Módulo II
Tecnología Criptográfica

Programa

1. *Criptología*
2. *Criptografia simétrica*
3. *Hash y compendio de mensajes*
4. *Criptografía de clave pública*
5. *Firmas digitales*
6. *Administración y distribución de clave simétrica*
7. *Sistema de autenticación Kerberos*
8. *Certificados digitales*
9. *Infraestructura de clave pública*
10. *Estándares de PKI*
11. *Implementación de PKI*

Criptografía

***Kriptos* – Oculto**

***Graphos* – Escritura**

La *criptografía* es la ciencia de codificar y decodificar la información para lograr:

- **Privacidad**
- **Integridad**
- **Autenticación**
- **No repudio**

Objetivos de la Criptografía

- ***Privacidad***

  Mantener la información inaccesible a terceros.

- ***Integridad***

  Evitar que la información sea alterada por terceros.

- ***Autenticación***

  Garantizar que el origen o autor de los datos es auténtico.

- ***No repudio***

  Evitar que se niegue haber emitido un mensaje.

Aplicaciones de la Criptografía

- **Comercio electrónico**
- **Financieras y bancarias**
- **Militares y de seguridad nacional**
- **Correo electrónico seguro**
- **Redes privadas virtuales (VPN)**
- **Preservación de derechos de autor (*watermarking*)**

Antecedentes Históricos

- ***Cifrado de César (Siglo I a.C.)***
  - *Ejemplo:*

    Mensaje: *V I N I V I D I V I NC I*

    Criptograma: *BMQM BMGM BMQFM*
- ***Cifrado de Vigenere (1586)***
  - *Ejemplo:*

    Mensaje: *PARIS VAUT BIEN UNE MESSE*

    Clave: *LOUPL OUPL OUPL OUP LOUPL*

    Criptograma: *AOLXD JUJE PCTY IHT XSMHP*

Antecedentes Históricos

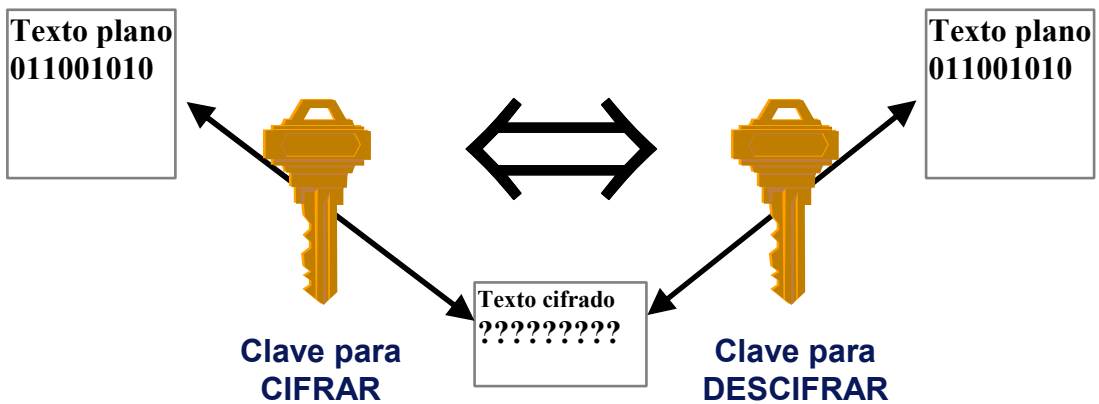
- ***Cifrado de Vernam (1917)***
  - ***Extensión del método de Vigenere.***
  - ***La longitud de la clave es igual a la del mensaje.***
  - ***La clave se utiliza solamente una vez. (One time pad)***
  - ***Utilizado durante la segunda guerra mundial por espías de diferentes nacionalidades.***
  - ***Shannon demostró en 1949 que es completamente seguro.***

Antecedentes Históricos

- **Segunda Guerra Mundial**
  - **Máquinas de rotores (Enigma, Purple, etc.)**
  - **Criptoanálisis**
  - **Primeras máquinas de criptoanálisis (Colossus)**
- **Guerra fría**
  - **Proyectos ARPA**
  - **ARPANET**
  - **Proyecto ECHELON**

Criptografía Simétrica

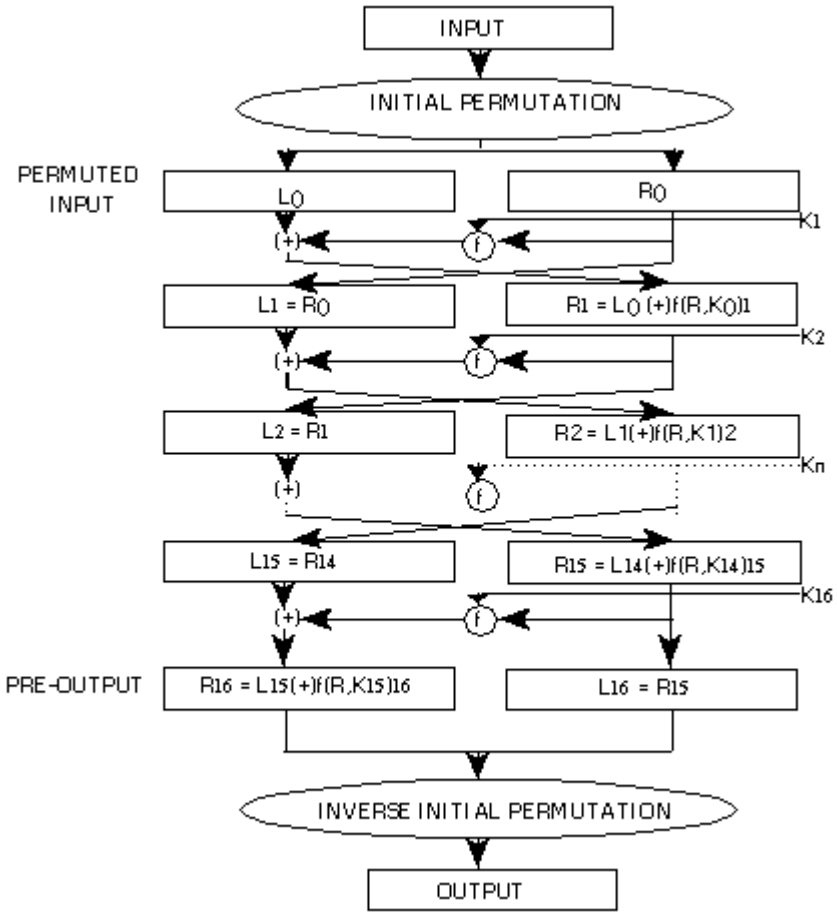
- *Cifrado Simétrico*
  - Se usa una misma clave para cifrar y descifrar
  - ¿Cómo hacer llegar la clave al destinatario a través de un canal seguro?
  - Las contrapartes deben acordar no divulgar la clave común
  - AES, IDEA, RC6, FEAL



Algoritmos Simétricos

- ***DES (Data Encryption Standard)***
  - **Cifrado en bloques de 64 bits, claves de 56 bits.**
  - **Diseñado en 1975 por IBM y adoptado como estándar por el gobierno americano en 1976.**
  - **En 1987 la NSA se opone a que se siga manteniendo como estándar pero, por motivos económicos, finalmente se renueva.**
  - **En 1997, tras 4 meses de cálculo se descifra un mensaje cifrado con el DES. Hoy el record es de 23 horas.**
  - **Sustituido a partir del 2000 por el AES.**
  - **Especificación: http://www.itl.nist.gov/fipspubs/fip46-2.htm**

DES


INPUT
INITIAL PERMUTATION
PERMUTED INPUT
L0
R0
K1
(+)
f
L1 = R0
R1 = L0 (+)f(R,K0)1
K2
L2 = R1
R2 = L1(+)f(R,K1)2
Kn
L15 = R14
R15 = L14(+)f(R,K14)15
K16
PRE-OUTPUT
R16 = L15(+)f(R,K15)16
L16 = R15
INVERSE INITIAL PERMUTATION
OUTPUT

DES

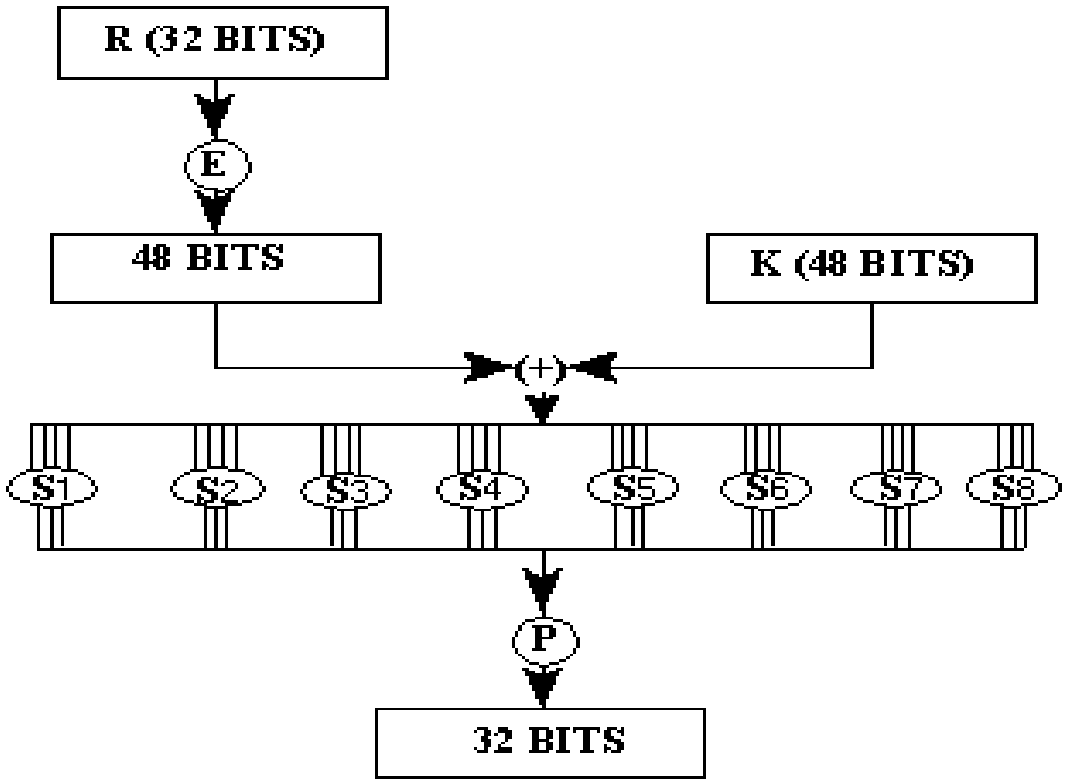
IP

58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

IP-1

40 8 48 16 56 24 64 32
39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30
37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28
35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26
33 1 41 9 49 17 57 25

Función de cifrado *DES*



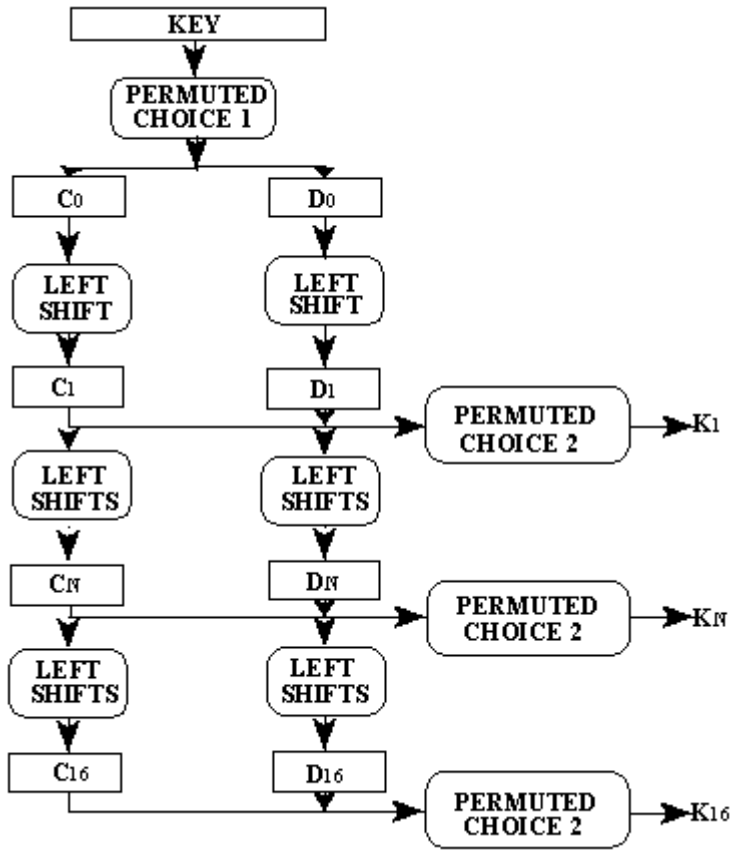
S-boxes

S_1

Número de Columna

Fila No.	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Cálculo de subclaves *DES*



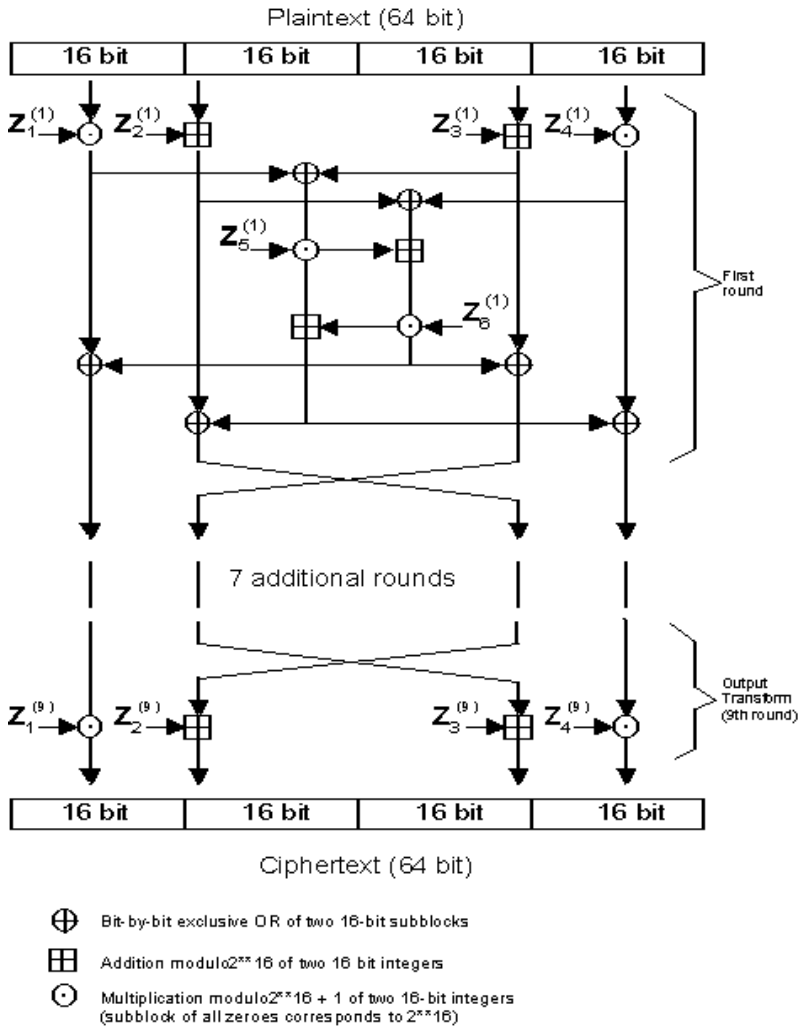
Seguridad del DES

- ***Actualmente se considera el tamaño de clave muy pequeño.***
- ***No se conoce ninguna técnica de criptoanálisis más eficiente que la fuerza bruta.***
- ***Se puede aumentar la seguridad mediante aplicaciones sucesivas del DES con diferentes claves.***
- ***3DES:*** $E_{k1}D_{k2}E_{k1}$

Algoritmos Simétricos

- ***IDEA (International Data Encryption Algorithm)***
  - ***Desarrollado en el ETH de Zurich, Suiza.***
  - ***Propuesto como estándar europeo en 1990.***
  - ***Cifrado en bloques de 64 bits.***
  - ***Utiliza claves de 128 bits.***
  - ***El único ataque posible es por fuerza bruta, pero es impracticable.***
  - ***Implementado en PGP***

IDEA


Plaintext (64 bit)
16 bit
16 bit
16 bit
16 bit
$Z_1^{(1)}$
$Z_2^{(1)}$
$Z_3^{(1)}$
$Z_4^{(1)}$
$Z_5^{(1)}$
$Z_6^{(1)}$
First round
7 additional rounds
$Z_1^{(9)}$
$Z_2^{(9)}$
$Z_3^{(9)}$
$Z_4^{(9)}$
Output Transform (9th round)
16 bit
16 bit
16 bit
16 bit
Ciphertext (64 bit)
Bit-by-bit exclusive OR of two 16-bit subblocks
Addition modulo2** 16 of two 16 bit integers
Multiplication modulo2**16 + 1 of two 16-bit integers (subblock of all zeroes corresponds to 2**16)

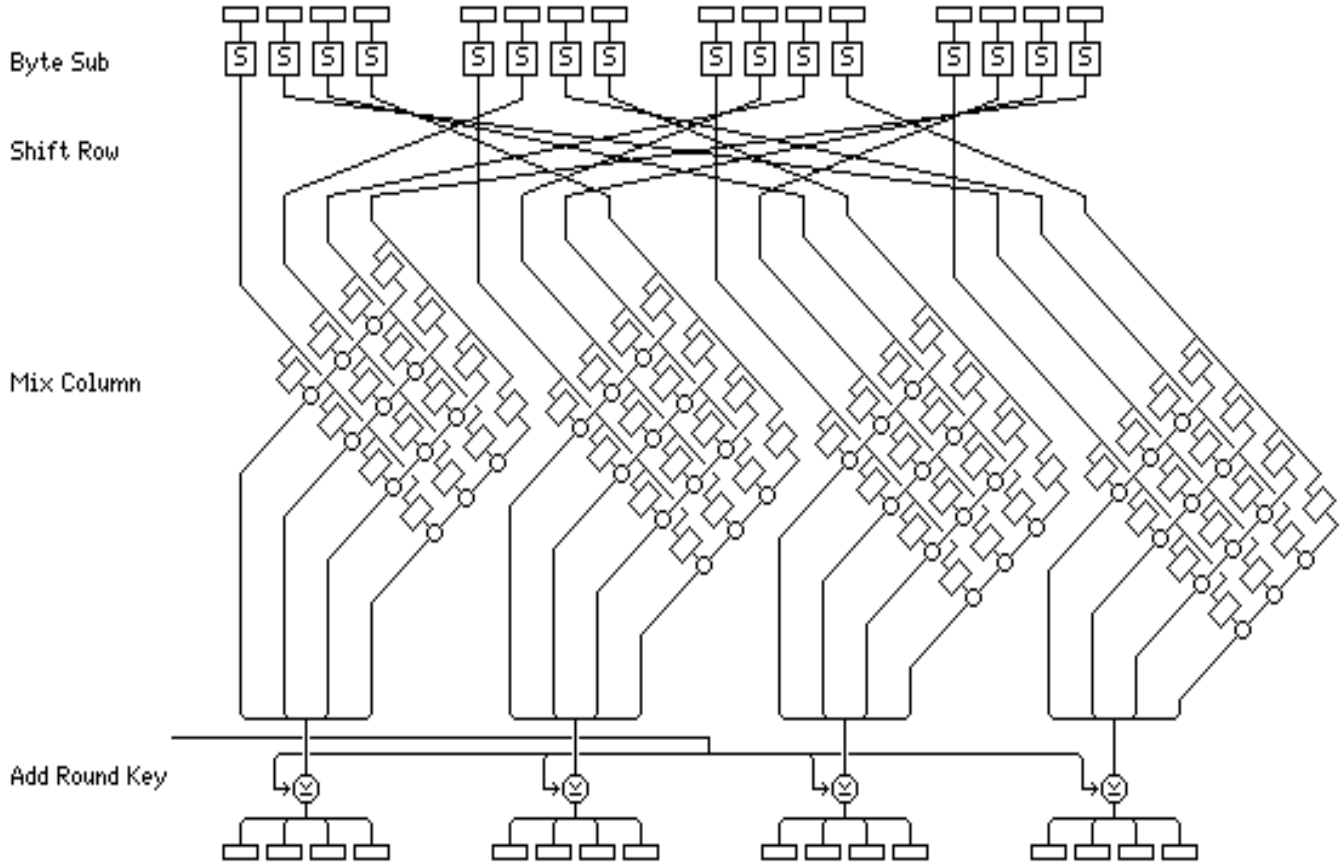
Algoritmos Simétricos

- ***AES (Advanced Encryption Standard)***
  - **Algoritmo simétrico adoptado como nuevo estándar del gobierno americano.**
  - **Originalmente llamado *Rinjdael*.**
  - **Cifrado en bloques de 128, 192 o 256 bits.**
  - **Utiliza claves de 128, 192 o 256 bits.**
  - **Especificaciónhttp://csrc.nist.gov/publications/fips/fips197/fips-197.pdf**

AES

- Número variable de rondas
  - 9 para claves/bloques de 128 bits
  - 11 para claves/bloques de 192 bits
  - 13 para claves/bloques de 256 bits
- Operación inicial: *ARK* (*AddRoundKey*)
- Ronda:
  1) *Byte Sub*
  2) *Shift Row*
  3) *Mix Column*
  4) Add Round Key

AES



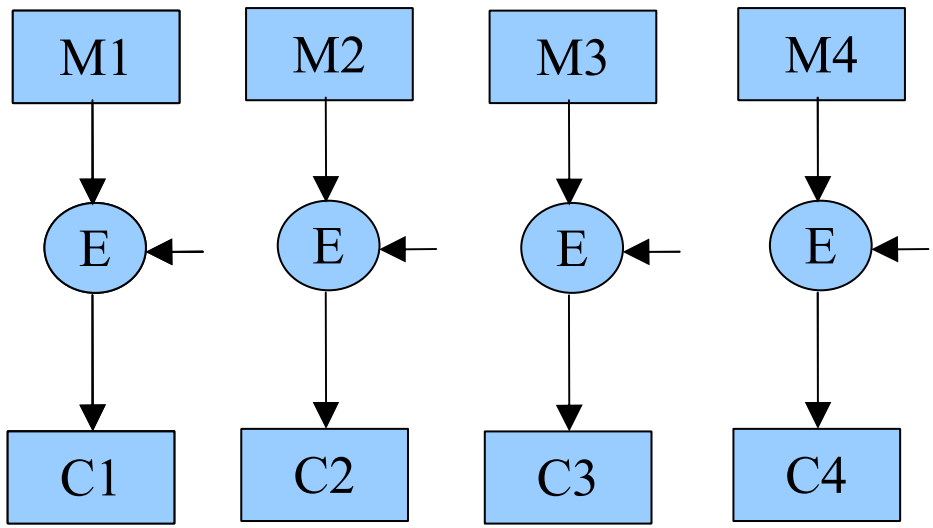
Modos de operación

- **Los algoritmos de cifrado en bloques pueden operarse en los modos:**

  1) ***Electronic Code Book*** **(ECB)**
  2) ***Cipher Block Chaining*** **(CBC)**
  3) ***Cipher Feedback Mode*** **(CFB)**
  4) ***Output Feedback Mode*** **(OFB)**
  5) ***Counter Mode*** **(CTR)**

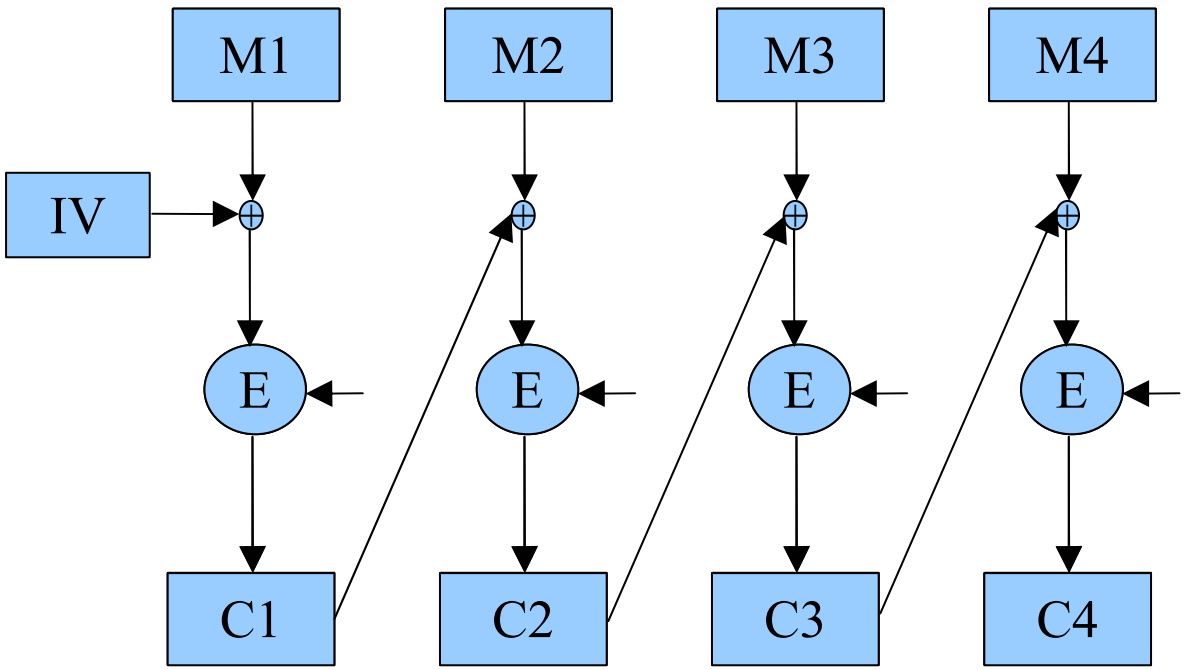
ECB

- **El cifrado en modo ECB se ilustra en el siguiente diagrama:**



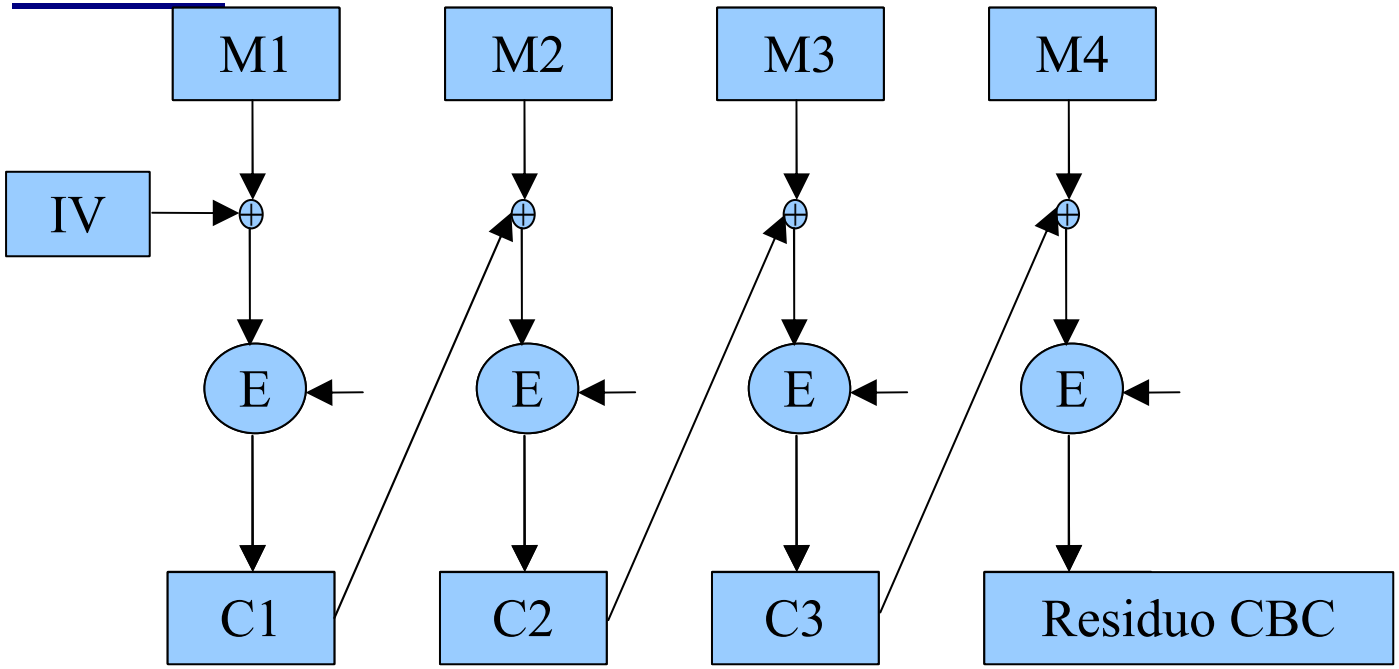
CBC

- **El cifrado en modo CBC se ilustra en el siguiente diagrama:**



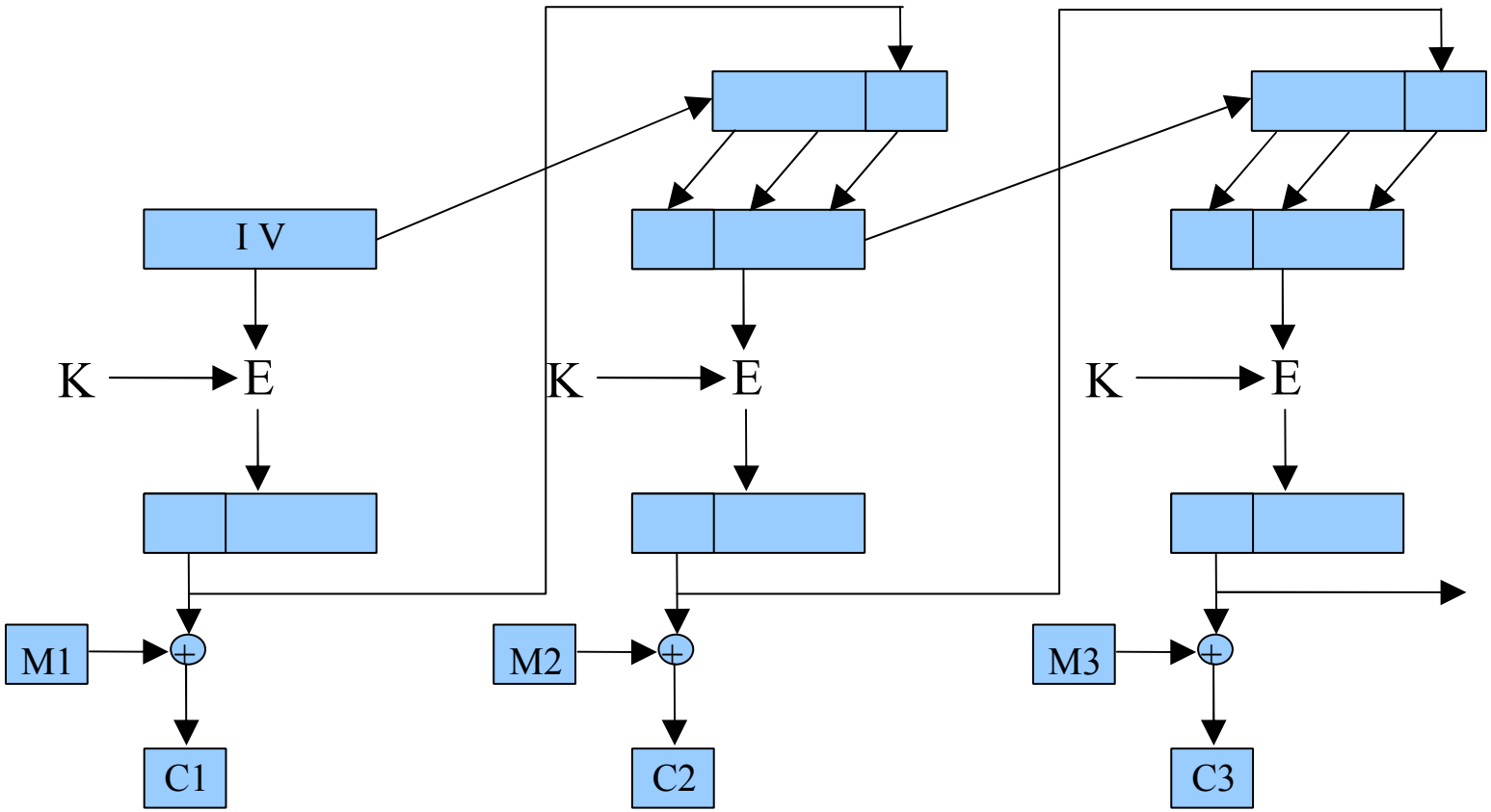
Generación de MAC

- **El cifrado en modo CBC puede utilizarse para generar un *MAC* (*Message Authentication Code*) mediante un residuo:**



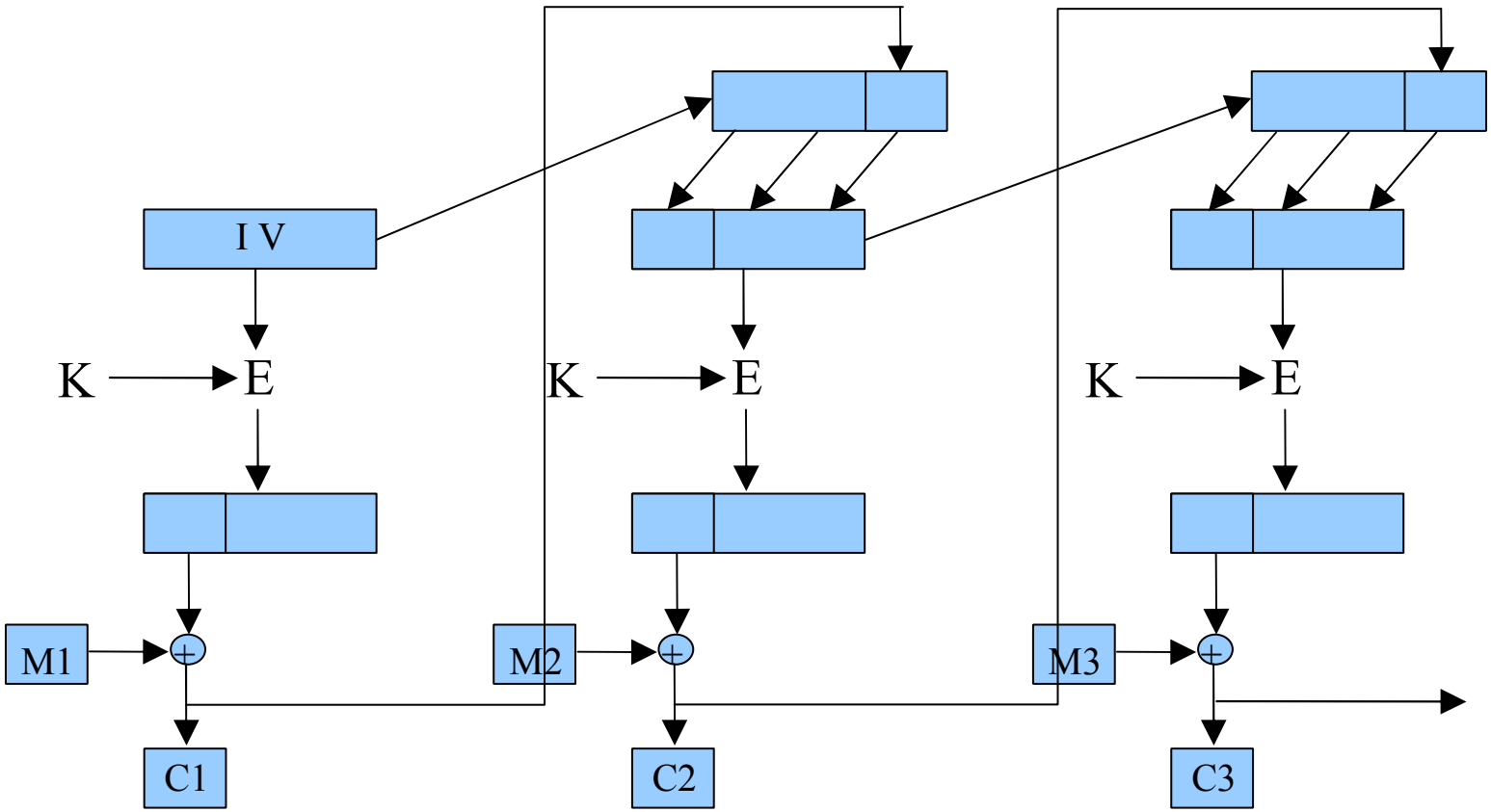
OFB

- **OFB (*Output Feedback Mode*) de *k* bits :**

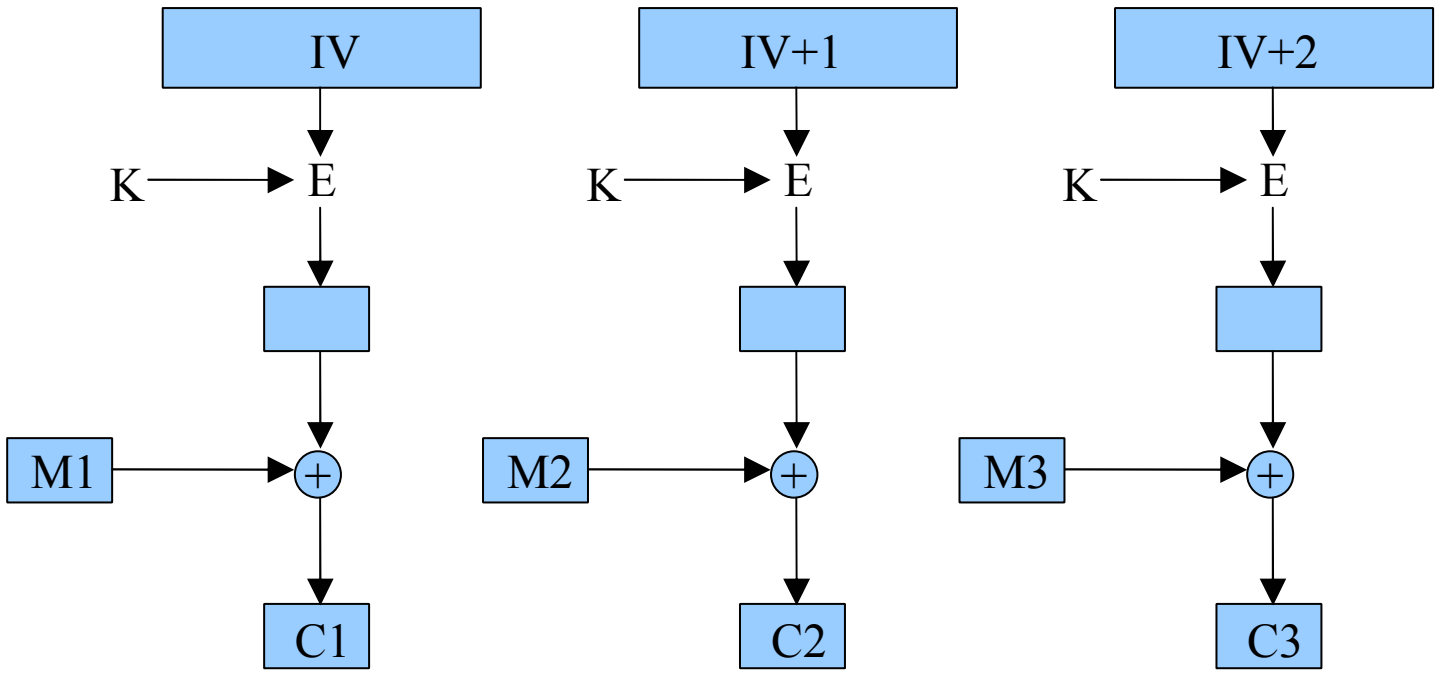


CFB

- **CFB (*Cipher Feedback Mode*) de *k* bits :**



- **CTR (*Counter Mode*) :**



Hash y compendio de mensajes

SEKUREIT
CONSULTORES EN SEGURIDAD INFORMATICA

- ***Hash: Función de una sola vía.***
- ***MD (Message Digest): Función de hash que toma como entrada un texto de una longitud arbitraria y como salida se tiene un bloque de tamaño fijo.***
- ***Propiedades de un hash/md seguro:***
  - ***Para un número grande de entradas seleccionadas aleatoriamente, cualquier bit de las correspondientes salidas deben estar en 1 en la mitad de las ocasiones.***
  - ***Cada salida debe tener, con alta probabilidad, la mitad de los bits en 1.***
  - ***Cualquier par de salidas no deben estar correlaciondas, no importa que tan semejantes sean las entradas.***

Hash y compendio de mensajes

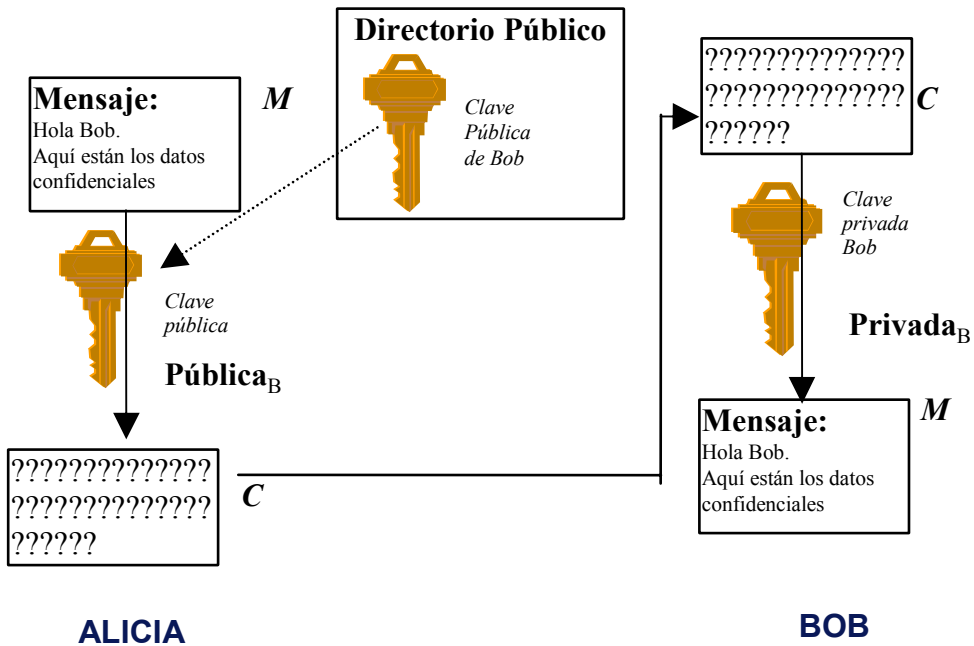
- ***Se utilizan para calcular un fingerprint de un archivo o un mensaje.***
- ***Permiten determinar integridad***
- ***Algunas funciones de hash criptográficamente fuertes:***
  - ***MD2***
  - ***MD4***
  - ***MD5***
  - ***SHA-1***

MD2

- ***MD2 toma un numero arbitrario de bytes y produce un bloque de 128 bits.***
- ***La idea básica de MD2 es la siguiente:***
  - ***Se añade un relleno al mensaje de entrada para hacerlo múltiplo de 16 bytes.***
  - ***Se añade un checksum de 16 bytes al final.***
  - ***Se procesa el mensaje, 16 bytes a la vez, mediante una función de substitución (basada en los dígitos de pi) que depende del bloque actual y la salida previa.***

Criptografía de Clave Pública

- ***Cifrado Asimétrico***
  - **También conocido como de Clave Pública**
  - **Se tiene una clave pública, no secreta para cifrar los datos. El destinatario tiene una clave privada, secreta, para descifrar**
  - **ECC, RSA, ElGamal, DSA**



Algoritmos de Clave Pública

- ***RSA***
  - **Inventado por Rivest, Shamir y Adleman en 1977.**
  - **Basado en el problema de la factorización de números primos.**
  - **Se recomiendan longitudes de clave mayores a 1024 bits.**
  - **Es el algoritmo de clave pública más ampliamente utilizado.**

Algoritmo RSA

Generación de claves:

- Se seleccionan dos primos *p* y *q*.
- Se hace *n=pq* y *z=(p-1)(q-1).*
- Seleccionar un *d* tal que *mcd(z,d)=1*.
- Encontrar un *e* tal que *ed=1(mod z).*
- Clave pública: *(n,e)*
- Clave privada: *d*

Algoritmo RSA

- Cifrado del mensaje M

$$C=E(M)=M^e \pmod{n}$$

- Descifrado del mensaje C

$$M=D(C)=C^d \pmod{n}$$

Recomendaciones en RSA

- El tamaño de *p* y *q debe ser de unos 512 bits y el de n no debe ser menor a 1024, recomendándose módulos de mayor tamaño*.
- *El entero p-q* no debe ser pequeño.
- Los primos *p* y *q deben ser criptográficamente fuertes.*
  - *Tanto p-1 como p+1 deben tener factores grandes.*

Factorización de RSA

- **El 22 de agosto de 1999 se anunció la factorización del RSA de 512 bits. Se realizó sobre 300 SGI workstations y Pentium PC, principalmente en la noche y en fines de semana, durante siete meses.**
- **El esfuerzo requerido fue 50 veces menor al utilizado para romper el DES.**
- **Actualmente se ofrecen $10,000.00 USD a quien factorice el RSA de 576 bits.**
- **http://www.rsasecurity.com/rsalabs/challenges/**

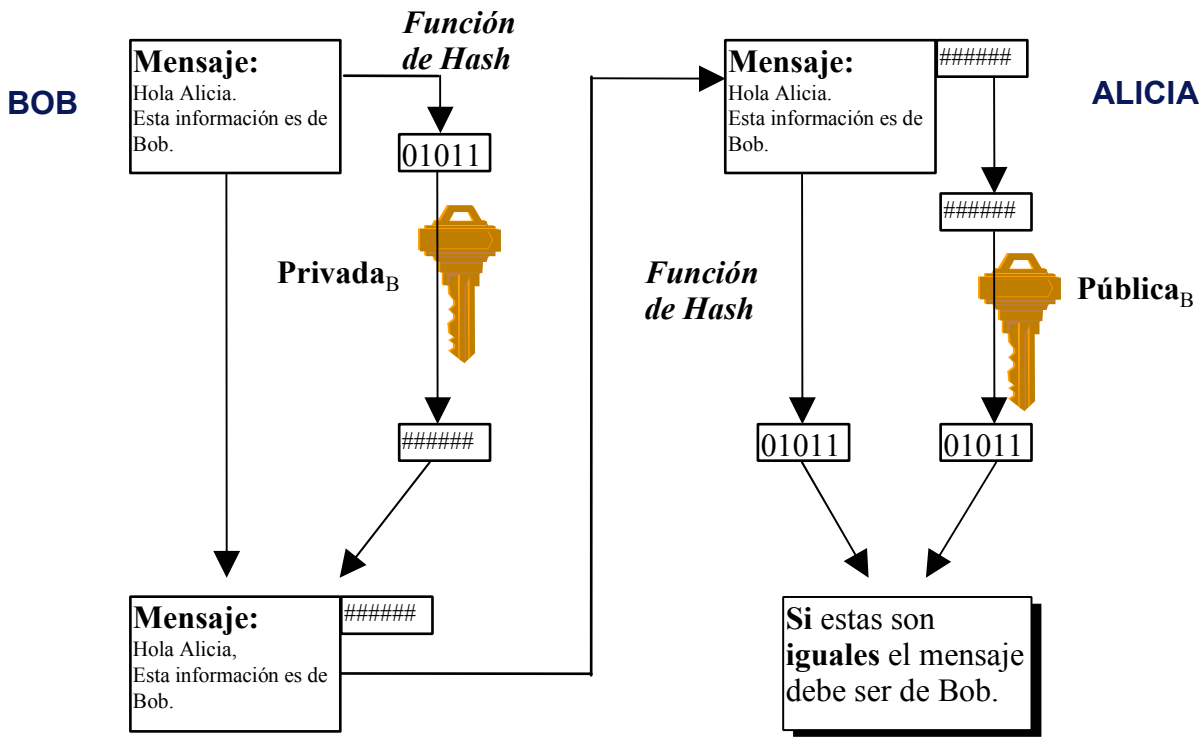
Algoritmos de Clave Pública

- ***ElGamal***
  - **Inventado por ElGamal en 1984.**
  - **Basado en el problema del logaritmo discreto.**
  - **Se recomienda longitud de claves de 1024 bits.**

- ***ECC (Elliptic Curve Cryptography)***
  - **Inventado de manera independiente por Neal Koblitz yVictor Miller en 1985.**
  - **Basado en el problema de logaritmo discreto sobre curvas elípticas.**
  - **Requiere de longitudes de claves menores.**
  - **Se sugieren longitudes de claves de al menos 163 bits.**
  - **Ideal para comunicación inalámbrica y aplicaciones de cómputo movil.**

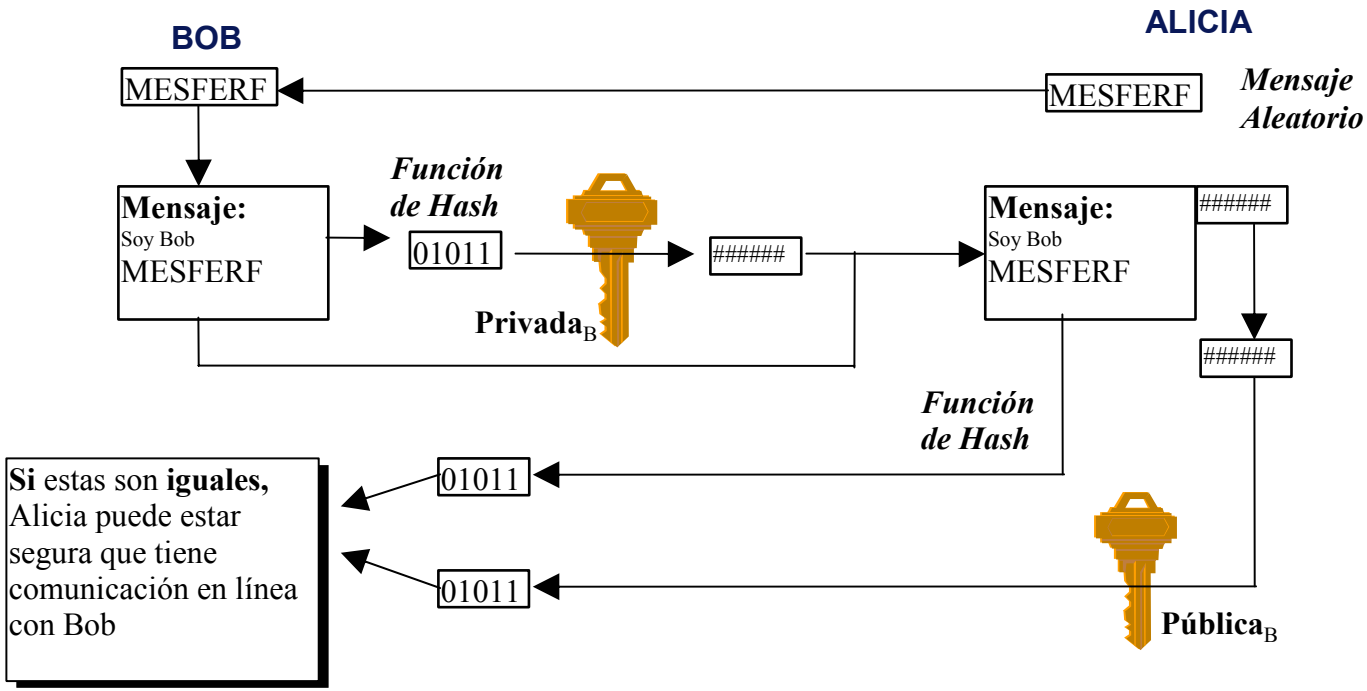
Firmas Digitales

- **Firmas Digitales**
  - **Uso de cifrado de clave pública**
  - **Proporcionan autenticación del origen de los datos, integridad de datos y no repudio**



Autenticación de Usuarios

- **Uso de Protocolos Criptográficos de Retos Firmados**
  - **En una comunicación en tiempo real, asegurarse que la contraparte efectivamente es quien dice ser.**



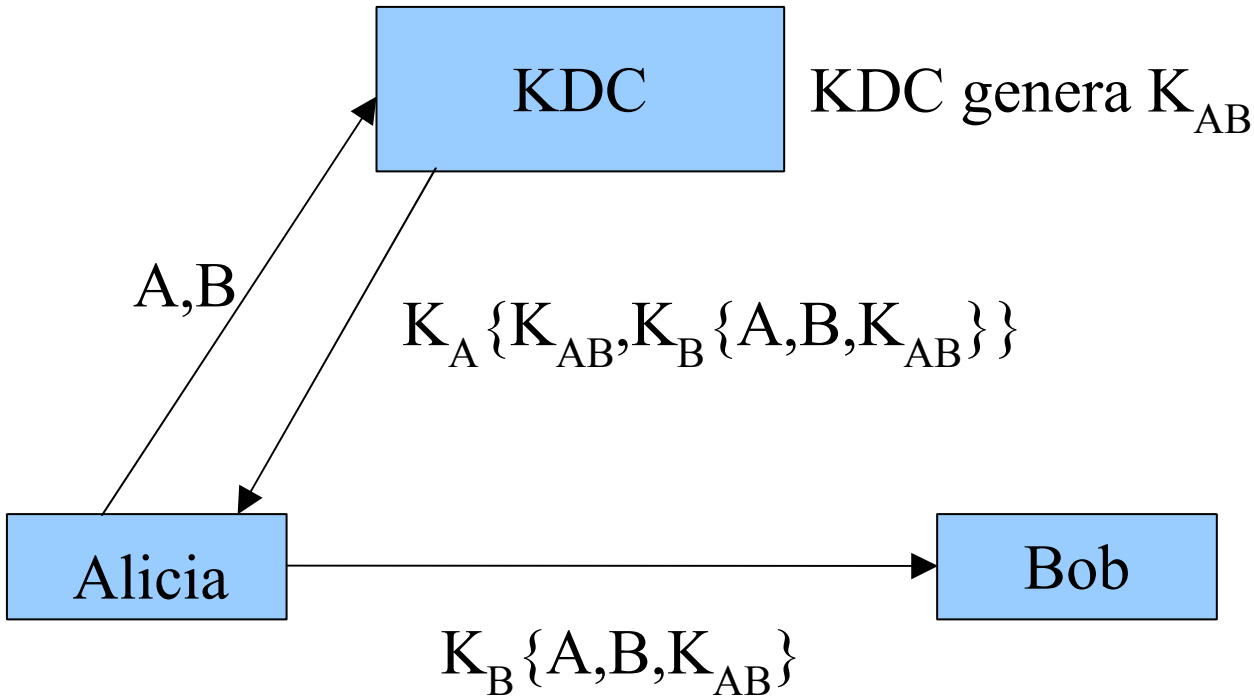
PGP (Pretty Good Privacy)

- **Sistema de cifrado para correo electrónico.**
- **Utiliza criptografía de clave simétrica, criptografía de clave pública, funciones de hash y firmas digitales.**
- **Proporciona privacidad, autenticación del emisor, integridad.**
- **Hay varias implementaciones, algunas gratuitas y otras comerciales.**

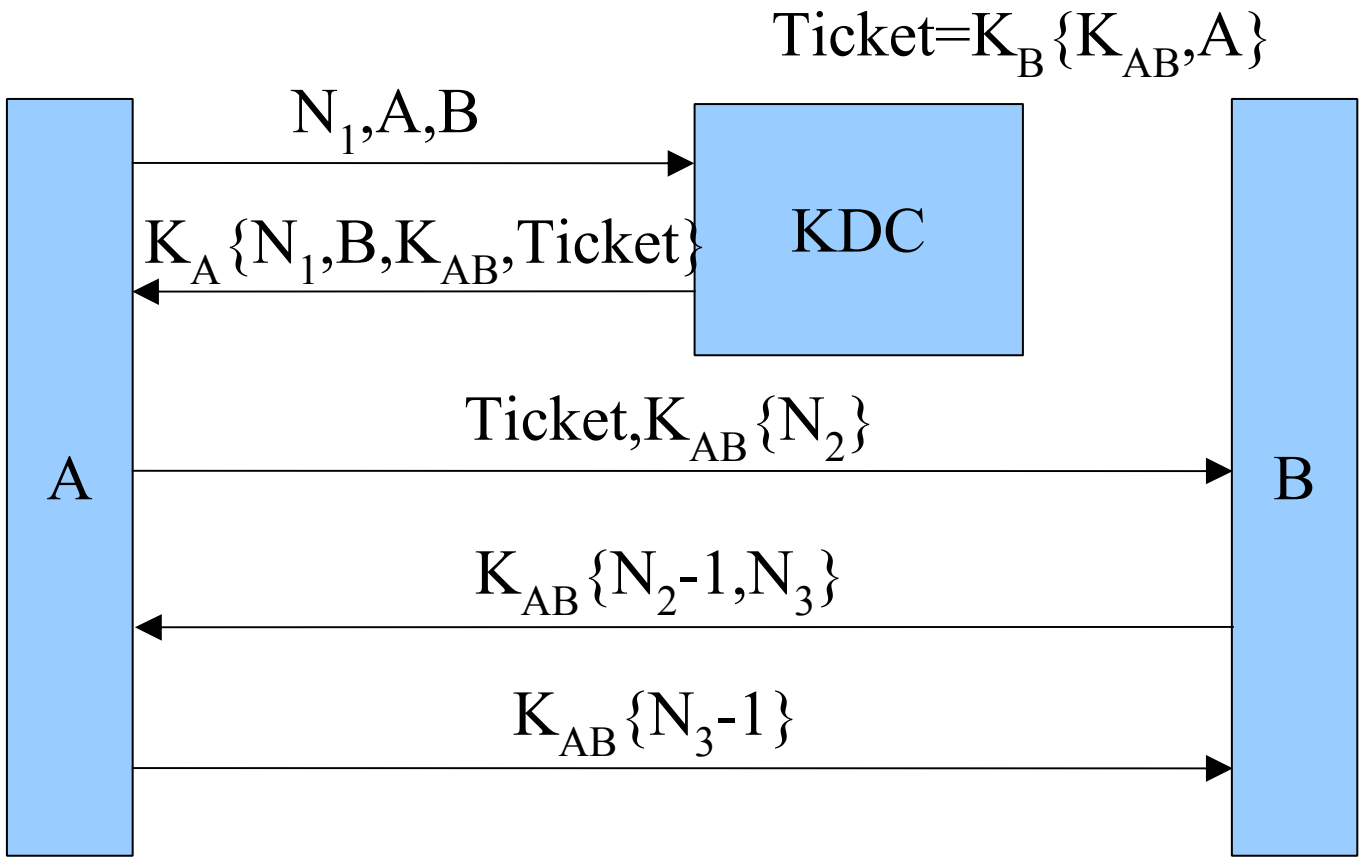
PGP (Pretty Good Privacy)

- **Algoritmos simétricos:**
  - **CAST, 3DES, IDEA, Twofish, AES**
- **Algoritmos de hash**
  - **SHA1**
  - **MD5 (versiones anteriores)**
- **Algoritmos de clave pública**
  - **RSA, DH**
- **Algoritmos de firma digital**
  - **DSA**

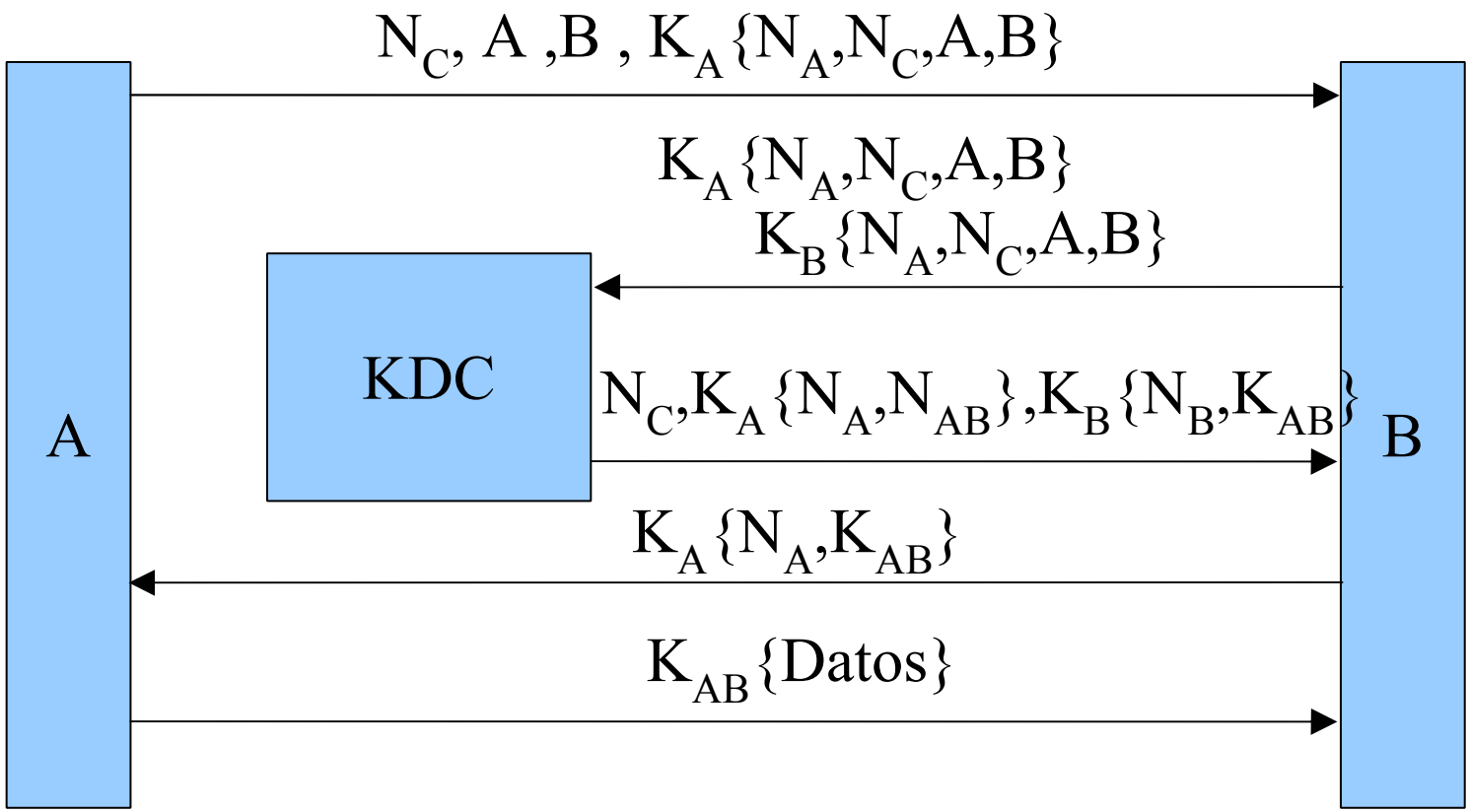
Autenticación mediante KDC



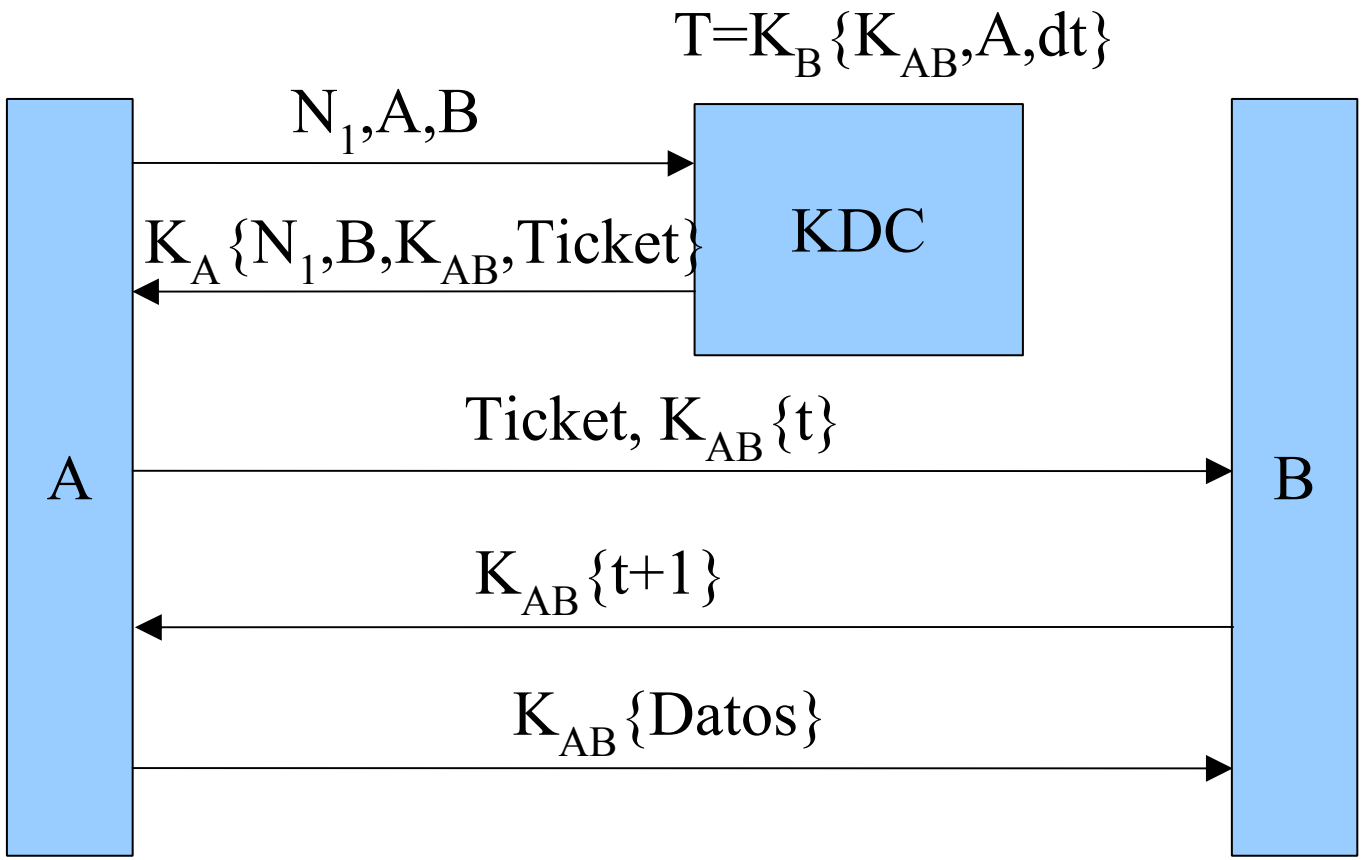
Protocolo de Needham-Schroeder



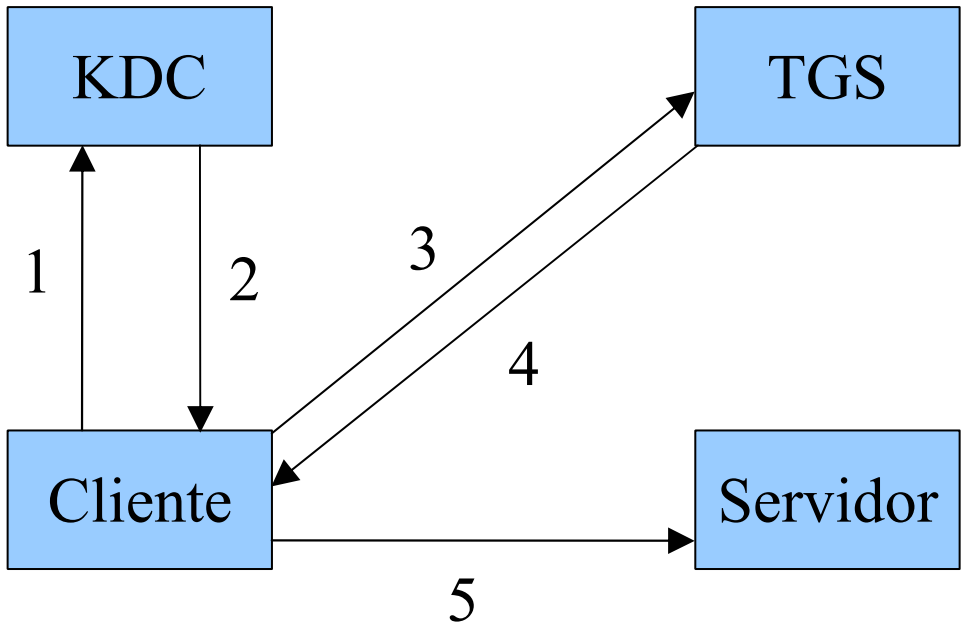
Protocolo de Otway-Rees



Protocolo Kerberos Simple



Protocolo Kerberos



1. Cliente, TGS, N

2. $K_C\{K_{C,TGS},N\}$, $T_{C,TGS}$

3. S, N, $K_{C,TGS}\{A_C\}$, $T_{C,TGS}$

4. $K_{C,TGS}\{K_{C,S},N\},T_{C,S}$

5. $K_{C,S}\{A_C\}$, $T_{C,S}$

Kerberos V4

- **En Kerberos V4:**
  - **2: $K_C\{K_{C,TGS}, N, T_{C,TGS}\}$**
  - **4: $K_{C,TGS}\{K_{C,S}, N, T_{C,S}\}$**
- **Limitaciones:**
  - **Dependencia del cifrado (DES)**
  - **Dependencia de IP**
  - **Ordenamiento de bytes del mensaje**
  - **Caducidad del boleto (21 h. 15 m.)**
  - **Nombres de principales: nombre, instancia, y dominio limitados a 39 caracteres.**
  - **Autenticación interdominios limitada.**

Cambios en Kerberos V5

- **Uso de cifrado modular**
- **Tipo de dirección variable**
- **Codificación de mensajes en ASN.1**
- **Formato de boletos extendido**
- **Nombres de principales son multicomponente**
- **Soporte de autenticación interdominios jerárquica.**
- **Boletos:**
  - **Renovables**
  - **Transferibles**
- **Datos de autorización (uso del boleto)**
- **Pre-autenticación (K_c cambiante)**

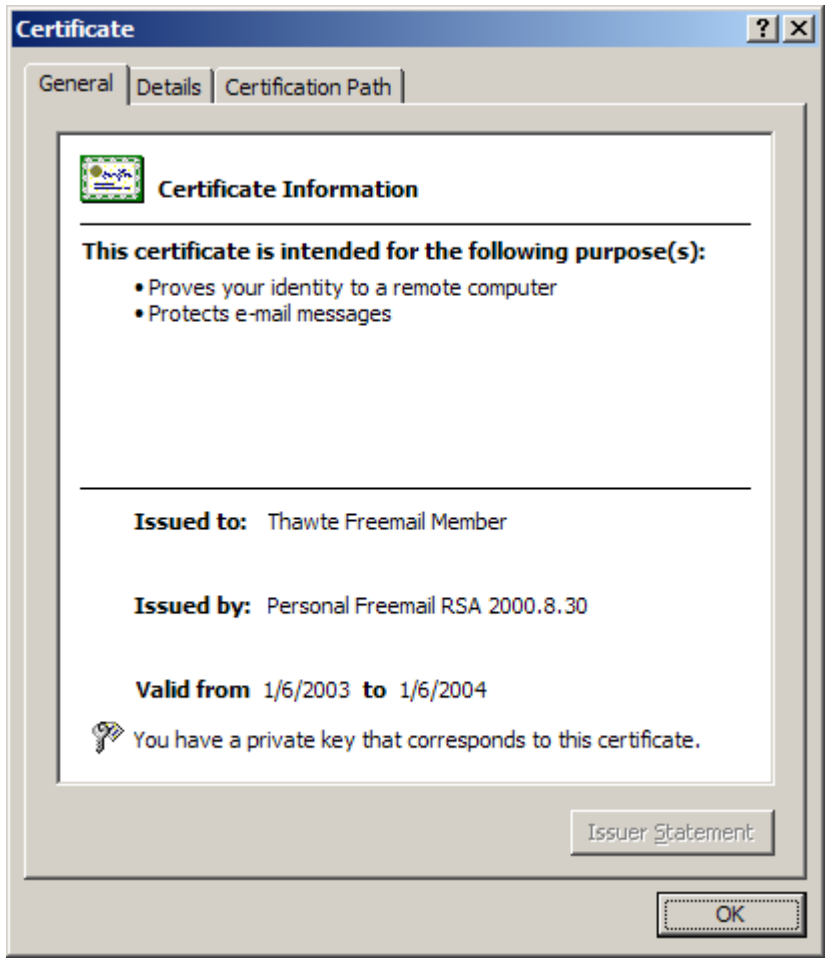
Implementaciones de Kerberos

- **UNIX:**
  - **Implementación del MIT**
    - **http://web.mit.edu/kerberos/www/**
    - **http://www.crypto-publish.org/**
  - **CyberSafe, Cygnus, OpenVision, etc.**
- **Windows 2000**
- **Cisco IOS**
- **Xylogic (Bay Networks)**
- **...**

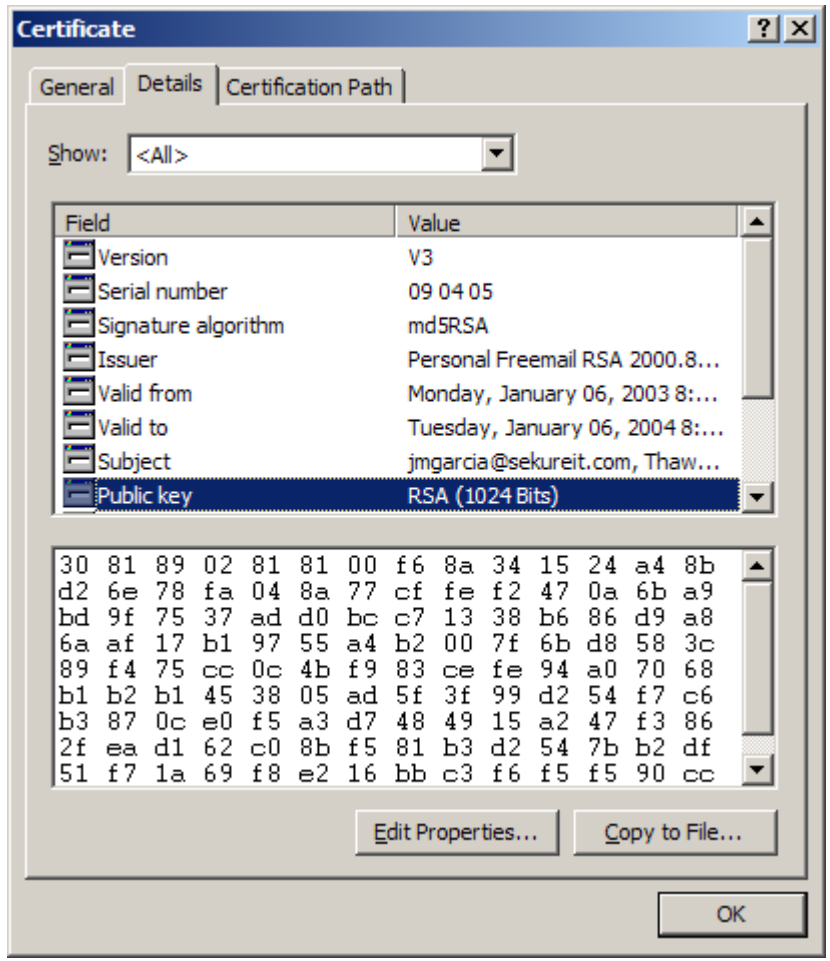
Certificados Digitales

- **Un certificado digital es un documento digital intransferible y no modificable firmado por una autoridad de certificación.**
- **Un certificado digital que siga el estándar X.509v3 contiene la siguiente información:**
  - **Identificación del titular del certificado**
  - **Clave pública del titular del certificado**
  - **Periodo de validez**
  - **Identificación del emisor del certificado**

Certificados Digitales



Certificados Digitales



Autoridad de Certificación (AC)

- Prevenir que algún usuario promueva una clave pública indicando que es de alguien más
- Un organismo en quien todos los usuarios confían
- Distribuir, Administrar y Revocar Certificados
  - Garantía a los usuarios de que las claves públicas son auténticas y pertenecen al usuario especificado

Certificados X.509

- Estándar ITU-T X.509 o ISO/IEC/ITU 9594-8.
- Versión 1 publicada en 1988 como parte del Directorio X.500
- Revisado en 1993, se añaden 2 campos y se publica como versión 2.
- De acuerdo a requerimientos del PEM, ISO/IEC/ITU y ANSI X9 desarrollaron la versión 3, en 1996.
- Algoritmos soportados:
  - Hash: MD2, MD5, SHA-1
  - Algoritmos de firma: RSA, DSA.
  - Claves públicas: RSA, DH

Certificados X.509v3

- **El certificado X.509v3 tiene como campos básicos los siguientes:**
  - Versión
  - Número de serie
  - Identificador de algoritmo de firma
  - Nombre del emisor
  - Validez
  - Sujeto
  - Información de la clave pública del sujeto
  - ID único del emisor
  - ID único del sujeto
  - Extensiones
  - Firma digital

Infraestructura de Clave Pública (PKI)

- **La infraestructura de clave pública (PKI) suministra los componentes y servicios que permitan:**
  - **Creación segura de claves**
  - **Validación de identidades**
  - **Expedición, renovación y revocación de certificados.**
  - **Distribución de certificados.**
  - **Almacenamiento seguro y recuperación de claves.**
  - **Establecimiento y administración de relaciones de confianza.**

Estándar PKIX

- **Es un estándar de PKI basado en certificados X.509.**
- **El grupo de trabajo PKIX ha producido varios estándares:**
  - **X.509v3 y CRLs para Internet (RFC 2459)**
  - **LDAP v2 para almacenamiento de certificados y CRLs (RFC 2587)**
  - **Certificate Management Protocol CMP (RFC 2510)**
  - **Online Certificate Status Protocol OCSP (RFC 2560)**
  - **Certificate Management Request Format (RFC 2511)**
  - **...**

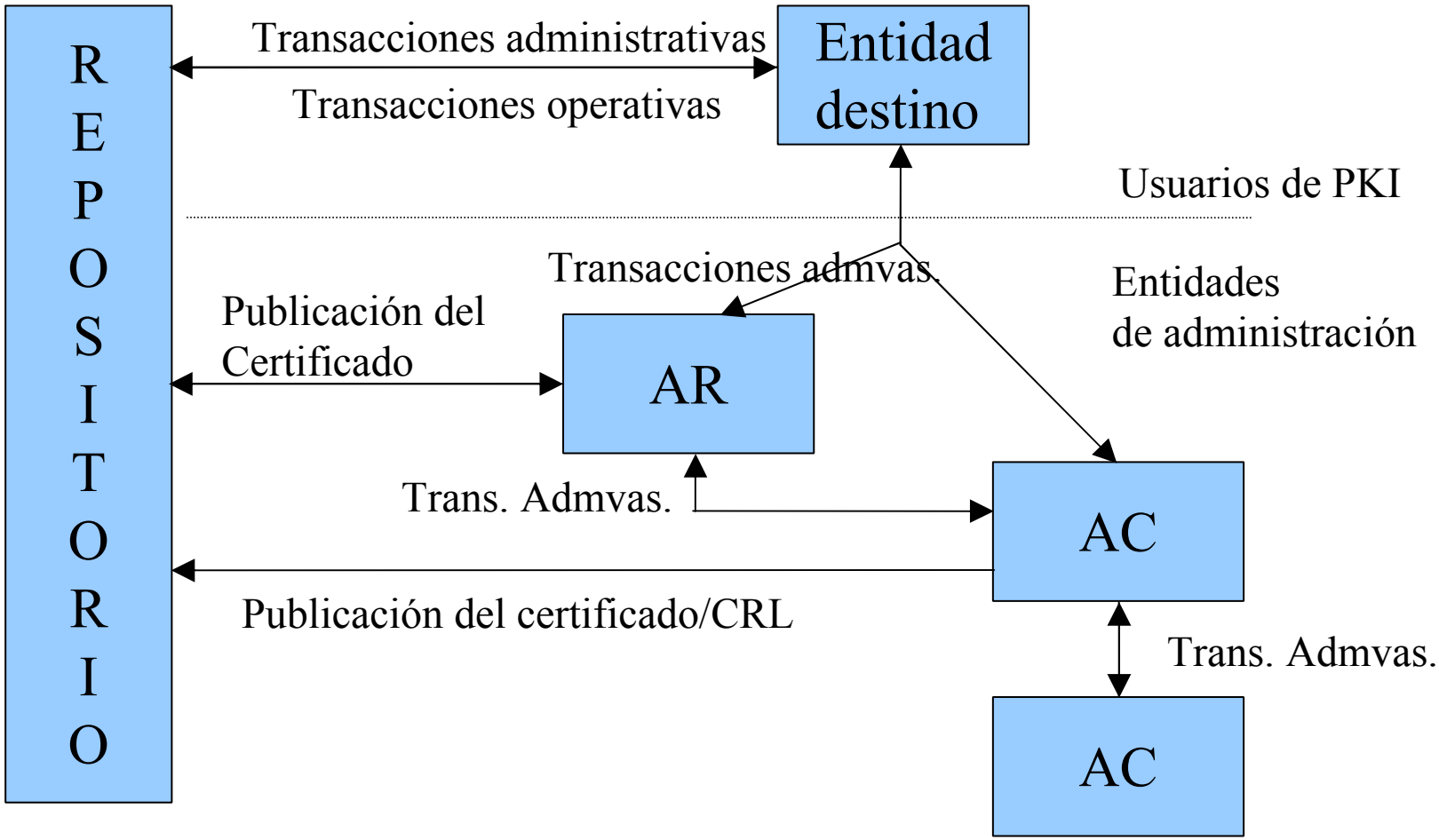
Estándares PKCS

- **PKCS Public Key Cryptography Standard**
- **Especificaciones producidas por RSA Labs en cooperación con desarrolladores de criptografía de clave pública.**
- **Varias aportaciones han pasado a formar parte de otros estándares: PKIX, SET, S/MIME y SSL.**
- **Tiene compatibilidad con otros estándares como:**
  - **PEM (Privacy Enhaced Mail)**
  - **Directorios X.500**
  - **Mensajes X.400**
  - **NIST DSS (Digital Signature Standard)**

Estándares PKCS

- **Estándares:**
  - **PKCS#1 RSA Encryption Standard**
  - **PKCS#3 Diffie-Hellman Key Agreement Standard**
  - **PKCS#5 Password-Based Encryption Standard**
  - **PKCS#6 Extended-Certificate Syntax Standard**
  - **PKCS#7 Cryptographic Message Syntax Standard**
  - **PKCS#8 Private Key Information Syntax Standard**
  - **PKCS#9 Selected Attribute Types**
  - **PKCS#10 Certification Request Syntax Standard**

Arquitectura PKIX



Funciones PKIX

- **Registro**
- **Iniciación**
- **Certificación**
- **Recuperación de la pareja de claves**
- **Generación de claves.**
- **Actualización de la clave.**
- **Certificación cruzada**
- **Revocación**
- **Distribución y publicación del certificado**

Especificaciones PKIX

- **Certificados X.509v3 y extensiones CRL v2**
- **Protocolos operativos: LDAP, HTTP, FTP y X.500**
- **Protocolos de administración:**
  - **CMP Certificate Management Protocol**
  - **CMS Cryptographic Messages Syntax**
- **Servicio de registro de hora**
- **Certificación de datos**

Entidades PKIX

- **Autoridad de Registro (opcional)**
  - Autenticación personal del sujeto que se registra
  - Verificación de la validez de la información suministrada por el sujeto
  - Validar el derecho del sujeto a los atributos del certificado solicitado
  - Prueba de posesión (POP)
  - Generación del par de claves
  - Iniciación del proceso de registro con la AC
  - Almacenamiento de la clave privada
  - Iniciación del proceso de recuperación de clave
- **Autoridad certificadora**
  - Creación, expedición y revocación de certificados
- **Repositorio**
  - Almacenamiento público de certificados y CRLs.

Gracias por su atención

http://www.sekureit.com