

Seguretat Informatica (SI)

Tema 2. Criptografía

Temario

- ▶ Tema 1. Introducción
 - ▶ Tema 2. Criptografía
 - ▶ Tema 4. Infraestructura PKI
-
- ▶ Tema 5. Seguridad en la red
 - ▶ Tema 6. Seguridad en las aplicaciones
-
- ▶ Tema 3. Seguridad en los sistemas operativos
 - ▶ Tema 7. Análisis forense



Temario

- ▶ Tema 1. Introducción
- ▶ **Tema 2. Criptografía**
- ▶ Tema 4. Infraestructura PKI

- ▶ Tema 5. Seguridad en la red
- ▶ Tema 6. Seguridad en las aplicaciones

- ▶ Tema 3. Seguridad en los sistemas operativos
- ▶ Tema 7. Análisis forense



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. Motivación

- ▶ Confidencialidad: solo origen y destino deben poder entender el mensaje
- ▶ Autentificación: origen y destino deben poder confirmar la identidad del otro
- ▶ Integridad del mensaje: origen y destino quieren poder asegurar que el mensaje se recibe sin alterar y que nadie más lo haya podido recibir
- ▶ Acceso y disponibilidad: los servicios deben ser accesibles y disponibles a los usuarios



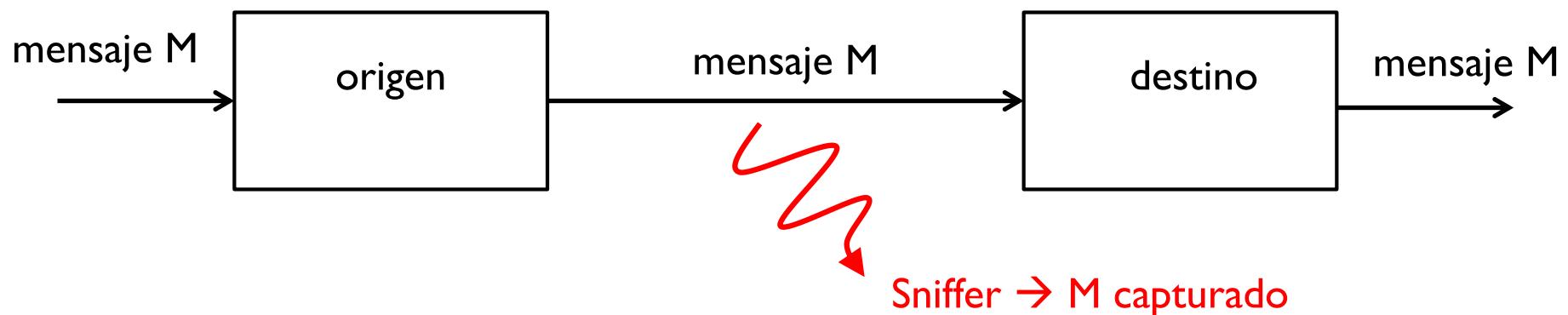
Tema 2. Motivación

- ▶ ¿Que es lo que puede hacer un “bad boy”?
 - ▶ Eavesdrop: interceptar mensajes
 - ▶ Insertar mensajes en una conexión
 - ▶ Impersonation: hacerse pasar por otro alterando campos de los datos (por ejemplo @IP origen) para acceder a determinados servicios
 - ▶ Hijacking: meterse en una conexión activa quitando uno de los dos extremos y hacerse pasar por este
 - ▶ Denial of Service: inhabilitar un servicio mediante el envío de gran cantidad de solicitudes desde uno o mas ordenadores (generalmente zombis) hasta saturar los dispositivos de red



Tema 2. Motivación

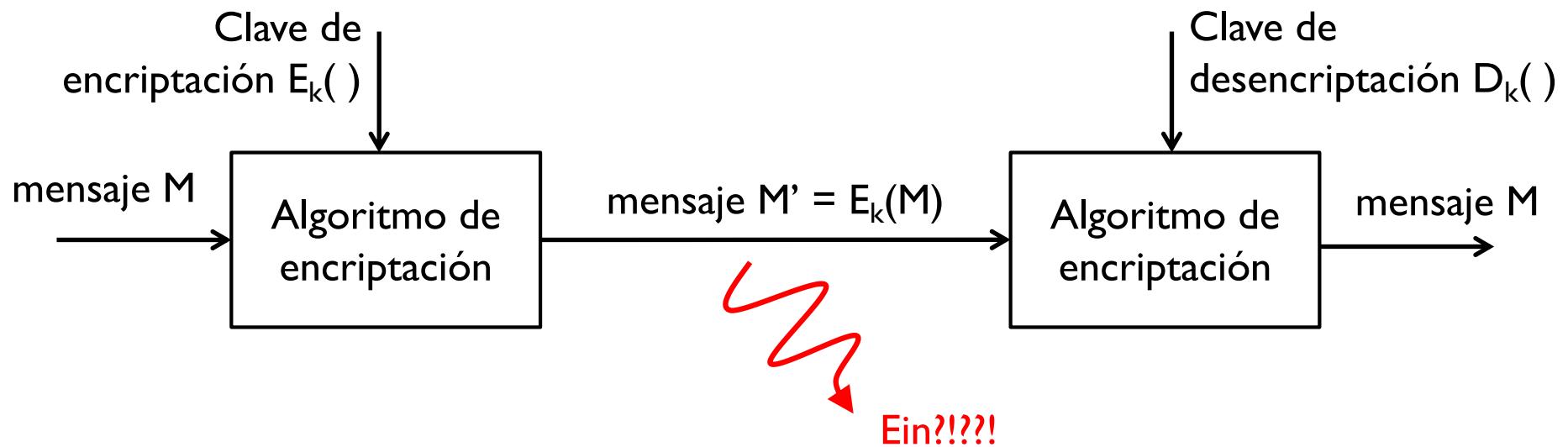
- ▶ Criptografía
 - ▶ Del griego *krypto* (oculta) y *grapho* (escritura)
 - ▶ Literalmente escritura oculta
 - ▶ Se ocupa de las técnicas de cifrado o codificado destinadas a alterar la representación lingüística de un mensaje con el fin de hacerlo ininteligible a receptores no autorizados



Tema 2. Motivación

▶ Criptografía

- ▶ Del griego *krypto* (oculta) y *grapho* (escritura)
- ▶ Literalmente escritura oculta
- ▶ Se ocupa de las técnicas de cifrado o codificado destinadas a alterar la representación lingüística de un mensaje con el fin de hacerlo ininteligible a receptores no autorizados



Tema 2. Criptosistemas históricos

- ▶ Los cifrados más clásicos son el de transposición y el de substitución
- ▶ Cifrado por **transposición**: reordenar las letras en un mensaje
- ▶ Ejemplo:
 - ▶ Transposición con un periodo fijo $k = 3$
 - ▶ $M = \text{CRYPTOGRAPHY}$ se convierte en $E_k(M) = \text{YCROPTAGRYPH}$
 - ▶ $D_k(E_k(M)) = \text{CRYPTOGRAPHY}$



Tema 2. Criptosistemas históricos

- ▶ Los cifrados más clásicos son el de transposición y el de substitución
- ▶ Cifrado por **substitución**: substituir letras o grupos de letras con otras letras o grupos de letras en un mensaje
- ▶ Ejemplo:
 - ▶ Substitución de una letra con otra $k = 3$ posiciones más adelante en el alfabeto
 - ▶ $M = \text{CRYPTOGRAPHY}$ se convierte en $E_k(M) = \text{GUBSXJRUDSKB}$
 - ▶ $D_k(E_k(M)) = \text{CRYPTOGRAPHY}$



Tema 2. Criptosistemas

- ▶ Generalmente
 - ▶ El algoritmo de encriptación y desencriptación es conocido
 - ▶ Lo que es secreto es la clave
 - ▶ En los ejemplos anteriores, k es el factor desconocido en el cifrado



Tema 2. Shannon best practices

- ▶ Idea de “confusión y difusión”
- ▶ Confusión
 - ▶ Hacer que la relación entre clave e mensaje cifrado sea la más compleja posible
 - ▶ Es decir, hacer realmente difícil encontrar la clave aunque se tuviera a disposición un gran número de mensajes no cifrados y mensajes cifrados con una misma clave
- ▶ Difusión
 - ▶ Hacer de manera que el bloque cifrado dependa del bloque no cifrado de una manera muy compleja
 - ▶ Es decir, si se cambiara aunque solo un bit del bloque no cifrado, el bloque cifrado debería cambiar completamente
- ▶ Shannon definió este concepto como una condición necesaria para un cifrado seguro y práctico



Tema 2. Tipos

- ▶ **Criptografía privada**
 - ▶ También conocida como criptografía simétrica
 - ▶ Origen y destino usan la misma clave secreta
- ▶ **Criptografía publica**
 - ▶ También conocida como criptografía asimétrica
 - ▶ Se usan dos claves, una pública y una privada



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. Criptografía privada

- ▶ También conocida como criptografía simétrica
- ▶ Origen y destino usan la misma clave secreta
- ▶ Única técnica de cifrado públicamente conocida hasta junio de 1976
- ▶ Actualmente se usan métodos basados en cifrado en **bloques** y cifrado de **flujo**
- ▶ Se necesita el intercambio de la clave entre los dos extremos a través de un sistema seguro
 - ▶ Hoy en día existen métodos de intercambio de claves de forma segura sobre un medio no seguro (por ejemplo el Diffie-Hellman)



Tema 2. Criptografía privada

- ▶ **Cifrado en bloques**
 - ▶ Se define un grupo de bits, llamado **bloque**, que tiene una transformación invariante
 - ▶ Por ejemplo el bloque de bits 1100 se transforma siempre en el 0111
- ▶ **Estándares más conocidos**
 - ▶ One Time Pad (OTP)
 - ▶ Data Encryption Standard (DES)
 - ▶ 3DES
 - ▶ Advanced Encryption Standard (AES)



Tema 2. OTP

- ▶ Cada bloque de bits del mensaje es encriptado usando una clave secreta aleatoria de la misma longitud que el bloque

```
SENDING
-----
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
pad:      1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      -----
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...
```

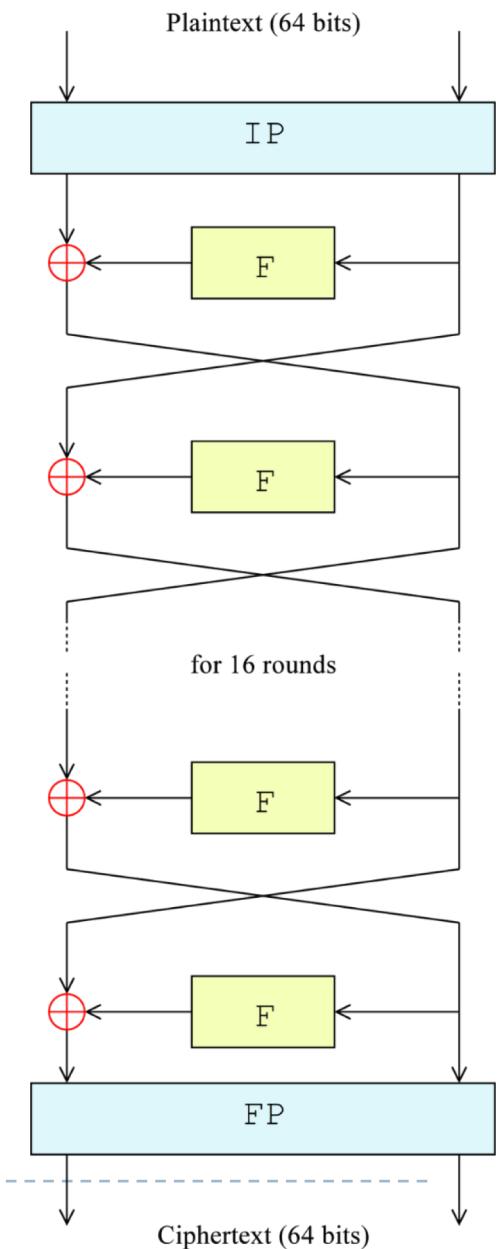
```
RECEIVING
-----
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...
pad:      1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      -----
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
```

- ▶ Si la clave es realmente aleatoria, del mismo tamaño que un bloque del mensaje y se usa una única vez, el mensaje cifrado es imposible de desencriptar sin conocer la clave
- ▶ Usado durante la guerra fría para la comunicación entre EEUU y URSS (famoso teléfono rojo en las pelis)



Tema 2. DES

- ▶ Elaborado por IBM y estandarizado en el 1976
- ▶ Usa bloques de 64 bites que se transforman en bloques cifrados de 64 bits
- ▶ Se usa una clave de 56 bits
- ▶ El algoritmo es conocido (en la figura)
 - ▶ Consiste de una permutación inicial (IP) y una permutación final (FP) que son una el inverso del otra
 - ▶ Y de 16 rondas F iguales
 - ▶ Antes de empezar las rondas, el bloque se divide en dos mitades de 32 bits que se procesan alternativamente en las rondas F
 - ▶ En cada ronda F, una mitad de 32 bits se mezcla con parte de la clave y el resultado se combina con la otra mitad de 32 bits



Tema 2. DES

- ▶ Fue la técnica de encriptación aceptada por la NSA de EEUU
 - ▶ Su esquema base así como sus mejoras fueron usadas hasta el 26 de mayo de 2002 cuando fue reemplazado por el AES
-
- ▶ El ataque más práctico para romper el cifrado DES es la fuerza bruta, es decir usar una por una todas las combinaciones posibles de claves que son 2^{56}
 - ▶ De hecho, se especula que la NSA impuso una clave de solo 56 bits porque en aquellos tiempos sola la NSA tenía la capacidad computacional necesaria para romper el cifrado DES
 - ▶ Hoy en día se puede descifrar un DES en pocos minutos (en 1998 se demostró que era rompible en 2 días)



Tema 2. 3DES

- ▶ Después de descubrir que el DES es “fácilmente” rompible, se pasó a usar el 3DES
- ▶ El 3DES aplica el DES tres veces con tres claves distintas, haciendo así incrementar la clave hasta los 168 bits (3×56 bits)
- ▶ De momento no hay vulnerabilidad conocida pero es extremadamente lento
- ▶ AES puede llegar a ser 6 veces más rápido que el 3DES



Tema 2. AES

- ▶ Reemplazo del DES como estándar de la NSA de EEUU desde 2002
- ▶ También conocido como cifrado Rijndael por sus dos autores Joan Daemen y Vincent Rijman que lo estandarizaron el 26 de noviembre de 2001
- ▶ Basado en una red de sustitución y permutación
- ▶ Relativamente fácil de implementar y usa poca memoria
- ▶ Hoy en día se usa a gran escala (por ejemplo en WPA2 en 802.11)
- ▶ Se usan bloques de 128 bits y tamaños de claves de 128, 192 o 256 bits



Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se organizan los 128 bits en una matriz de 4x4 bytes (16 bytes x 8 = 128 bits)

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$A_{3,1}$	$a_{3,2}$	$a_{3,3}$



Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se organizan los 128 bits en una matriz de 4x4 bytes (16 bytes × 8 = 128 bits)
 - ▶ Se hace un primera operación de combinación de cada byte con la clave modificada según una determinada operación

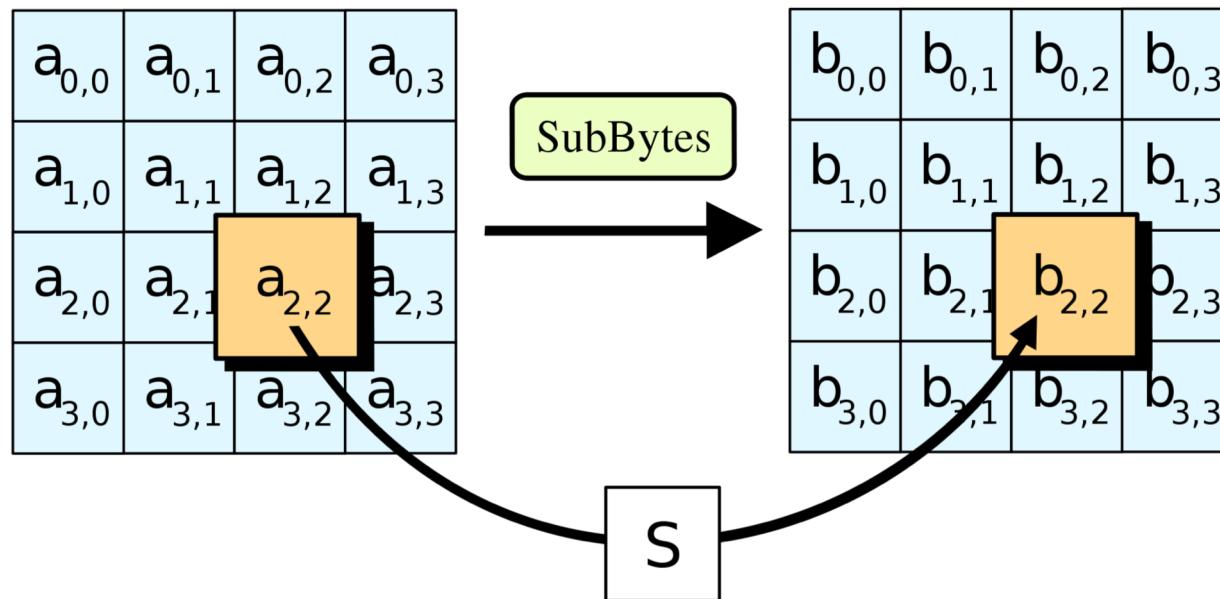
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$A_{3,1}$	$a_{3,2}$	$a_{3,3}$

+ RoundKey



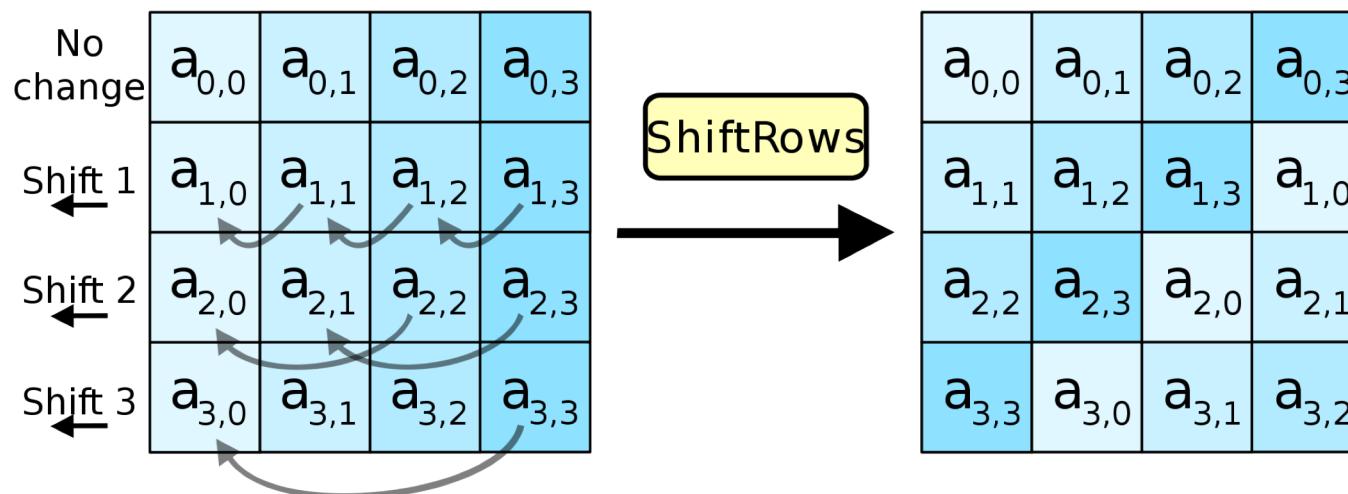
Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se hacen luego 10 (clave de 128 bits), 12 (192 bits) o 14 (256 bits) rondas, cada una con estos pasos
 - I. SubBytes: En cada ronda se hace una substitución de cada byte por otro según una tabla conocida S



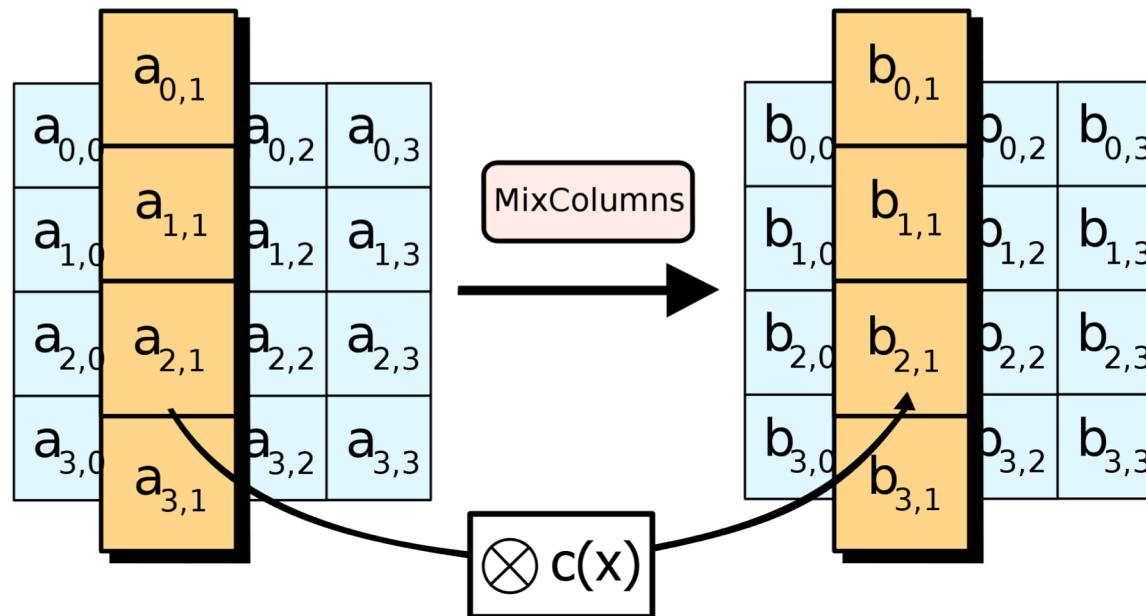
Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se hacen luego 10 (clave de 128 bits), 12 (192 bits) o 14 (256 bits) rondas, cada una con estos pasos
 2. ShiftRows: Las últimas tres líneas de bytes de la matriz se desplazan un cierto número de posiciones



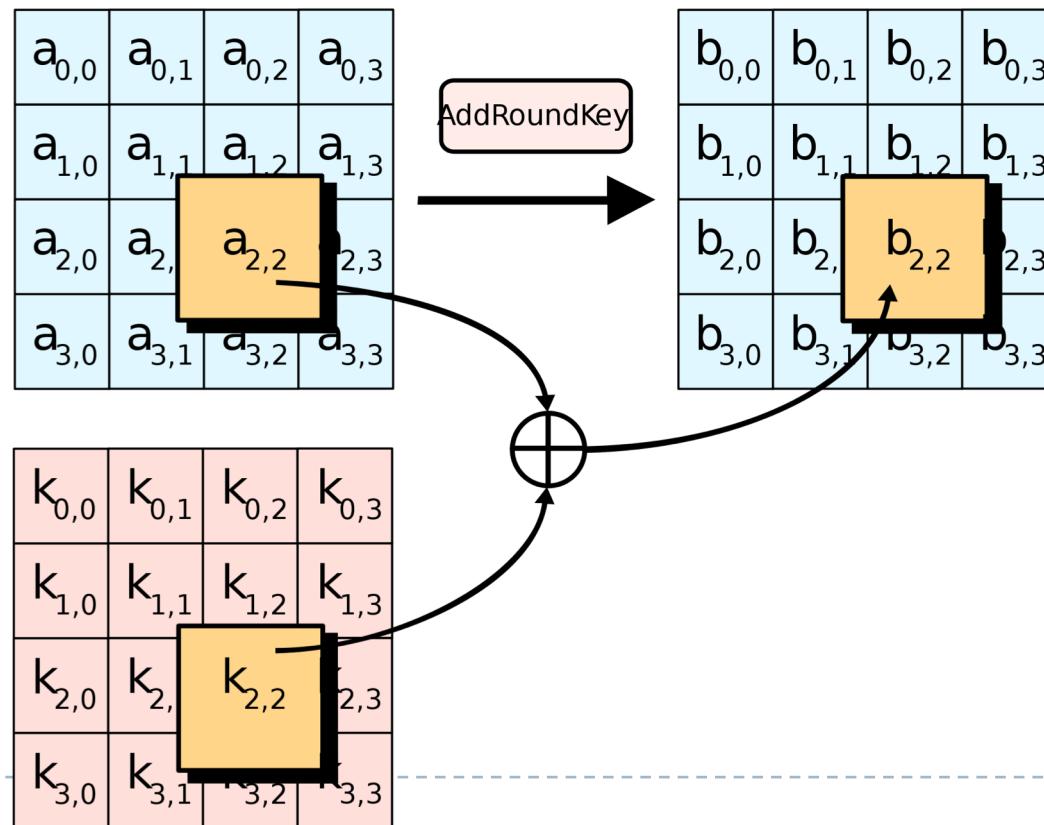
Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se hacen luego 10 (clave de 128 bits), 12 (192 bits) o 14 (256 bits) rondas, cada una con estos pasos
 3. MixColumns: Se combinan los 4 bytes de cada columna usando una transformación lineal conocida $c(x)$



Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se hacen luego 10 (clave de 128 bits), 12 (192 bits) o 14 (256 bits) rondas, cada una con estos pasos
 - 4. AddRoundKey: Se combina cada bytes de la matriz con la clave modificada según la ronda



Tema 2. AES

- ▶ El algoritmo es conocido
 - ▶ Se hace una última etapa donde se aplican una última vez los pasos 1, 2 y 4
 1. SubBytes: En cada ronda se hace una substitución de cada byte por otro según una tabla conocida S
 2. ShiftRows: Las últimas tres líneas de bytes de la matriz se desplazan un cierto número de posiciones
 4. AddRoundKey: Se combina cada bytes de la matriz con la clave modificada según la ronda



Tema 2. Criptografía privada

- ▶ **Cifrado de flujo**
 - ▶ Para algunas aplicaciones, el cifrado en bloques es inapropiada porque los flujos de datos se producen en tiempo real en pequeños fragmentos (por ejemplo telefonía).
 - ▶ Técnicas de cifrado que realizan el cifrado incrementalmente, convirtiendo el mensaje en claro en mensaje cifrado bit a bit.

- ▶ **Estándares más conocidos**
 - ▶ RC4 (usado en WEP de 802.11)
 - ▶ A5/I (usado en GSM)



Tema 2. Problemas

- ▶ **Distribución de la clave**
 - ▶ Los usuarios deben intercambiarse la clave antes de empezar la comunicación
- ▶ **Gestión de la clave**
 - ▶ Si hay n usuarios, cada pareja debe intercambiarse una clave, con lo que se van a necesitar $n(n-1)/2$ claves
- ▶ **Firma digital**
 - ▶ No es posible tener una firma propia digital ya que cada clave es compartida entre, por lo menos, dos usuarios



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ **Criptografía publica**
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. Criptografía publica

- ▶ También conocida como criptografía asimétrica
- ▶ Cada extremo posee dos claves, una pública y una privada
 - ▶ Las claves públicas deben estar disponibles para todos (repositorio de claves públicas)
 - ▶ Las claves privadas las mantienen secretas los usuarios
 - ▶ Las dos claves se generan a través de un algoritmo de generación de claves
- ▶ Los algoritmos de encriptación y desencriptación son conocidos (públicos)
- ▶ De esta forma no se necesita el intercambio de claves para encriptar y desencriptar los mensajes



Tema 2. Criptografía publica

▶ Funcionamiento en el origen

- ▶ El origen A quiere transmitir un mensaje M al destino B
- ▶ A encuentra la clave pública PK_b de B en un directorio publico
- ▶ A computa $M' = E_{PK_b}(M)$ donde E es un algoritmo de encriptación publico
- ▶ A envía el mensaje M' a B

▶ Funcionamiento en el destino

- ▶ El destino B recupera su clave privada SK_b
- ▶ B computa $D_{SK_b}(M') = M$ donde D es un algoritmo de desencriptación publico
- ▶ B lee el mensaje M



Tema 2. Firma digital

- ▶ Esta forma de encriptar también se usa para la firma digital pero de forma inversa
- ▶ Si U quiere firmar un mensaje M , simplemente aplica el algoritmo E con su clave privada de forma que el mensaje firmado es $S = E_{SK_u}(M)$
- ▶ Para verificar que el que ha firmado es realmente U , cualquier usuario puede aplicar el algoritmo de desencriptación usando la clave publica de U sobre el mensaje cifrado y comparar el resultado con el mensaje no cifrado, es decir verificar que $D_{PK_u}(S) = M$



Tema 2. Criptografía híbrida

- ▶ Se emplean ambos cifrados
 - ▶ Se usa un cifrado asimétrico para enviar la clave del cifrado simétrico al destino usando la clave pública del destino
 - ▶ Se usa el cifrado simétrico para encriptar el mensaje
- ▶ Ejemplos
 - ▶ PGP y GnuPG usan un sistema de cifrado híbrido
 - ▶ La clave de la comunicación (clave simétrica) es cifrada con la clave pública del destino y el mensaje es cifrado con la clave simétrica. Se junta todo en un mismo paquete y se envía
 - ▶ El destino usa su clave privada para descifrar la clave simétrica y luego descifra el mensaje con esta
 - ▶ De esta forma la clave puede cambiar por cada comunicación



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. Diffie-Hellman

- ▶ Usado para
 - ▶ Generación de clave privada en la criptográfica simétrica
 - ▶ Parte del mecanismo de cifrado asimétrico



Tema 2. Diffie-Hellman

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo cíclico finito G de orden n
 - ▶ Un generador $\alpha \in G$
 - ▶ Estos valores se pueden intercambiar sin cifrar



Tema 2. Diffie-Hellman

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden n
 - ▶ Un generador $\alpha \in G$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G$
 - ▶ Computa el valor $\alpha^a \text{ mod } n$
 - ▶ Envía el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G$
 - ▶ Computa el valor $\alpha^b \text{ mod } n$
 - ▶ Envía el resultado a A



Tema 2. Diffie-Hellman

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden n
 - ▶ Un generador $\alpha \in G$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G$
 - ▶ Computa el valor $\alpha^a \text{ mod } n$
 - ▶ Envía el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G$
 - ▶ Computa el valor $\alpha^b \text{ mod } n$
 - ▶ Envía el resultado a A
- ▶ A
 - ▶ Recibe $\alpha^b \text{ mod } n$
 - ▶ Computa $(\alpha^b \text{ mod } n)^a \text{ mod } n = X$
- ▶ B
 - ▶ Recibe $\alpha^a \text{ mod } n$
 - ▶ Computa $(\alpha^a \text{ mod } n)^b \text{ mod } n = X$



Tema 2. Diffie-Hellman

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden n
 - ▶ Un generador $\alpha \in G$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G$
 - ▶ Computa el valor $\alpha^a \text{ mod } n$
 - ▶ Envía el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G$
 - ▶ Computa el valor $\alpha^b \text{ mod } n$
 - ▶ Envía el resultado a A
- ▶ A
 - ▶ Recibe $\alpha^b \text{ mod } n$
 - ▶ Computa $(\alpha^b \text{ mod } n)^a \text{ mod } n = X$
- ▶ B
 - ▶ Recibe $\alpha^a \text{ mod } n$
 - ▶ Computa $(\alpha^a \text{ mod } n)^b \text{ mod } n = X$

► **X es la clave privada y solo la conocen A y B**

Tema 2. Diffie-Hellman

- ▶ Mecanismo usado para compartir una clave privada

- ▶ Los usuarios A y B

- ▶ Eligen un grupo finito G de orden n
- ▶ Un generador $\alpha \in G$
- ▶ Estos valores se pueden intercambiar sin cifrar

- ▶ A

- ▶ Elige un número $a \in G$
- ▶ Computa el valor $\alpha^a \text{ mod } n$
- ▶ Envía el resultado a B

- ▶ B

- ▶ Elige un número $b \in G$
- ▶ Computa el valor $\alpha^b \text{ mod } n$
- ▶ Envía el resultado a A

- ▶ A

- ▶ Recibe $\alpha^b \text{ mod } n$
- ▶ Computa $(\alpha^b \text{ mod } n)^a \text{ mod } n = X$

Números privados,
solo A conoce a, solo B conoce b

- ▶ B

- ▶ Recibe $\alpha^a \text{ mod } n$
- ▶ Computa $(\alpha^a \text{ mod } n)^b \text{ mod } n = X$

▶ X es la clave privada y solo la conocen A y B

Tema 2. Diffie-Hellman - Ejemplo

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 53$
 - ▶ Un generador $\alpha \in G = 2$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 29$
 - ▶ Computa el valor $2^{29} \bmod 53 = 45$
 - ▶ Envía 45 el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G = 19$
 - ▶ Computa el valor $2^{19} \bmod n = 12$
 - ▶ Envía 12 el resultado a A

▶ 21 es la clave privada y solo la conocen A y B

Tema 2. Diffie-Hellman - Ejercicio

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 11$
 - ▶ Un generador $\alpha \in G = 3$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 7$
- ▶ B
 - ▶ Elige un número $b \in G = 8$



Calcula la clave privada

Tema 2. Diffie-Hellman - Ejercicio

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 11$
 - ▶ Un generador $\alpha \in G = 3$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 7$
 - ▶ Computa el valor $3^7 \text{ mod } 11 = 9$
 - ▶ Envía 9 el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G = 8$
 - ▶ Computa el valor $3^8 \text{ mod } n = 5$
 - ▶ Envía 5 el resultado a A

▶ 3 es la clave privada y solo la conocen A y B

Tema 2. Diffie-Hellman - Ejercicio

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 217$
 - ▶ Un generador $\alpha \in G = 5$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 27$
- ▶ B
 - ▶ Elige un número $b \in G = 20$



Calcula la clave privada

Tema 2. Algún problema?

- ▶ Calcular $5^{27} \bmod 217$
- ▶ Complicado cuando los números son demasiado grandes
- ▶ Pero ...



Tema 2. Algún problema?

- ▶ Calcular $5^{27} \text{ mod } 217$
- ▶ Complicado cuando los números son demasiado grandes
- ▶ Pero ...
- ▶ La aritmética modular simplifica estos cálculos



Tema 2. Algún problema?

- ▶ Calcular $5^{27} \text{ mod } 217$
- ▶ Complicado cuando los números son demasiado grandes
- ▶ Pero ...
- ▶ La aritmética modular simplifica estos cálculos
 - ▶ Dos números a y b se dicen congruentes de modulo n si ambos dejan el mismo resto si los dividimos entre n
 - ▶ $a \equiv b \pmod{n}$
 - ▶ Algoritmo de exponenciación binaria



Tema 2. Exponenciación binaria

- ▶ Se usa para computar números exponenciales sin tratar números excesivamente grandes

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

begin

```
x = 1;  
z1 = binary representation of z;  
// starting by the most significant bit  
foreach bit  $z_i^1 \in z^1$  do  
    x =  $x^2 \bmod n$ ;  
    // multiply x by a if  $z_i^1$  is equal to one  
    if  $z_i^1 == 1$  then  
        x = x · a mod n  
return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit z1i ∈ z1 do
        x = x2 mod n;
        // multiply x by a if z1i is equal to one
        if z1i == 1 then
            x = x · a mod n
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit zi1 ∈ z1 do
        x = x2 mod n;
        // multiply x by a if zi1 is equal to one
        if zi1 == 1 then
            x = x · a mod n
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$
- ▶ Bucle $i = 0$ to 4
 - ▶ $z^1_0 = 1$
 - ▶ $x = 1^2 \bmod 217 = 1$ (operación de squaring)
 - ▶ Si $z^1_0 == 1$ (cierto)
 - ▶ $x = 1 \times 5 \bmod 217 = 5$ (operación de multiply)

```
Exponentiation by squaring (a,z,n)  $x = a^z \bmod n$ 
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit  $z_i^1 \in z^1$  do
        x =  $x^2 \bmod n$ ;
        // multiply x by a if  $z_i^1$  is equal to one
        if  $z_i^1 == 1$  then
            x =  $x \cdot a \bmod n$ 
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$
- ▶ Bucle $i = 0$ to 4
 - ▶ $z^1_1 = 1$
 - ▶ $x = 5^2 \bmod 217 = 25$ (operación de squaring)
 - ▶ Si $z^1_0 == 1$ (cierto)
 - ▶ $x = 25 \times 5 \bmod 217 = 125$ (operación de multiply)

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit z1i ∈ z1 do
        x = x2 mod n;
        // multiply x by a if z1i is equal to one
        if z1i == 1 then
            x = x · a mod n
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$
- ▶ Bucle $i = 0$ to 4
 - ▶ $z^1_2 = 0$
 - ▶ $x = 125^2 \bmod 217 = 15625 \bmod 217 = 1$ (operación de squaring)
 - ▶ Si $z^1_0 == 1$ (falso)

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit z1i ∈ z1 do
        x = x2 mod n;
        // multiply x by a if z1i is equal to one
        if z1i == 1 then
            x = x · a mod n
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$
- ▶ Bucle $i = 0$ to 4
 - ▶ $z^1_3 = 1$
 - ▶ $x = 1^2 \bmod 217 = 1$ (operación de squaring)
 - ▶ Si $z^1_0 == 1$ (cierto)
 - ▶ $x = 1 \times 5 \bmod 217 = 5$ (operación de multiply)

```
Exponentiation by squaring (a,z,n)  $x = a^z \bmod n$ 
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit  $z_i^1 \in z^1$  do
        x =  $x^2 \bmod n$ ;
        // multiply x by a if  $z_i^1$  is equal to one
        if  $z_i^1 == 1$  then
            x =  $x \cdot a \bmod n$ 
    return x
```



Tema 2. Exponenciación binaria

- ▶ Hay que calcular $5^{27} \bmod 217$
- ▶ Se calcula el binario de 27 que es 11011
- ▶ Al principio $x = 1$
- ▶ $z^1 = 11011$
- ▶ Bucle $i = 0$ to 4
 - ▶ $z^1_4 = 1$
 - ▶ $x = 5^2 \bmod 217 = 25$ (operación de squaring)
 - ▶ Si $z^1_0 == 1$ (cierto)
 - ▶ $x = 25 \times 5 \bmod 217 = 125$ (operación de multiply)
- ▶ El resultado de $5^{27} \bmod 217$ es 125

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z1 = binary representation of z;
    // starting by the most significant bit
    foreach bit z1i ∈ z1 do
        x = x2 mod n;
        // multiply x by a if z1i is equal to one
        if z1i == 1 then
            x = x · a mod n
    return x
```

Tema 2. Diffie-Hellman - Ejercicio

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 217$
 - ▶ Un generador $\alpha \in G = 5$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 27$
 - ▶ Computa el valor $5^{27} \text{ mod } 217 = 125$
 - ▶ Envía 125 el resultado a B
- ▶ B
 - ▶ Elige un número $b \in G = 20$

▶ Calcula la clave privada

Tema 2. Diffie-Hellman - Ejercicio

- ▶ Mecanismo usado para compartir una clave privada
- ▶ Los usuarios A y B
 - ▶ Eligen un grupo finito G de orden $n = 217$
 - ▶ Un generador $\alpha \in G = 5$
 - ▶ Estos valores se pueden intercambiar sin cifrar
- ▶ A
 - ▶ Elige un número $a \in G = 27$
 - ▶ Computa el valor $5^{27} \text{ mod } 217 = 125$
 - ▶ Envía 125 el resultado a B
- ▶ B
 - ▶ Recibe 125
 - ▶ Computa $125^{27} \text{ mod } 217 = 1$
- ▶ A
 - ▶ B
 - ▶ Recibe 125
 - ▶ Computa $125^{20} \text{ mod } 217 = 1$
- ▶ B
 - ▶ Recibe 125
 - ▶ Computa $125^{20} \text{ mod } 217 = 1$

▶ Calcula la clave privada

Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. RSA

- ▶ Generador de clave pública y privada en criptografía asimétrica
- ▶ Algoritmo descrito en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman del MIT
 - ▶ RSA: Rivest, Shamir, Adleman
- ▶ Primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente
- ▶ El funcionamiento se basa en el producto de dos números primos grandes elegidos al azar y mantenidos en secreto
- ▶ Actualmente estos números primos son del orden de 10^{300} (cuanto más grandes, más difícil de encontrarlos)



Tema 2. RSA

- ▶ Se eligen dos números primos muy grandes p y q
- ▶ Se computa $n = p \cdot q$, donde n será la base del modulo (grupo \mathbb{Z}_n)
- ▶ Se computa la función de Euler $\Phi(n) = (p-1) \cdot (q-1)$
- ▶ Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
 - ▶ e es el exponente de la clave publica
- ▶ Se determina d como el multiplicador modular inverso de e mod $\Phi(n)$
 - ▶ d es el exponente de la clave privada
- ▶ La clave publica es (n,e)
- ▶ La clave privada es (n,d)
- ▶ p, q y $\Phi(n)$ también deben mantenerse privados



Tema 2. RSA – cifrado/descifrado

- ▶ A tiene clave publica (n,e) y privada (n,d)
- ▶ Si B quiere enviar un mensaje m a A,
- ▶ B busca la clave publica de A (n,e) y crea el mensaje encriptado c

$$c = m^e \bmod n$$

- ▶ A recibe el mensaje y desencripta usando su clave privada (n,d)

$$m = c^d \bmod n$$



Tema 2. RSA

- ▶ Se eligen dos números primos muy grandes p y q
- ▶ Se computa $n = p \cdot q$, donde n será la base del modulo (grupo \mathbb{Z}_n)
- ▶ Se computa la función de Euler $\Phi(n) = (p-1) \cdot (q-1)$
- ▶ Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
 - ▶ e es el exponente de la clave publica
- ▶ Se determina d como el multiplicador modular inverso de e mod $\Phi(n)$
 - ▶ d es el exponente de la clave privada
- ▶ La clave publica es (n,e)
- ▶ La clave privada es (n,d)
- ▶ p, q y $\Phi(n)$ también deben mantenerse privados



Tema 2. Números coprimos

- ▶ Dos números a y b son coprimos si no tienen ningún factor primo en común
- ▶ Dicho de otra manera
 - ▶ Si no tienen otro divisor común más que 1
 - ▶ Equivalentemente son coprimos , si y solo si, su máximo común divisor es igual a 1, $(\text{mcd}(a, b) = 1)$



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1

- ▶ 45 y 6 son coprimos?



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1
- ▶ 45 y 6 son coprimos?
- ▶ Divisores de 45: 1, 3 y 5
- ▶ Divisores de 6: 1, 2 y 3



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1
- ▶ 45 y 6 son coprimos?
 - ▶ Divisores de 45: 1, 3 y 5
 - ▶ Divisores de 6: 1, 2 y 3
- ▶ Tienen 1 y 3 en común
 - ▶ El máximo común divisor de hecho es 3
- ▶ No son coprimos!



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1

- ▶ 120 y 23 son coprimos?



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1
- ▶ 120 y 23 son coprimos?
 - ▶ Divisores de 120: 1, 2, 3 y 5
 - ▶ Divisores de 23: 1 y 23
- ▶ Son coprimos ya que solo tienen el 1 en común



Tema 2. Números coprimos - Ejemplo

- ▶ Son coprimos si no tienen otro divisor común más que 1
- ▶ 120 y 23 son coprimos?
- ▶ Resolución más rápida:
- ▶ 23 es un número primo, simplemente hay que verificar que $120/23 = 5,21739\dots \rightarrow$ no es un número entero
- ▶ 23 no es un divisor de 120, por lo tanto son coprimos



Tema 2. RSA

- ▶ Se eligen dos números primos muy grandes p y q
- ▶ Se computa $n = p \cdot q$, donde n será la base del modulo (grupo \mathbb{Z}_n)
- ▶ Se computa la función de Euler $\Phi(n) = (p-1) \cdot (q-1)$
- ▶ Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
 - ▶ e es el exponente de la clave publica
- ▶ Se determina d como el multiplicador modular inverso de e mod $\Phi(n)$
 - ▶ d es el exponente de la clave privada
- ▶ La clave publica es (n,e)
- ▶ La clave privada es (n,d)
- ▶ p, q y $\Phi(n)$ también deben mantenerse privados



Tema 2. Multiplicador modular inverso

- ▶ Se determina d como el multiplicador modular inverso de $e \bmod \Phi(n)$

$$d = e^{-1} \bmod \Phi(n)$$

- ▶ Dicho de otra manera $(d \cdot e) \bmod \Phi(n)$ es igual a 1
 - ▶ El multiplicador modular inverso de $e \bmod \Phi(n)$ existe solo si e y $\Phi(n)$ son coprimos
- ▶ ¿Como se calcula este inverso?
 - ▶ Un poco de ecuaciones ahora



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$392 = 27 \times 14 + 14 \rightarrow$ se calculan cociente y residuo



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$392 = 27 \times 14 + 14 \rightarrow$ divisor y residuo se expanden en la siguiente

$$27 = 14 \times 1 + 13$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$27 = 14 \times 1 + 13 \rightarrow$ divisor y residuo se expanden en la siguiente

$$14 = 13 \times 1 + 1$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1 \rightarrow \text{hasta que quede 1 como residuo}$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$1 = 14 - 1 \times 13 \rightarrow$ ahora se gira la última para que quede como 1 =



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 14 - 1 \times 13$$

$13 = 27 - 1 \times 14 \rightarrow$ y la penúltima para que quede como $13 =$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 14 - 1 \times 13$$

13 = 27 - 1 × 14 → y se substituye el 13 de la primera por esta ecuación

$$\rightarrow 1 = 14 - 1 \times (27 - 1 \times 14)$$

$$\rightarrow 1 = 14 - 1 \times 27 + 1 \times 14$$

$$\rightarrow 1 = 2 \times 14 - 1 \times 27$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 14 - 1 \times 13$$

$$13 = 27 - 1 \times 14$$

$$\rightarrow 1 = 14 - 1 \times (27 - 1 \times 14)$$

$$\rightarrow 1 = 14 - 1 \times 27 + 1 \times 14$$

$$\rightarrow 1 = 2 \times 14 - 1 \times 27 \rightarrow \text{deben quedar divisor y residuo de la primera}$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 14 - 1 \times 13$$

$$13 = 27 - 1 \times 14$$

$$\rightarrow 1 = 14 - 1 \times (27 - 1 \times 14)$$

$$\rightarrow 1 = 14 - 1 \times 27 + 1 \times 14$$

$$\rightarrow 1 = 2 \times 14 - 1 \times 27 \rightarrow \text{nos quedamos con esta}$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 2 \times 14 - 1 \times 27$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 2 \times 14 - 1 \times 27$$

$$14 = 392 - 14 \times 27 \rightarrow \text{se gira la primera para que quede como } 14 =$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 2 \times 14 - 1 \times 27$$

14 = 392 - 14 x 27 → y se substituye el 14 de la primera por esta ecuación

$$\rightarrow 1 = 2 \times (392 - 14 \times 27) - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 28 \times 27 - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 29 \times 27$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 2 \times 14 - 1 \times 27$$

$14 = 392 - 14 \times 27 \rightarrow$ y se substituye el 14 de la primera por esta ecuación

$$\rightarrow 1 = 2 \times (392 - 14 \times 27) - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 28 \times 27 - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 29 \times 27 \rightarrow$$
 deben quedar los valores de e y $\Phi(n)$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

$$392 = 27 \times 14 + 14$$

$$27 = 14 \times 1 + 13$$

$$14 = 13 \times 1 + 1$$

$$1 = 2 \times 14 - 1 \times 27$$

$14 = 392 - 14 \times 27 \rightarrow$ y se substituye el 14 de la primera por esta ecuación

$$\rightarrow 1 = 2 \times (392 - 14 \times 27) - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 28 \times 27 - 1 \times 27$$

$$\rightarrow 1 = 2 \times 392 - 29 \times 27 \rightarrow$$
 nos quedamos con esta



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$
- ▶ De momento hemos llegado a eso

$$1 = 2 \times 392 - 29 \times 27$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$
- ▶ De momento hemos llegado a eso
$$1 = 2 \times 392 - 29 \times 27$$
- ▶ Ahora se aplica el mod 392
$$1 \bmod 392 = 1$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$
- ▶ De momento hemos llegado a eso
$$1 = 2 \times 392 - 29 \times 27$$
- ▶ Ahora se aplica el mod 392
$$1 \bmod 392 = 1$$
$$2 \times 392 \bmod 392 = 0$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

- ▶ De momento hemos llegado a eso

$$1 = 2 \times 392 - 29 \times 27$$

- ▶ Ahora se aplica el mod 392

$$1 \bmod 392 = 1$$

$$2 \times 392 \bmod 392 = 0$$

$$-29 \times 27 \bmod 392 \rightarrow 392 - 29 = 363 \rightarrow 363 \times 27 \bmod 392$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

- ▶ De momento hemos llegado a eso

$$1 = 2 \times 392 - 29 \times 27$$

- ▶ Ahora se aplica el mod 392

$$1 \bmod 392 = 1$$

$$2 \times 392 \bmod 392 = 0$$

$$-29 \times 27 \bmod 392 \rightarrow 392 - 29 = 363 \rightarrow 363 \times 27 \bmod 392$$

- ▶ Entonces queda como

$$363 \times 27 = 1 \bmod 392$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

- ▶ De momento hemos llegado a eso

$$1 = 2 \times 392 - 29 \times 27$$

- ▶ Ahora se aplica el mod 392

$$1 \bmod 392 = 1$$

$$2 \times 392 \bmod 392 = 0$$

$$-29 \times 27 \bmod 392 \rightarrow 392 - 29 = 363 \rightarrow 363 \times 27 \bmod 392$$

- ▶ Entonces queda como

$$363 \times 27 = 1 \bmod 392$$

$$\rightarrow 363 = 27^{-1} \bmod 392$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 27, \Phi(n) = 392$
- ▶ Calcular $d = 27^{-1} \bmod 392$

- ▶ De momento hemos llegado a eso

$$1 = 2 \times 392 - 29 \times 27$$

- ▶ Ahora se aplica el mod 392

$$1 \bmod 392 = 1$$

$$2 \times 392 \bmod 392 = 0$$

$$-29 \times 27 \bmod 392 \rightarrow 392 - 29 = 363 \rightarrow 363 \times 27 \bmod 392$$

- ▶ Entonces queda como

$$363 \times 27 = 1 \bmod 392$$

$$\rightarrow \mathbf{d = 363 = 27^{-1} \bmod 392}$$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 23, \Phi(n) = 120$
- ▶ Calcular $d = 23^{-1} \bmod 120$



Tema 2. MM inverso - Ejemplo

- ▶ $e = 23, \Phi(n) = 120$
- ▶ Calcular $d = 23^{-1} \bmod 120$
- ▶ Resultado $d = 47$



Tema 2. RSA

- ▶ Se eligen dos números primos muy grandes p y q
- ▶ Se computa $n = p \cdot q$, donde n será la base del modulo (grupo \mathbb{Z}_n)
- ▶ Se computa la función de Euler $\Phi(n) = (p-1) \cdot (q-1)$
- ▶ Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
 - ▶ e es el exponente de la clave publica
- ▶ Se determina d como el multiplicador modular inverso de e mod $\Phi(n)$
 - ▶ d es el exponente de la clave privada
- ▶ La clave publica es (n,e)
- ▶ La clave privada es (n,d)
- ▶ p, q y $\Phi(n)$ también deben mantenerse privados



Tema 2. RSA - Ejemplo

- ▶ Se eligen dos números primos muy grandes $p = 61$ y $q = 53$
- ▶ Se computa $n = p \cdot q = 61 \cdot 53 = 3223$
- ▶ Se computa $\Phi(n) = (p-1) \cdot (q-1) = 60 \cdot 52 = 3120$
- ▶ Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
 - ▶ $e = 17$
- ▶ Se determina d como el multiplicador modular inverso de e mod $\Phi(n)$
 - ▶ $d = e^{-1} \text{ mod } \Phi(n) = 17^{-1} \text{ mod } 3120 = 2753$
- ▶ La clave publica es $(n,e) = (3233, 17)$
- ▶ La clave privada es $(n,d) = (3233, 2753)$



Tema 2. RSA – cifrado/descifrado

- ▶ A tiene clave publica (3233, 17) y clave privada (3233, 2753)

- ▶ Si B quiere enviar un mensaje $m = 65$ a A,
- ▶ B busca la clave publica de A (3233, 17) y crea el mensaje encriptado c

$$c = m^e \bmod n = 65^{17} \bmod 3233 = 2790$$

- ▶ A recibe el mensaje y desencripta usando su clave privada (3233, 2753)

$$m = c^d \bmod n = 2790^{2753} \bmod 3233 = 65$$



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. ElGamal

- ▶ Se basa en el generador de claves privadas Diffie-Hellman
- ▶ Es un algoritmo de criptografía asimétrica (clave publica/privada)
- ▶ Es de libre uso (no hay patente)
- ▶ Se puede usar en GNU Privacy Guard, PGP y otros sistemas criptográficos

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2

```
iQlcBAEBCAAGBQJaHrrMAAoJEA5SAxxF+nojApYQAMxICG2ivxBKS9KGpq51bjFo  
kiypqYo2WAMu25v9q/b2kHijzA4VgOSaZ+UrPMgzuHWdXoJPHPvypMFnbYHz95eg  
fNVxBKi/UAbSZBmuktq/wtcyzbfXOi0nu+pGggEZEM5W9KGZ5tQ/q18WwbJgZXnX  
q96YyvSbZltpHIL5Z7LRxOILNtN9oA3NpxeCBRof0vds0uRP1alEwxJZBjj9OpVg  
W9flMe1STrBmPGcTEB8aCo2Buwd9pdwd0oSKkX3Gb9jRgl3CMmGmqHtfWA8NZYXH  
L3Vv10Tar4Yv6oghf1nMHSmrK/+dhkMYqhXTj/JXT9wctsqNCYrefqmoYPLrL4dx  
K6bV66ITNr65Age+BWwc0clmRTs9iPX0g2giLeji7HjB+z/aHvFUyvmLIMGMSIsH  
Uzf7e9lpMoJhDDgz93I/7UfEbXAFb3OGZMvOX90smNgkTXI9dunyMo0XZ9KnsTJK  
CVZoFMQDW+ +WxFY1QvW/JZFwYeqDqlZ/nluscPlg/Lf25DtGzHUoBR3Al8qRmDp5  
I4fXYnLfyZFJ2BjsVmzLIFakGoVTWg/akVu3qtzMrKXIGbOdaTuchhFTzOfHitqD  
+zKdKKII7mHpazP5Nn2OIBfPD4UNbGh13yUD7GDxqBjjSSolKj01RdhdAX058kM8  
8PqrxFVeYn4P5SzTsRurF  
=3i08  
-----END PGP SIGNATURE-----
```



Tema 2. ElGamal - preparación

- ▶ Se elige grupo cíclico finito G de orden n
- ▶ Un elemento α de este grupo $\alpha \in G$
- ▶ Un usuario A
 - ▶ Elige un número aleatorio a (será parte de su clave privada)
 - ▶ Calcula $\alpha^a \in G$ (esta será la clave publica)
 - ▶ $\alpha, G, \alpha^a \in G$ son todos valores públicos (a debe mantenerse secreta)



Tema 2. ElGamal - encriptación

- ▶ Si B quiere enviar un mensaje $m \in \mathbf{G}$ a A, entonces debe
 - ▶ Recibir la clave publica de A $(\alpha, \mathbf{G}, \alpha^a)$
 - ▶ Elegir un número aleatorio b y calcular $\alpha^b \in \mathbf{G}$ *(nota)*
 - ▶ Calcular el mensaje cifrado $c = m \cdot (\alpha^a)^b \in \mathbf{G}$
 - ▶ Enviar a A el mensaje (α^b, c)
- ▶ Nota: se recomienda que sea de un único uso



Tema 2. ElGamal - desencriptación

- ▶ A recibe el mensaje cifrado (α^b, c)
 - ▶ Calcula $x = (\alpha^b)^a \in \mathbb{G}$
 - ▶ Calcula el mensaje en claro $m = c \cdot x^{-1} \in \mathbb{G}$



Tema 2. ElGamal - desencriptación

- ▶ A recibe el mensaje cifrado (α^b, c)
 - ▶ Calcula $x = (\alpha^b)^a \in \mathbb{G}$
 - ▶ Calcula el mensaje en claro $m = c \cdot x^{-1} \in \mathbb{G}$
- ▶ Os acordáis que es eso ($x^{-1} \in \mathbb{G}$)?



Tema 2. ElGamal - desencriptación

- ▶ A recibe el mensaje cifrado (α^b, c)
 - ▶ Calcula $x = (\alpha^b)^a \in G$
 - ▶ Calcula el mensaje en claro $m = c \cdot x^{-1} \in G$

- ▶ Os acordáis que es eso ($x^{-1} \in G$)?
- ▶ Multiplicador modular inverso



Tema 2. ElGamal - ejemplo

- ▶ $G = 13$
- ▶ $\alpha = 2$
- ▶ Un usuario A
 - ▶ Elige un número aleatorio $a = 9$
 - ▶ Calcula $\alpha^a \in G \rightarrow 2^9 \bmod 13 = 5$
 - ▶ Clave publica = $(2, 13, 5)$
 - ▶ Clave privada = 9
 - ▶ También se podría indicar como $(2, 13, 9)$



Tema 2. ElGamal - ejemplo

- ▶ Un usuario B quiere enviar el mensaje $m=11$ a A
 - ▶ Recibir la clave publica de A $(2, 13, 5)$
 - ▶ Elegir un número aleatorio $b = 10$ y calcular $\alpha^b \in G \rightarrow 2^{10} \text{ mod } 13 = 10$
 - ▶ Calcular el mensaje cifrado $c = m \cdot (\alpha^a)^b \in G$
 $\rightarrow c = 11 \cdot 5^{10} \text{ mod } 13 = 11 \cdot 12 \text{ mod } 13 = 2$
 - ▶ Enviar a A el mensaje $(\alpha^b, c) = (10, 2)$



Tema 2. ElGamal - ejemplo

- ▶ A recibe el mensaje cifrado $(\alpha^b, c) = (10, 2)$
 - ▶ Calcula $x = (\alpha^b)^a \in \mathbb{G} = 10^9 \text{ mod } 13 = 12$
 - ▶ Calcula el mensaje en claro $m = c \cdot x^{-1} \in \mathbb{G}$
 $\rightarrow m = 2 \cdot 12^{-1} \text{ mod } 13$



Tema 2. ElGamal - ejemplo

- ▶ A recibe el mensaje cifrado $(\alpha^b, c) = (10, 2)$

- ▶ Calcula $x = (\alpha^b)^a \in \mathbb{G} = 10^9 \text{ mod } 13 = 12$

- ▶ Calcula el mensaje en claro $m = c \cdot x^{-1} \in \mathbb{G}$

- $\rightarrow m = 2 \cdot 12^{-1} \text{ mod } 13$

- $\rightarrow 12^{-1} \text{ mod } 13 \rightarrow \text{MM inverso}$

$$13 = 12 \times 1 + 1$$

$$1 = 13 - 1 \times 12$$

$$1 \text{ mod } 13 = 1$$

$$13 \text{ mod } 13 = 0$$

$$-1 \times 12 \text{ mod } 13 \rightarrow 13 - 1 = 12 \rightarrow 12 \times 12 \text{ mod } 13$$

$$1 = 12 \times 12 \text{ mod } 13$$

$$12^{-1} = 12 \text{ mod } 13$$

$$\rightarrow m = 2 \cdot 12 \text{ mod } 13 = 11$$



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Tema 2. Firma Digital

▶ Para firmar de forma digital un documento

- ▶ Si U quiere firmar un mensaje M, simplemente aplica el algoritmo E con su clave privada de forma que el mensaje firmado es $S = E_{SKu}(M)$
- ▶ Para verificar que el que ha firmado es realmente U, cualquier usuario puede aplicar el algoritmo de desencriptación usando la clave publica de U sobre el mensaje cifrado y comparar el resultado con el mensaje no cifrado, es decir verificar que $D_{PKu}(S) = M$

VISTO BUENO DEL INFORME ANUAL DE EVALUACIÓN

I. INFORME DEL DIRECTOR/A

Valoración de la consecución de los objetivos por parte del beneficiario/a durante la anualidad a la que se refiere este informe:

- Favorable: se aconseja la continuidad de la ayuda
 NO favorable: NO se aconseja la continuidad de la ayuda

Motivación del informe NO favorable:

Grado aproximado de consecución de los objetivos marcados para la anualidad objeto de este informe:

	Excelente	Notable	Aceptable	Insuficiente
Metodología	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tareas y resultados	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Programa formativo	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Motivación de la calificación:

La valoración del desarrollo de la tesis doctoral hasta este punto es muy positiva. Cabe destacar las numerosas colaboraciones lideradas por el beneficiario con instituciones tanto nacionales (p.e., Telefónica I+D, Fundación i2CAT, ATOS Origin) como internacionales (p.e., Predictive Network Solutions, Brno University of Technology), las cuáles han permitido la preparación de un número substancial de artículos de investigación para su publicación en revistas de prestigio y para su presentación en conferencias. Un ejemplo de estos es el artículo aceptado en la revista indexada en los JCR European Transactions on Telecommunications, o las ponencias en IEEE GLOBECOM o en el Workshop NetCloud 2016.

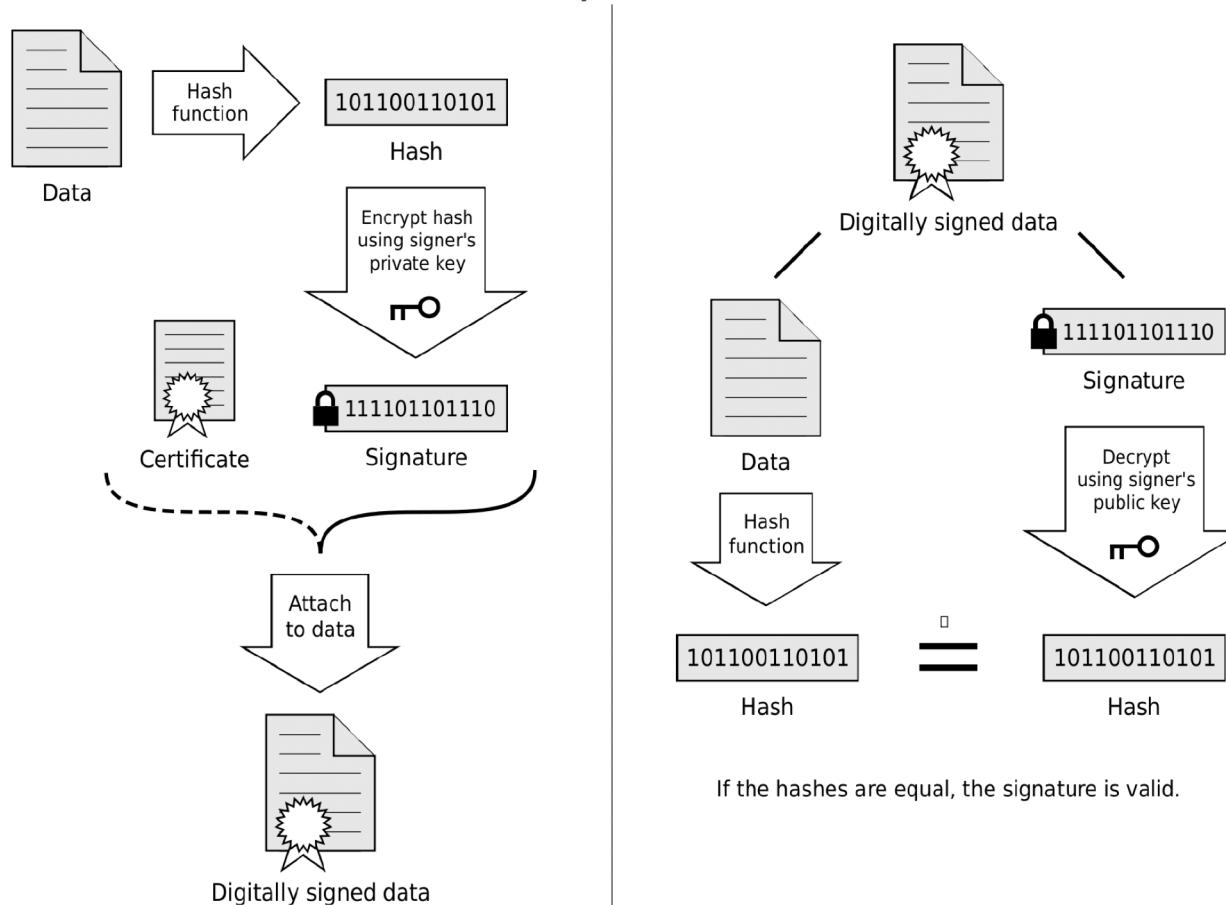
Firma electrónica del director/a:

Una vez firmado, debe enviar este documento a la COMISIÓN ACADÉMICA para que cumplimente y firme electrónicamente la página 8.
Es importante que al firmar NO bloquee el documento.



Tema 2. Firma Digital

- ▶ Ya que cifrar todo el documento puede resultar computacionalmente costoso, lo que se hace es
 - ▶ Calcular una función de Hash (de un tamaño fijo) sobre el documento
 - ▶ Firmar el resultado de esta función
 - ▶ Para autenticar la firma, se hace la operación inversa



Tema 2. RSA Firma Digital

- ▶ RSA se puede usar para firmar digitalmente un documento (no es el único)
- ▶ **Firma**
 - ▶ A tiene clave publica (n,e) y privada (n,d)
 - ▶ A calcula la función Hash $H(m)$ del documento m
 $s = (H(m))^d \text{ mod } n$
 - ▶ A envía el documento no firmado m y s
- ▶ **Verificación**
 - ▶ B recibe el documento no firmado m y la firma s
 - ▶ B calcula la función Hash $H(m)$ del documento m
 - ▶ B calcula $H'(m) = s^e \text{ mod } n$
 - ▶ B verifica que $H(m) = H'(m)$



Tema 2. Índice

- ▶ Motivación
- ▶ Definición
- ▶ Ejemplos
- ▶ Criptografía privada
- ▶ Criptografía publica
- ▶ Firma digital
- ▶ Algunos algoritmos
 - ▶ Diffie-Hellman
 - ▶ RSA
 - ▶ ElGamal
 - ▶ RSA (firma digital)



Seguretat Informatica (SI)

Tema 2. Criptografia - Problemas

Tema 2. Problema 1

- ▶ Alice y Bob quiere usar una clave privada para crear un canal seguro usando criptografía DES
 - ▶ Contestar a estas preguntas
- I) ¿Que pueden usar para compartir una clave privada de forma segura?



Tema 2. Problema 1

- ▶ Alice y Bob quiere usar una clave privada para crear un canal seguro usando criptografía DES
 - ▶ Contestar a estas preguntas
- I) ¿Que pueden usar para compartir una clave privada de forma segura?

El metodo Diffie-Helman



Tema 2. Problema 1

- ▶ Alice y Bob quiere usar una clave privada para crear un canal seguro usando criptografía DES
 - ▶ Contestar a estas preguntas
- I) ¿Que pueden usar para compartir una clave privada de forma segura?

El metodo Diffie-Helman

- 2) Eligen un grupo cíclico finito G de 29 y un generador $\alpha = 2$

Alice elige el número 5

Bob elige el número 12

Describe que valores se intercambian Alice y Bob y que clave privada usaran.



Tema 2. Problema 1

- ▶ Alice y Bob quiere usar una clave privada para crear un canal seguro usando criptografía DES
 - ▶ Contestar a estas preguntas
- I) ¿Que pueden usar para compartir una clave privada de forma segura?

El metodo Diffie-Helman

- 2) Eligen un grupo cíclico finito G de 29 y un generador $\alpha = 2$

Alice elige el número 5

Bob elige el número 12

Describe que valores se intercambian Alice y Bob y que clave privada usaran.

Alice calcula $2^5 \text{ mod } 29 = 3$ y envía 3 a Bob

Bob calcula $2^{12} \text{ mod } 29 = 7$ y envía 7 a Alice

Alice calcula $7^5 \text{ mod } 29 = 16$

Bob calcula $3^{12} \text{ mod } 29 = 16$

16 será la clave privada



Tema 2. Problema 2

- ▶ Alice quiere usar ElGamal para recibir mensajes privados de Bob
 - ▶ Deciden usar el grupo cíclico finito G de 23 y un $\alpha = 11$
 - ▶ Contestar a las siguientes preguntas
- 1) Alice elige $a = 6$ como clave privada. Ayuda Alice a calcular su clave pública
 - 2) Bob quiere enviar el mensaje $m = 10$ a Alice y elige el número $b = 3$.
Ayuda Bob a calcular el mensaje cifrado c
 - 3) Ayuda Alice a descifrar el mensaje c



Tema 2. Problema 2

- ▶ Alice quiere usar ElGamal para recibir mensajes privados de Bob
 - ▶ Deciden usar el grupo cíclico finito G de 23 y un $\alpha = 11$
 - ▶ Contestar a las siguientes preguntas
- 1) Alice elige $a = 6$ como clave privada. Ayuda Alice a calcular su clave pública
- $$\alpha^a \in G = 11^6 \bmod 23 = 9$$
- Alice envía a Bob la clave pública $(11, 23, 9)$
- 2) Bob quiere enviar el mensaje $m = 10$ a Alice y elige el número $b = 3$.
Ayuda Bob a calcular el mensaje cifrado c
- 3) Ayuda Alice a descifrar el mensaje c



Tema 2. Problema 2

- ▶ Alice quiere usar ElGamal para recibir mensajes privados de Bob
- ▶ Deciden usar el grupo cíclico finito G de 23 y un $\alpha = 11$
- ▶ Contestar a las siguientes preguntas

1) Alice elige $a = 6$ como clave privada. Ayuda Alice a calcular su clave pública

$$\alpha^a \in G = 11^6 \bmod 23 = 9$$

Alice envía a Bob la clave pública $(11, 23, 9)$

2) Bob quiere enviar el mensaje $m = 10$ a Alice y elige el número $b = 3$.

Ayuda Bob a calcular el mensaje cifrado c

$$\alpha^b \in G = 11^3 \bmod 23 = 20$$

$$c = m \cdot (\alpha^a)^b \in G = 10 \cdot 9^3 \bmod 23 = 22$$

Bob envía a Alice el mensaje $(20, 22)$

3) Ayuda Alice a descifrar el mensaje c



Tema 2. Problema 2

- ▶ Alice quiere usar ElGamal para recibir mensajes privados de Bob
- ▶ Deciden usar el grupo cíclico finito G de 23 y un $\alpha = 11$
- ▶ Contestar a las siguientes preguntas

1) Alice elige $a = 6$ como clave privada. Ayuda Alice a calcular su clave pública

$$\alpha^a \in G = 11^6 \bmod 23 = 9$$

Alice envía a Bob la clave pública $(11, 23, 9)$

2) Bob quiere enviar el mensaje $m = 10$ a Alice y elige el número $b = 3$.

Ayuda Bob a calcular el mensaje cifrado c

$$\alpha^b \in G = 11^3 \bmod 23 = 20$$

$$c = m \cdot (\alpha^a)^b \in G = 10 \cdot 9^3 \bmod 23 = 22$$

Bob envía a Alice el mensaje $(20, 22)$

3) Ayuda Alice a descifrar el mensaje c

$$x = (\alpha^b)^a \in G = 20^6 \bmod 23 = 16$$

$$x^{-1} \in G = 16^{-1} \bmod 23 = 13$$

$$m = c \cdot x^{-1} \in G = 22 \cdot 13 \bmod 23 = 10$$



Tema 2. Problema 3

- ▶ A usa ElGamal con grupo cíclico finito G de 991, un $\alpha = 7$ y su clave privada a es 323
 - ▶ A recibe el mensaje $(\alpha^b = 415, c = 862)$
- I) Calcula el mensaje no cifrado



Tema 2. Problema 3

- ▶ A usa ElGamal con grupo cíclico finito G de 991, un $\alpha = 7$ y su clave privada a es 323
- ▶ A recibe el mensaje $(\alpha^b = 415, c = 862)$

I) Calcula el mensaje no cifrado

$$x = (\alpha^b)^a \in G = 415^{323} \bmod 991 = 850$$

$$x^{-1} \in G = ((\alpha^b)^a)^{-1} \in G = 850^{-1} \bmod 991 = 745$$

$$m = c \cdot x^{-1} \in G = 862 \cdot 745 \bmod 991 = 22$$



Seguretat Informatica (SI)

Tema 2. Criptografia