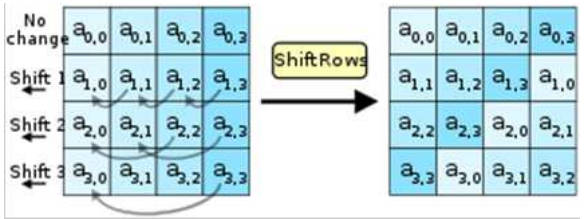
- ✓ Funciones de cifrado que trabajan sobre bloques de datos de tamaño fijo.
- ✓ Los cifradores de clave simétrica más utilizados lo son: DES, TDES, **AES**

AES (*Advanced Encryption Standard*) { **bloques de 128 bits (4x4 bytes)**
clave de 128, 192 o 256 bits

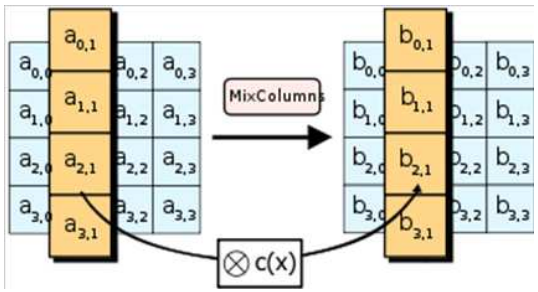
Transformaciones: sustituciones, permutaciones, mezcla con clave ... :



Substitución de bytes (S-box)

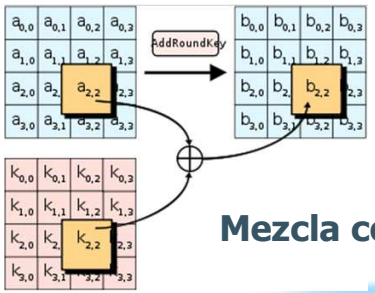


Desplazamientos en filas



Combinaciones por columnas

(a la inversa para descifrar)



Mezcla con clave

FiberNet

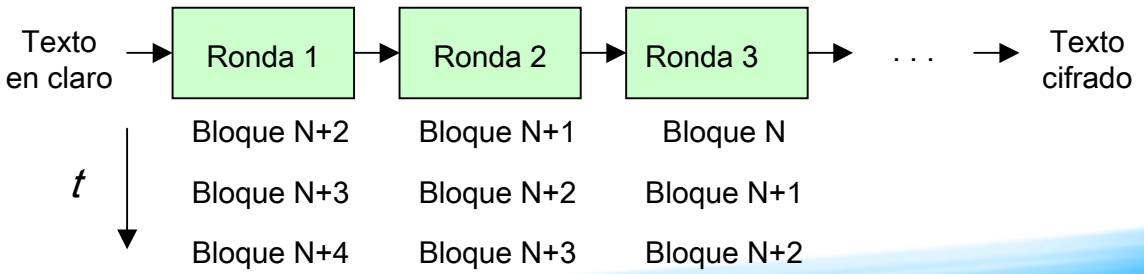
Rondas del AES

- ✓ Las anteriores etapas se repiten un número de "rondas" (ej. 14 rondas si la clave es de 256 bits)
- ✓ En cada ronda se utiliza una "clave de ronda" derivada de la clave definida.
- ✓ En conjunto:
  - La clave afecta de una forma complicada a la salida
  - Cualquier cambio en la entrada produce grandes variaciones en la salida

Claude Shannon

Implementación en hardware

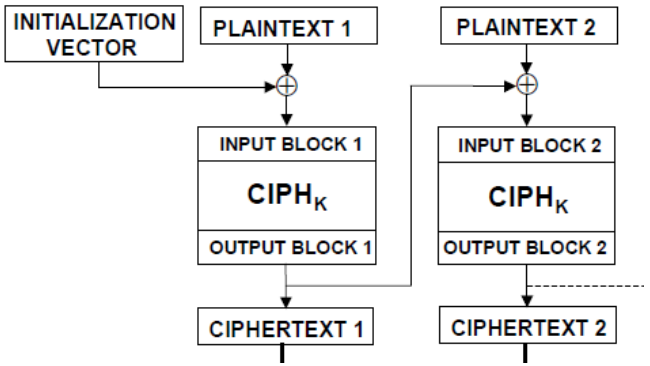
- ✓ Es posible combinar etapas
- ✓ Se puede utilizar "pipelining"



FiberNet

El problema del modo "*Electronic Codebook*" (ECB)

- ✓ Dos bloques de entrada al AES idénticos dan dos bloques de salida idénticos.
  No deseable, especialmente cuando puede haber datos "típicos".
- ✓ Para solventarlo: "**modos de operación**". *Modo ECB* = cifrador sin más.
  Ejemplo: Modo CBC

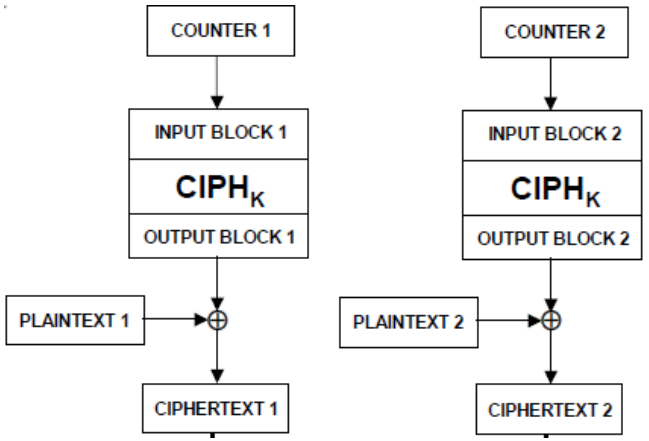


- ✓ Cada operación de cifrado depende del resultado cifrado anterior -> salidas diferentes
- ✓ **Problema**: la realimentación acaba con la posible ventaja del "pipelining"
  Las comunicaciones en fibra óptica alcanzan velocidades muy altas.
  → ¡No disponemos de mucho tiempo!
  Ej.: Comunicación 10 Gbps, bloques de 128 bits → 1 bloque cada 12.8 ns

FiberNet

El modo "*Counter*" (CTR)

- ✓ En vez de cifrar los datos, se cifra una secuencia numérica conocida por ambos interlocutores (contador).
- ✓ El texto cifrado se obtiene mezclando con XOR el contador cifrado con los datos en claro.



- ✓ Se mantiene la posibilidad de implementar un pipeline, pues no hay lazos de realimentación.
- ✓ Ventaja adicional: no hay cifrador y descifrador AES, el cifrador vale para ambos propósitos (*C xor R = [P xor R] xor R = P*).

El modo CTR es de utilización habitual cuando se trata de transmisión de datos de alta velocidad

FiberNet

Protección dada por el AES

- ✓ El AES (FIPS-197) es un cifrador concienzudamente diseñado y muy probado.
- ✓ Es el algoritmo estándar de referencia para cifrado de datos de alta velocidad.
- ✓ En principio la protección será mayor cuanto más larga sea la clave utilizada.

➡ Selección de la clave más larga: **256 bits**

Representa $2^{256} \sim 10^{77}$ combinaciones posibles

... probabilidad ganar Premio Especial Lotería Primitiva: ~ $1 / 10^{8.}$

... un super-ordenador a 10 GHz que pudiese probar 1 combinación por ciclo tardaría más de 10^{59} años en probarlas todas, muchas veces la edad del universo

Duración de la clave

Aunque parece imposible romper el cifrado por fuerza bruta...

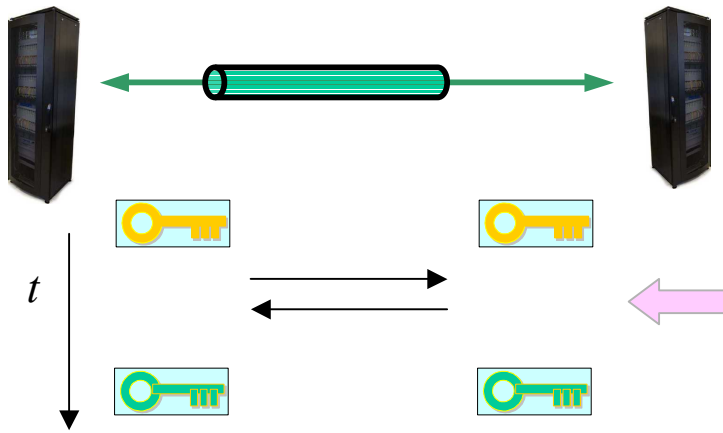
- El enlace de datos puede estar activo mucho tiempo (años...)
- La cantidad de datos transportada es gigantesca (años a 10 Gigabit / segundo...)
- Para garantizar la seguridad del modo CTR se necesita que todos los valores del "contador" que utilicemos sean únicos para una clave dada.

➡ Estaría bien poder cambiar la clave cada cierto tiempo

FiberNet

Intercambio (negociación) de claves

Nos permite determinar la clave a utilizar y cambiarla con cierta frecuencia.



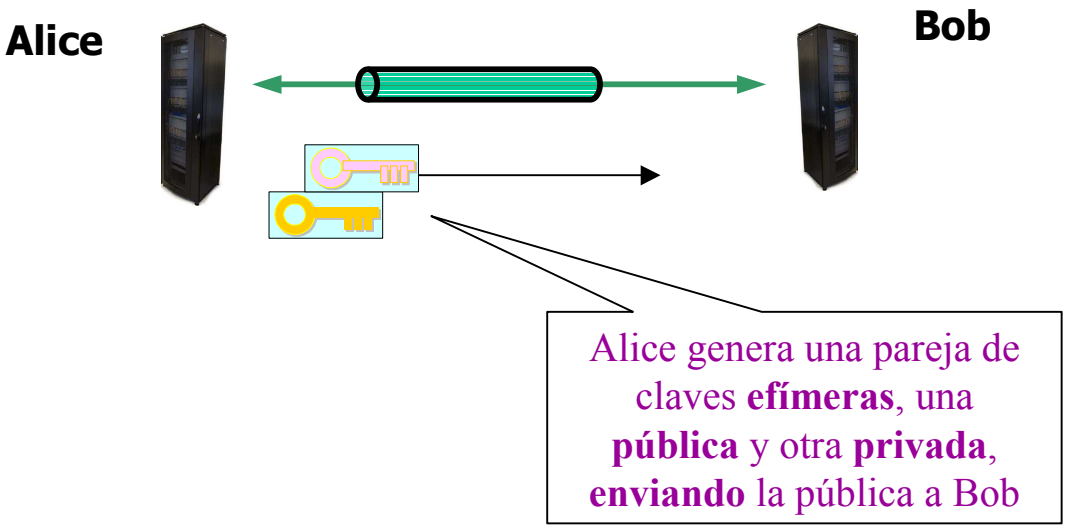
"Intercambio de claves" = intercambio de información que permita definir en ambos extremos una misma clave nueva.

La clave NO circula por el canal.

- ✓ El mecanismo de negociación de claves más utilizado es el algoritmo de **Diffie-Hellman**, estandarizado por NIST (SP800-56A) y por las RFC de IETF (2409:IKE).

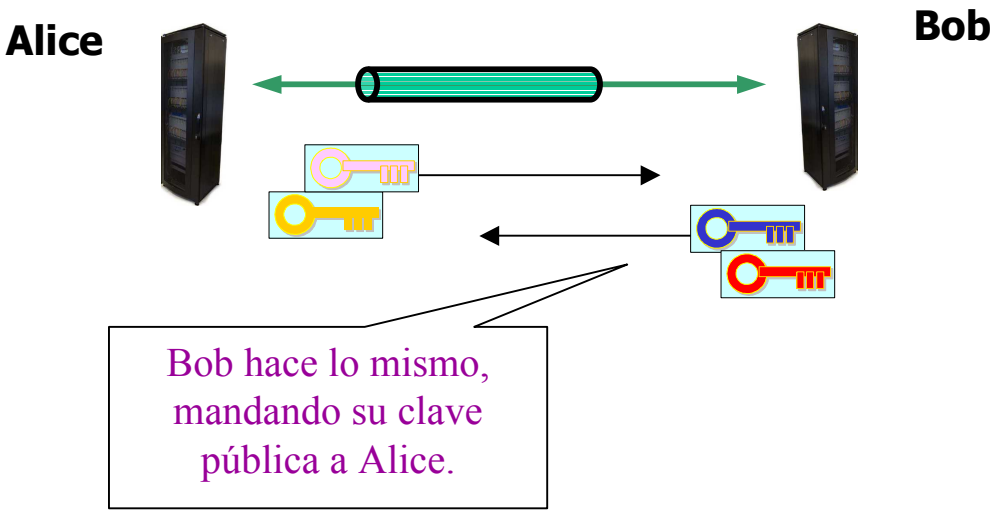
FiberNet

Diffie-Hellman



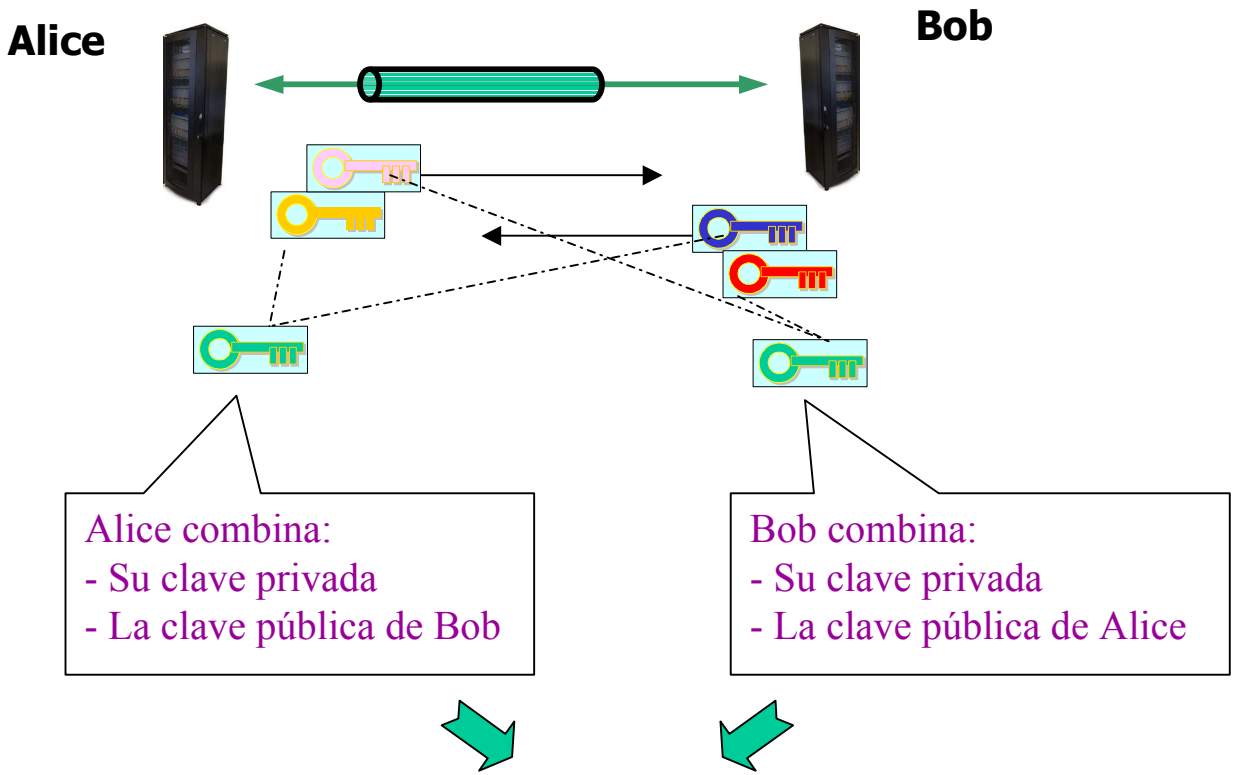
FiberNet

Diffie-Hellman



FiberNet

Diffie-Hellman

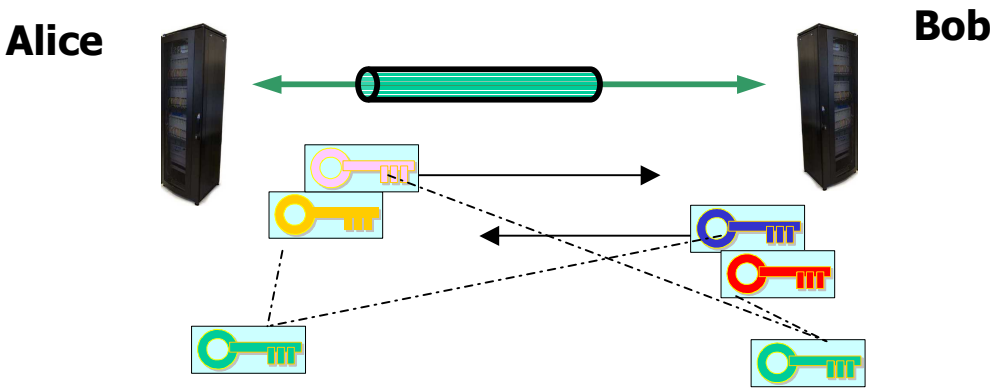


Ambas operaciones dan el mismo resultado: la clave de sesión

La aplicaremos en el AES de ambos extremos

FiberNet

Diffie-Hellman



✓ Herramienta matemática utilizada: DLC (Discrete Logarithm Cryptography)

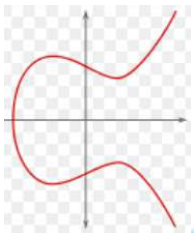
- FFC (*Finite Field Cryptography*)

  Privada = n. aleatorio = a, pública = (g^a) ; $(g^b)^a = (g^a)^b$

  (Fórmulas simplificadas)

- ECC (*Elliptic Curve Cryptography*)

  Privada = n. aleatorio = a, pública = $(a \cdot G)$; $a \cdot (b \cdot G) = b \cdot (a \cdot G)$



Autenticación

¿Alice negocia Diffie-Hellman con Bob o con la malvada Eve?

La **autenticación** permite a cada tarjeta comprobar que los mensajes recibidos provienen del interlocutor esperado, mediante la **firma** de estos mensajes.

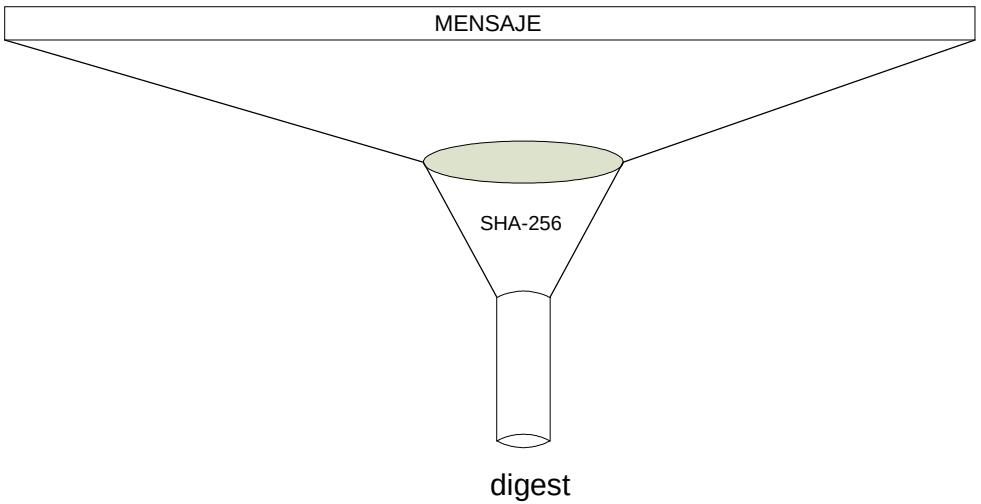
En un enlace de fibra entre dos tarjetas:

- ✓ Validamos a las tarjetas interlocutoras desde el mismo comienzo de la comunicación.
- ✓ Garantizamos la seguridad del "intercambio de claves".

FiberNet

Funciones de hash

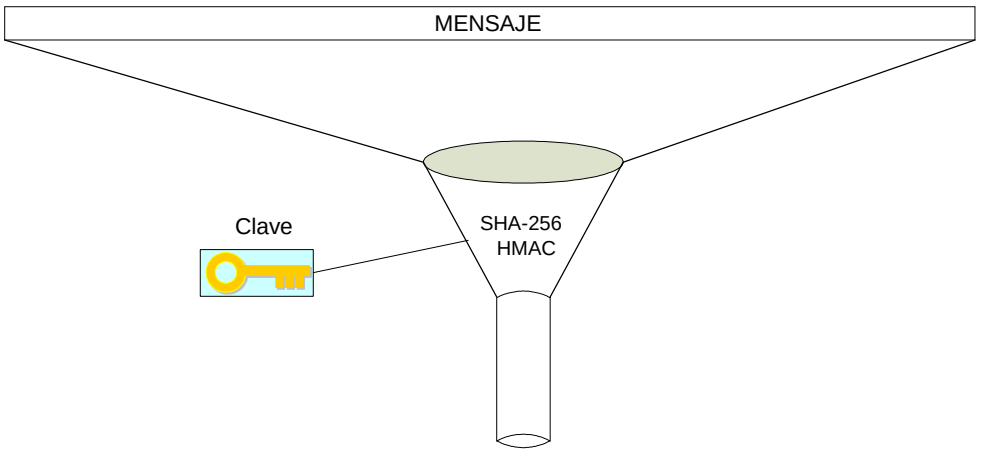
- ✓ Condensan un conjunto de datos de longitud arbitraria en otro conjunto de datos de longitud fija y normalmente mucho menor ("**digest**" o "huella digital").
- ✓ Es muy difícil (no es viable) modificar los datos sin modificar el resultado, por lo cual la disponibilidad de un "digest" fiable garantiza la **integridad** de los datos.
- ✓ Ejemplos de algoritmos bien conocidos: MD5, SHA-1, SHA-256



FiberNet

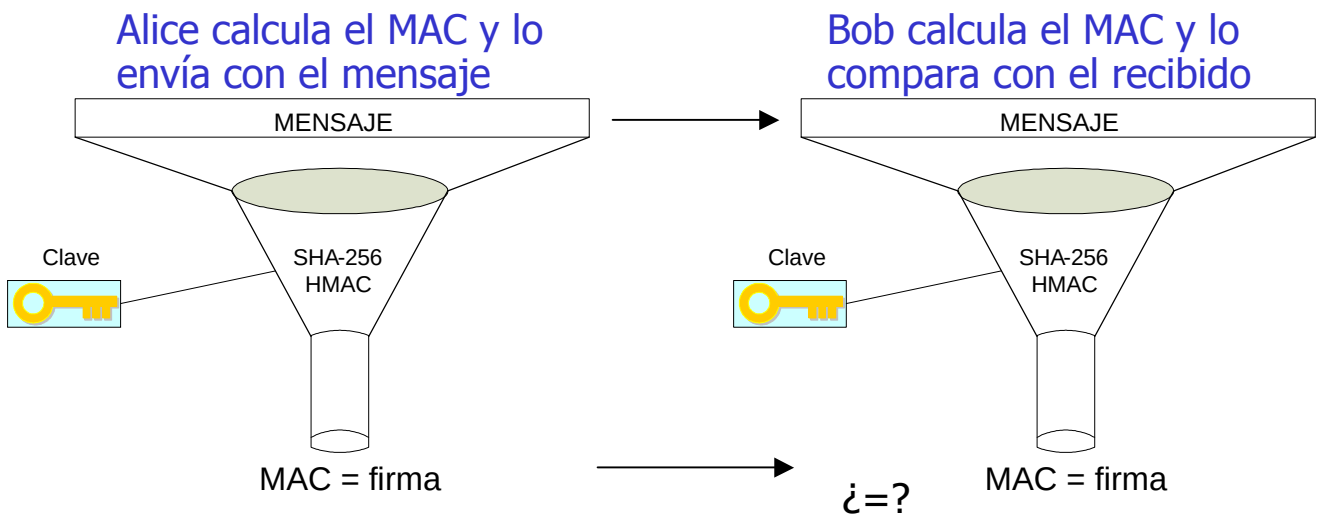
Message Authentication Code (MAC)

- ✓ Se genera añadiendo el uso de una **clave** a la función de hash.
- ✓ Sólo se puede generar un MAC correcto si se conoce la clave, y el más mínimo cambio en el mensaje provoca un cambio sustancial en el MAC
- ✓ Algoritmo más utilizado: HMAC.



MAC = **firma**

- ✓ Podemos utilizar el MAC para autenticar a los interlocutores (p.ej. firmando los mensajes Diffie-Hellman).



- ✓ El mensaje puede además incorporar números de secuencia, aleatorios, etc.

Para los MAC Fibernet ha escogido algoritmos de última generación y alta seguridad:

- ✓ **HMAC** (Hash-based Message Authentication Code, FIPS-198), corriendo sobre
- ✓ **SHA-256** (Secure Hash Algorithm con salida de 256 bits, FIPS-180-3)

FiberNet

Contraseñas de usuario

- ✓ La autenticación mutua de las dos tarjetas que forman un enlace de fibra (una tarjeta en cada extremo del enlace) se basa en la utilización de una **contraseña de usuario**, que es la misma para las dos tarjetas.
- ✓ Una persona configura esta contraseña mediante una interfaz gráfica de usuario.

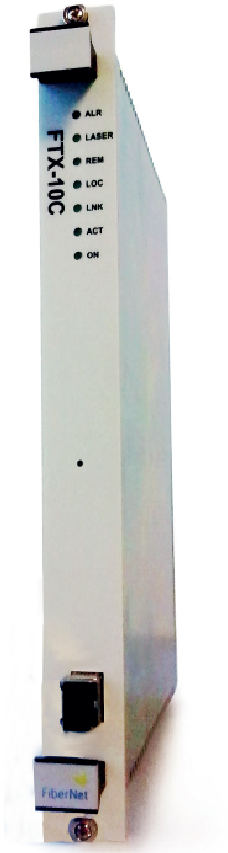
- ✓ Independientemente de las recomendaciones que se hagan, no se puede confiar en la robustez de una "clave humana" frente a posibles ataques de diccionario.
  - ***Stretching*** : larga computación intermedia antes de convertirse en una clave que realmente utilice el sistema
  - ***Salting***: utilización de números aleatorios en el proceso

Soluciones de cifrado de Fibernet

Concepto general

Disponibilidad de una gama de tarjetas cifradoras, insertables en bastidores DUSAC 4800 y DUSAC 350, soportando diversos protocolos.

FTX-10C



- ✓ **Ethernet 10 Gbps (10GBASE-R)**
- ✓ Interfaz local mediante SFP+

- ✓ Interfaz de línea en conectores ópticos BSC II

- ✓ Sintonizable en banda C o L (la tarjeta cubre una banda entera) para su uso en DWDM

FTX-1C

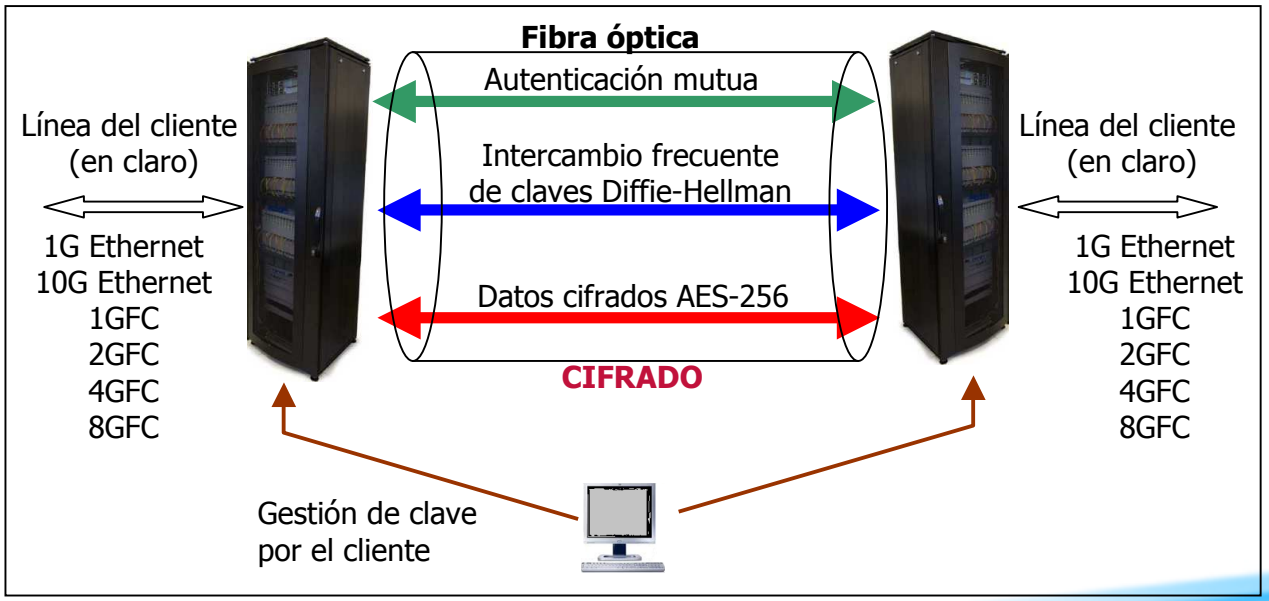
- ✓ **Ethernet 1 Gbps (1000BASE-X)**
- ✓ Interfaz local mediante SFP
- ✓ Interfaz de línea mediante SFP
- ✓ Posibilidad de conexión de línea en frontal o en trasera (conectores ópticos BSC II)

MUX-8

- ✓ **Multi-protocolo:**
  - **Ethernet 1G**
  - **Fibre Channel 1G / 2G / 4G / 8G**
- ✓ Agregación de canales
  - Ej.: 2x4GFC, 2x1GE + 3x2GFC, etc.
- ✓ El cifrado es una opción (licencia)
- ✓ Interfaces locales mediante SFP/SFP+
- ✓ Interfaz de línea a través de XFP
- ✓ Posibilidad de conexión de línea en frontal o en trasera (conectores ópticos BSC II)

Resumen de características básicas

- ✓ Transparencia y mínima latencia
- ✓ Protocolos Ethernet a 1 y 10 Gbps y Fibre Channel a 1, 2, 4 y 8 Gbps
- ✓ Cifrado AES-256
- ✓ Cambio automático de claves frecuente y sin interrupciones en la comunicación
- ✓ Autenticación segura extremo a extremo
- ✓ Gestión del cliente mediante su propia clave



Gracias por su atención.

FiberNet