Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

EXAMEN FINAL

CONVOCATORIA ORDINARIA MAYO 2014

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final Convocatoria Ordinaria — Leganés – Mayo 2014

Apellidos: **Nombre:**

Grupo magistral: **Grupo reducido:**

PREGUNTAS DE RESPUESTA OBJETIVA (1 punto)

Señale con una X la respuesta correcta de cada una de las siguientes preguntas de respuesta objetiva. Cada contestación erróneas resta ¼ del valor que se obtendría si se contestase correctamente.

1. Señale la respuesta correcta.

- ☐ $7^{13} \bmod 13 = 1$.
- ☐ $7^{13} \bmod 13 = 7$.
- ☐ 7 no es generador de Z_{13}.
- ☐ Ninguna de las anteriores es correcta.

2. En los ataques de texto en claro conocido y elegido:

- ☐ Sólo se conoce el texto en claro y el algoritmo de cifrado.
- ☐ En el elegido se conoce la clave.
- ☐ Sólo en el conocido se conoce el algoritmo.
- ☐ En ambos se dispone del criptograma.

3. El método de Kasiski se utiliza:

- ☐ En criptoanálisis de métodos de sustitución monoalfabeto.
- ☐ En criptoanálisis de métodos de sustitución polialfabeto.
- ☐ Complementando al análisis de frecuencias en métodos de sustitución monoalfabeto.
- ☐ Ninguna de las anteriores es correcta.

4. En los modos de cifrado de bloque:

- ☐ En todos los modos de cifrado de bloque cada bloque se cifra separadamente de los demás sin dependencia de otros bloques.
- ☐ En el modo ECB cada bloque cifrado depende del bloque cifrado anteriormente.
- ☐ En el modo CBC el texto cifrado correspondiente a un determinado bloque de texto en claro depende del bloque de texto cifrado anterior. Asimismo, el bloque de texto en claro correspondiente a un determinado bloque de texto cifrado depende del bloque de texto cifrado anterior.
- ☐ En el modo CFB un error en un bit del criptograma afectará sólo a un bloque del texto en claro recuperado.

5. **Considere un cifrador de bloque en modo CFB en el que el texto en claro se dispone en bloques de 16 bits y el cifrador toma entradas de 48 bits. Si un bloque de texto cifrado se recibe con un error en el receptor, dicho error**

- ☐ Afecta a 16 bloques del texto en claro descifrado.
- ☐ Afecta a 3 bloques del texto en claro descifrado.
- ☐ Afecta a 4 bloques del texto en claro descifrado.
- ☐ Afecta a 2 bloques del texto en claro descifrado.

6. **En un criptosistema compuesto por n usuarios:**

- ☐ Si se utiliza cifrado simétrico el número total de claves implicadas es 2n.
- ☐ Si se utiliza cifrado simétrico el número de claves que maneja un usuario es 2n.
- ☐ Si se utiliza cifrado asimétrico el número total de claves implicadas es 2n.
- ☐ Si se utiliza cifrado asimétrico el número de claves que maneja un usuario es 2n.

7. **En criptografía asimétrica:**

- ☐ El algoritmo de clave pública de Diffie-Hellman permite el acuerdo entre dos entidades de una clave simétrica, a través de comunicaciones exclusivamente públicas.
- ☐ El algoritmo de cifrado de El Gamal, produce bloques de texto cifrado mayores que los bloques de texto en claro.
- ☐ El criptoanálisis del algoritmo de Diffie-Hellman se basa en la resolución del problema del logaritmo discreto.
- ☐ Todas las anteriores son correctas.

8. **En relación a la firma digital, el servicio de "no repudio" :**

- ☐ garantiza que los datos recibidos han sido enviados por una entidad autorizada.
- ☐ protege contra la negación de autoría frente a terceras partes.
- ☐ previene del uso no autorizado de un recurso.
- ☐ protege contra el acceso no autorizado a la información.

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final Convocatoria Ordinaria — Leganés – Mayo 2014

Apellidos: **Nombre:**

Grupo magistral: **Grupo reducido:**

9. Señale la respuesta correcta en relación a los parámetros del algoritmo RSA

a

p – número primo, (privado, escogido)
$n = p^2$, (público, calculado)
e, m.c.d. ($\Phi(n),e$) = 1, $1 < e < \Phi(n)$, (público, escogido)
$d = e^{-1}$, [mod($\Phi(n)$)], (privado, calculado)

b

p, q – dos números primos, (público, escogido)
$n = p \cdot q$, (privado, calculado)
e, m.c.d. ($\Phi(n),e$) = 1, $1 < e < \Phi(n)$, (público, escogido)
$d = e^{-1}$, [mod($\Phi(n)$)], (privado, calculado)

x

c

p, q – dos números primos, (privado, escogido)
$n = p \cdot q$, (público, calculado)
e, m.c.d. ($\Phi(n),e$) = 1, $1 < e < \Phi(n)$, (público, escogido)
$d = e^{-1}$, [mod($\Phi(n)$)], (privado, calculado)

d

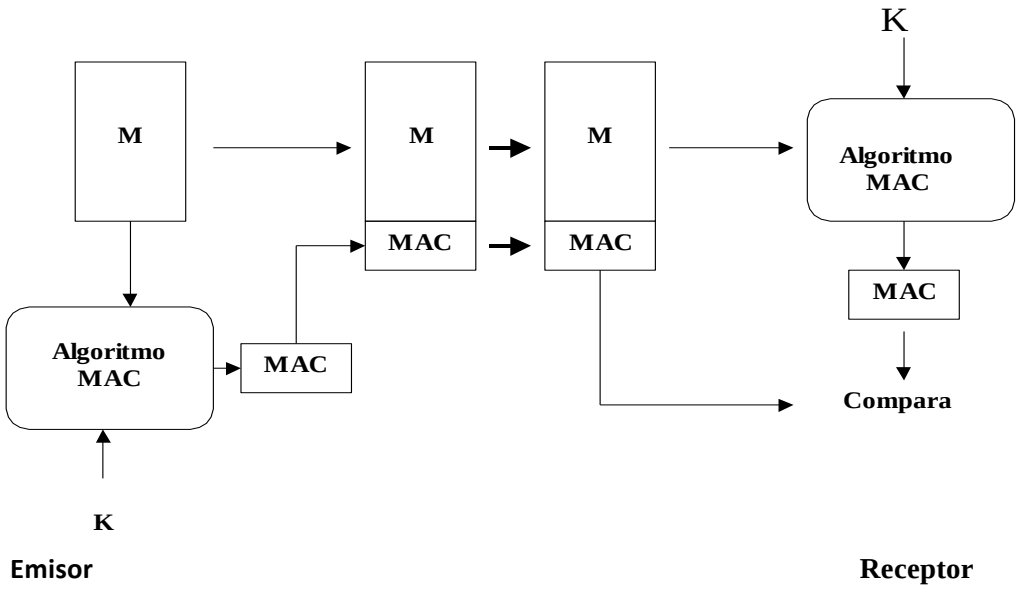
p, q – dos números primos, (privado, escogido)
$n = p \cdot q$, (público, calculado)
e, m.c.d. (e,n) = 1, $1 < e < \Phi(n)$, (público, escogido)
$d = e^{-1}$, (mod(n)], (privado, calculado)

10. Si la información ha sido objeto de una modificación por parte de usuarios no autorizados, entonces se dice que se vio afectada en su _____.

- ☒ Integridad.
- ☐ disponibilidad.
- ☐ validez.
- ☐ confidencialidad.

CUESTION (0,50 puntos)

1. Explique, mediante un diagrama de bloques, la autenticación de mensajes mediante funciones MAC.



El emisor añade un Código de Autenticación de Mensaje (MAC) al mensaje enviado M. Este MAC es un valor de longitud fija, que depende de una clave previamente acordada entre emisor y receptor. El algoritmo para calcular el MAC es público y su construcción se suele basar en funciones resumen (HMAC) o en cifradores de bloque simétricos (CBC-MAC). El receptor puede comprobar la integridad del mensaje recibido M calculando el MAC de dicho mensaje M con la clave K y comparando dicho valor con el MAC recibido. Es computacionalmente imposible encontrar un mensaje M' con la misma MAC que M.

EJERCICIO 1 (1,25 punto)

Considere un sistema de infraestructura de clave pública que sigue el siguiente modelo jerárquico de certificación:

- Cada Autoridad de Certificación tiene un identificador numérico único.
- Los campos de los certificados se expresan en base decimal y siguen el formato especificado en la figura adjunta.
- La firma digital de los certificados sigue un esquema con función resumen proporcionando integridad a todos los campos restantes del certificado. La firma se realiza mediante el algoritmo RSA. La función resumen utilizada (H) produce como salida un dígito decimal y su ejecución consta de dos fases: 1.- Suma en base decimal de todos los campos del certificado y 2.- Suma de los dígitos decimales obtenidos en 1, repitiéndose el proceso hasta obtener un solo dígito decimal (ver ejemplo más abajo).
- A continuación se muestran los campos de los certificados (simplificación del formato X.509) y su descripción.

CAMPO	DESCRIPCIÓN
ID EMISOR	Identificador del emisor del certificado
ID SUJETO	Identificador del sujeto
NUMERO DE SERIE	Número de serie del certificado
ALG_ID	Identificador del algoritmo de firma utilizado
e	Exponente de la clave pública RSA
N	Módulo de la clave pública RSA
FIRMA	Firma digital del certificado

Considere la siguiente información en relación a las tres Autoridades de Certificación del sistema:

AC1 – Autoridad de Certificación Raíz

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final Convocatoria Ordinaria — Leganés – Mayo 2014

Apellidos: **Nombre:**

Grupo magistral: **Grupo reducido:**

Certificado de AC1→ C_{AC1} (1,1,0,1,5,91,34)

Datos de interés de AC1 correspondientes al proceso de emisión de certificados:
Primos: p=7,q=13, exponente de la clave pública RSA: e=5

Salida de la función resumen H aplicada a los campos de C_{AC1}:

1+1+0+1+5+91=99→

9+9=18→ 1+8 =9 → **H_{AC1}= 9**

AC2 – Autoridad subordinada a AC1

Cert_AC2 → C_{AC2} (1,2,2,1,5,51,X)

Datos de interés de AC2 correspondientes al proceso de emisión de certificados:
Primos: p=17,q=3

AC3 – Autoridad subordinada a AC2

Cert_AC3 → C_{AC3} (2,3,4,1,5,21,Y)

1. Calcule la firma de los certificados de las autoridades subordinadas AC3 y AC2.

2. Considere un usuario que recibe un certificado firmado por la AC subordinada AC3, junto a la correspondiente cadena de certificación. Considere que el usuario ya ha verificado la firma de dicho certificado por parte de AC3. Verifique el resto de la cadena de certificación e indique si el usuario puede confiar en el certificado recibido. Si no puede confiar, indique el porqué y realice los cálculos necesarios para subsanarlo. Precise si se requiere algún paso adicional para confiar en el certificado recibido.

SOLUCIONES:

Se adjuntan los datos completos de los cálculos RSA utilizados para firmar

DATO	AC1	AC2	AC3
p	7	17	7
q	13	3	3
n	91	51	21
$\phi(n)$	72	32	12
e	5	5	5
d	29	13	1
Hash Certificado	9	8	9
Firma sobre Hash	34 (81)	**8**	**42**

1 Cálculo de la firma del certificado de la autoridad subordinada AC3 y AC2

AC3

HASH: 2+3+4+1+5+21= 36 → 3+6 = 9 → **H_{AC3}=9**

FIRMA DEL RESUMEN:

No se proporciona d_{AC2} pero lo podemos calcular a partir de p,q y e:

p*q=n→ 17*3=51 → n=51

$\phi(n)=(p-1)*(q-1)=16*2=32$ → $\phi(n)=32$

e*d=1 mod 32 → e=5 → 5d=1 mod 32 → **d_{AC2}=13**

$FRSA_{AC3} = H_{AC3}^{dAC2} \bmod n_{AC2} = 9^{13} \bmod 51=42$ → **$FRSA_{AC3}$=42**

AC2

HASH: 1+2+2+1+5+51=62→6+2=8 → **H_{AC2}=8**

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final Convocatoria Ordinaria — Leganés – Mayo 2014

Apellidos: **Nombre:**

Grupo magistral: **Grupo reducido:**

FIRMA DEL RESUMEN:

De forma parecida a la anterior:

p*q=n→ 7*13=91 → n=91

$\phi(n)=(p-1)*(q-1)=6*12=72$ → $\phi(n)=72$

e*d=1 mod 72 → e=5 → 5d=1 mod 72 → $\mathbf{d_{AC1}=29}$

$FRSA_{AC2} = H_{AC2}^{dAC1} \bmod n_{AC1} = 8^{29} \bmod 91=8$ → $(8^4 \bmod 91 =1)$ → $(8^4)^7*8 \bmod 91$→ 1*8 mod 91=8 mod 91→ $\mathbf{FRSA_{AC2}=8}$

2. Verificación de la cadena de certificación

Para verificar el certificado de AC3:

Realizamos el resumen de los campos del certificado (ya realizado en el paso anterior)

$\mathbf{H_{AC3}=9}$

Ciframos con la clave pública de AC2 (5,51) la firma de AC3:

$(\mathbf{FRSA_{AC3}})^{eAC2} \bmod n_{AC2} = 42^5 \bmod 51= (-9)^5 \bmod 51=9 = \mathbf{H_{AC3}}$

El certificado de AC3 es correcto (efectivamente, está firmado por AC2)

Ahora hay que verificar si el certificado de AC2 es correcto:

Realizamos el resumen del certificado (ya realizado en el paso anterior)

$\mathbf{H_{AC2}=8}$

Ciframos con la clave pública de AC1 (5,91) la firma de AC2:

$(\mathbf{FRSA_{AC2}})^{eAC1} \bmod n_{AC1} = 8^5 \bmod 91= 8 = \mathbf{H_{AC2}}$

El certificado de AC2 es correcto (efectivamente, está firmado por AC1)

Ahora hay que verificar si el certificado de AC1 es correcto: Al ser la autoridad raíz, su certificado estará autofirmado.

Realizamos el resumen del certificado de AC1 (está en el enunciado)

H_{AC1}= 1+1+0+1+5+91=99→ 9+9=18→1+8=9

H_{AC1}=9

Ciframos con la clave pública de AC1 (5,91) la firma de AC1:

$(\mathbf{FRSA_{AC1}})^{eAC1} \bmod n_{AC1} = 34^5 \bmod 91 = 34$

34 debería ser igual a H_{AC1}, pero no lo es. El certificado es erróneo o falso y la cadena no es válida. Para que fuera correcta, habría que modificar la firma del certificado para poner la correcta:

$FRSA_{AC1} = H_{AC1}^{dAC1} \bmod n_{AC1} = 9^{29} \bmod 91 = 81$

$(9^9)^3 * 9^2 \bmod 91 \rightarrow 81$

$FRSA_{AC1} = 81 \bmod 91$

Con lo que el certificado de AC1 quedaría C_{AC1} (1,1,0,1,5,91,81)

Comprobando de nuevo la firma: $(\mathbf{FRSA_{AC1}})^{eAC1} \bmod n_{AC1} = 81^5 \bmod 91 = 9$, que en este caso si es igual a **H_{AC1}=9.**

Faltaría disponer de algún procedimiento para verificar que la clave pública de AC1, empleada para verificar el certificado autofirmado de AC1, es realmente de AC1. Por ejemplo los navegadores web traen embebidos los certificados autofirmados. Además habría que comprobar que los certificados no estuviesen revocados…

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final Convocatoria Ordinaria — Leganés – Mayo 2014

Apellidos: **Nombre:**

Grupo magistral: **Grupo reducido:**

EJERCICIO 2 (1,25 puntos)

Un inspector de policía quería resolver el asesinato de Alicia. Disponía de la interceptación de dos comunicaciones, una en claro en claro y otra cifrada (C) entre el presunto asesino y quien le contrató. La comunicación no cifrada decía: "Jefe, no nos pillarán. Cuando complete el trabajo te mandaré la primera letra del nombre de la víctima firmada y cifrada con algoritmos distintos. Primero la firmaré, con un algoritmo que proporciona firmas distintas aunque se firme el mismo texto en claro (consideraré como resumen la propia primera letra de la víctima). Luego cifraré tanto la mencionada primera letra como la firma obtenida, y te mandaré el resultado. Ya sabes dónde encontrar mis claves públicas; yo ya tengo las tuyas". El inspector sospechaba que el asesino no utilizaba estándares para cifrar y firmar, sino que aplicaba los algoritmos directamente. Además, tras el registro del domicilio del presunto asesino y del análisis forense de su ordenador encontró dos conjuntos de datos de interés:

1. N=33, e=7
2. p=17, g=7, X=5, k=9

Si la comunicación cifrada interceptada fue C={C_1, C_2 ,C_3} = {0,10,20} y el alfabeto utilizado para la codificación de los datos fue:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

¿Qué algoritmo de cifrado y qué algoritmo de firma utilizó el asesino? ¿Qué inicial se escondía tras el texto cifrado? ¿Se corresponde la comunicación cifrada interceptada con los datos encontrados en el ordenador del presunto asesino?

Solución:

¿Qué algoritmo de cifrado y qué algoritmo de firma utilizó el asesino? ¿Qué inicial se escondía tras el texto cifrado? ¿Eran los datos encontrados en el ordenador los del asesino?

En base a las comunicaciones interceptadas y al análisis forense del ordenador, se deduce que para la firma se utilizó elGamal puesto que un mismo texto en claro da lugar a distintos textos firmados, es decir, las firmas son aleatorias en base a un parámetro k. Por tanto, como se indica que son algoritmos distintos para la firma y para el cifrado y teniendo en cuenta el primer conjunto de datos proporcionados, el cifrado se realizó mediante RSA.

Lo primero a tener en cuenta es que $C = Cifrar_{RSA}(Firma_{elGamal}(M)) \rightarrow Firma_{elGamal}(M) = \{M,r,s\}$

$Descifrar_{RSA}(C) = Firmar_{elGamal}(M)$

Clave pública del jefe: e=7, N=33=p x q = 11 x 3

Clave privada del jefe: fi(33)= 20, d= 3, ed mod fi(n) =1

Descifrar (C_1) = 0^3 mod 33=0; ‘A’

Descifrar (C_2) =parámetro r de ElGamal= 10^3 mod 33=10

Descifrar (C_3)=parámetro s de ElGamal= 20^3 mod 33=14

Por tanto el mensaje descifrado es {0,10,14} y la inicial que se escondía tras el texto cifrado era la A. Ahora comprobamos si se corresponde con la firma de la inicial de Alicia A por parte del presunto asesino (utilizando los valores encontrados en el computador).

Y=7^5mod17=11

V1=11^10 x 10^14 mod 17=15 x 8mod17 =1

V2=7^0 mod17=1

Como V1=V2 se puede afirmar que el presunto asesino es `el asesino’, dado que se indica que la A de Alicia ha sido firmada con una clave privada que él poseía.

Creación del ejercicio: $C=Cifrar_{RSA}(Firmar_{elGamal}(M))=\{0, 10,20\}$

$Firmar_{elGamal}(M)$:

- H(M)= M= 0 (‘A’)
- r=7^9mod17=10
- 0=5 x r + 9 x smod16=5 x 10 + 9 x smod16 -> 14=9smod16
    - Realizando un cambio de variable z=s/14 1=9zmod16->z=9
    - S=9 x 14mod16=14
- $Firmar_{elGamal}(M)=\{r,s\}=\{0,10,14\}$
- {M,r,s}={0,10,14}

$Cifrar_{RSA}(Firmar_{elGamal}(M)$

- C1=0^7 mod 33=0
- C2=10^7 mod 33=10
- C3=14^7 mod 33=20
- C={0,10,20}