FIB

Seguretat Informàtica

Col·lecció de problemes

Cryptography

SOLUCIONS

Curs 2017-18 Q2
Marzo 2018

Jaime Delgado
Dept. AC

True/False Test questions. Indicate if the following sentences are true or false.

2. AES and DES are symmetric key encryption systems.

☐ True ☐ False

Answer: True.

3. DES and AES are examples of block-based ciphering mechanisms.

☐ True ☐ False

Answer: True.

4. It is not possible to use the DES algorithm for digital signature.

☐ True ☐ False

Answer: True.

5. In cryptography, the "confusion" principle is the one that provokes that a small change in the key achieves a big change in the ciphered text.

☐ True ☐ False

Answer: True.

6. In cryptography, the "diffusion" principle is the one that achieves that with a small change in the clear text, a big change in the ciphered text will happen (plain text vs. cipher text independence).

☐ True ☐ False

Answer: True.

7. El principio de "difusión" en criptografía es el que consigue que con un pequeño cambio en la clave haya un gran cambio en el texto cifrado.

☐ Cierto ☐ Falso

Respuesta: Falso. Es el que consigue que un pequeño cambio en el texto en claro provoque un gran cambio en el texto cifrado.

8. Diffie-Hellman allows sharing a secret key through the communication channel in a secure manner.

☐ True ☐ False

Answer: True.

9. SubBytes, ShiftRows and MixColumns are examples of permutations of the RSA algorithm for symmetric encryption.

☐ True ☐ False

Answer: False. It is for AES. RSA is asymmetric.

10. ShiftRows, MixColumns, and AddRoundKey are examples of permutations of the DES algorithm for symmetric encryption.

☐ True ☐ False

Answer: False. They are for AES.

11. In "asymmetric encryption", the recipient's private key is used to encrypt a message.

☐ True ☐ False

Answer: False. The recipient's public key is used.

12. It is not useful ciphering with symmetric key and sending that key through a public key mechanism.

☐ True ☐ False

Answer: False. Ciphering with symmetric key is more efficient, and sending the symmetric key using PKI solves the key distribution problem.

13. Una firma electrónica se genera con la clave pública del firmante.

☐ Cierto ☐ Falso

Respuesta: Falso. Con la clave privada del firmante.

14. In security, Hash algorithms are used to interchange symmetric keys.

☐ True ☐ False

Answer: False. They are used to "summarize" (without the possibility of recovering the original) the content of a message to sign.

15. En los sistemas de cifrado de clave asimétrica, la parte secreta de la clave se puede deducir de la clave pública.

☐ Cierto ☐ Falso

Respuesta: Falso.

16. En los sistemas de cifrado de clave simétrica, la parte pública de la clave va encriptada con la clave secreta.

☐ Cierto ☐ Falso

Respuesta: Falso. Los sistemas de clave simétrica no tienen clave pública.

17. No es posible encriptar con clave simétrica y después enviar la clave a través de un mecanismo de clave asimétrica.

☐ Cierto ☐ Falso

Respuesta: Falso. Se hace muy frecuentemente.

18. En RSA, el valor de la e de la clave pública ha de ser coprimo con el valor de Φ(n).

☐ Cierto ☐ Falso

Respuesta: Cierto.

19. In RSA, the secret part of the key is calculated directly from the two values of the public part, e and n.

☐ True ☐ False

Answer: False. Module n is not used, but numbers p and q are used for the calculation.

20. In the ElGamal mechanism for asymmetric encryption, the secret key *Ks* is calculated as $Ks = \alpha^{Kp}$, being *Kp* the public key, and α a known number.

☐ True ☐ False

Answer: False. It is just the contrary; i.e., $Kp = \alpha^{Ks}$.

21. In the ElGamal mechanism for asymmetric encryption, the public key *Kp* is calculated as $Kp = \alpha^{Ks}$, being *Ks* the secret key, and α a known number.

☐ True ☐ False

Answer: True.

22. In the ElGamal mechanism for asymmetric encryption, to encrypt m we should calculate $c=m*(\alpha^a)^v \bmod g$, where v is a random number chosen by the sender, which is not sent.

☐ True ☐ False

Answer: True.

PROBLEMA 1

Un usuario A quiere firmar con RSA un mensaje m de sólo un octeto: **00001110**, que envía a otro usuario B.

Los datos disponibles son:

Claves públicas de los usuarios A y B: $(e_A, n_A) = (3, 22)$ $(e_B, n_B) = (11, 35)$

Nota: En la firma RSA, $s = m^d \bmod n$; $m = s^e \bmod n$; $d = e^{-1} \bmod \Phi(n)$.

Calcular la firma que generará A.

Para calcular s necesitamos m, d y n. m será el octeto 00001110 = 14 en decimal. En este caso concreto en el que A firma con su clave secreta, necesitamos d_A y n_A. n_A vale 22, pero nos falta d_A, que es su clave secreta. La podríamos calcular si tuviésemos $\Phi(n) = (p-1)*(q-1)$, siendo p y q los factores de n. Como n (n=p*q, siendo ambos primos) es muy pequeño, podemos deducir que n=22=2*11 y, por tanto $\Phi(n) = 1*10=10$.
Por tanto, $d_A = e_A^{-1} \bmod \Phi_A(n) = 3^{-1} \bmod 10$. Y calculamos el inverso con la "magic box":

b	d	k
0	10	-
1	3	3
-3	1	

por lo que el inverso es igual a 10 – 3 = 7, y $d_A = 7 \bmod 10 = 7$.

Ahora simplemente queda aplicar la fórmula $s = m^d \bmod n$

Con los valores que tenemos:

$s = 14^7 \bmod 22 = 105413504 \bmod 22 = 20$

PROBLEMA 2

Una companyia fa servir RSA. Les claus públiques de A (Anna) i B (Bob) són:

$(e_A, n_A) = (13, 299 = 13*23)$

$(e_B, n_B) = (3, 319 = 11*29)$

Reproduir les operacions que ha de fer l'Anna per
(1) signar el missatge m=200,
(2) xifrar el resultat de la signatura i
(3) xifrar el missatge original.

També reproduir les operacions que ha de fer en Bob per desxifrar i verificar la signatura de l'Anna.

1) signar: $s = m^{dA} \bmod n_A$

Ens falta d_A ($d_A = e^{-1} \bmod \Phi(n_A)$), però tenim la factorització de n_A i podem calcular $\Phi(n) = (p-1) * (q-1) = 12 * 22 = 264$, llavors calculem amb el magic box $d_A = 61$

b	d	k
0	264	-
1	13	20
-20	4	3
61	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

$s = 200^{61} \bmod 299 = 96$

(per exemple, podem calcular la exponenciació modular a *http://ptrow.com/perl/calculator.pl*)

2) xifrar signatura: $c_s = s^{eB} \bmod n_B = 96^3 \bmod 319 = 149$

3) xifrar missatge: $c_m = m^{eB} \bmod n_B = 200^3 \bmod 319 = 118$

4) desxifrar signatura: $s = c^{dB} \bmod n_B$ com abans no tenim d_B però tenim els factors de n_B i podem calcular $\Phi(n) = (p-1)*(q-1) = 10 * 28 = 280$, llavors calculem amb el magic box $d_B = 187$

b	d	k
0	280	-
1	3	93
-93	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

Per tant, d = 280 - 93 = 187.

$s = 149^{187} \bmod 319 = 96$

5) desxifrar missatge: $m = 118^{187} \bmod 319 = 200$

6) verificar signatura $m = s^{eA} \bmod n_A \rightarrow 200 = 96^{13} \bmod 299$

PROBLEMA 3

A y B utilizan RSA para intercambiar mensajes cifrados. Sus claves públicas son:

$(e_A, n_A) = (11, 35)$

$(e_B, n_B) = (3, 22)$

C consigue averiguar, tanto para A como para B, los valores “p” y “q” con los que han obtenido “n” (han seleccionado un primo demasiado pequeño que C ha conseguido factorizar).

C intercepta un mensaje encriptado que A envía a B. En concreto, c = 14.

SE PIDE:

¿Cuál es el mensaje `m` original que se ha enviado y que C es capaz de desencriptar? Detallar todos los cálculos que C debe hacer para obtener `m`.

Nota: En RSA, $c = m^e \bmod n$, $m = c^d \bmod n$, $d = e^{-1} \bmod \Phi(n)$.

El mensaje c que C ha interceptado se habrá calculado:

$c = 20^3 \bmod 22 = 8000 \bmod 22 = 14$

Los valores p y q de A y B serán:

n = p * q; en A: n = 35 = 5 * 7; en B: n = 22 = 2 * 11

Y $\Phi(n)$:

$\Phi(n)$=(p-1)*(q-1); en A: $\Phi_A(n) = 4*6 = 24$; B: $\Phi_B(n) = 1*10 = 10$

Teniendo en cuenta que A envía a B, para calcular m tenemos:

$m = 14^{dB} \bmod 22$, por lo que debemos calcular d_B.

Aplicando la fórmula y con los valores que tenemos:

$d_B = e_B^{-1} \bmod \Phi_B(n) = 3^{-1} \bmod 10$

Y calculamos el inverso con la “magic box”:

b	d	k
0	10	-
1	3	3
-3	1	

por lo que el inverso es igual a 10 – 3 = 7, y $d_B = 7 \bmod 10 = 7$.

Y ya tenemos todos los datos para calcular m:

$m = 14^7 \bmod 22 = 105413504 \bmod 22 = 20$

PROBLEMA 4

Recibimos un mensaje encriptado c y su firma s. En concreto, nos llega c=16 y s=14. Usamos RSA.

Las claves pública y privada de nuestro interlocutor son: (e, n) = (11, 35) d = 11

Nuestras claves pública y privada son: (e, n) = (3, 22) d = 7

Nota: Ejemplo de operaciones RSA: $x = y^d \bmod n;\ y = x^e \bmod n;\ d = e^{-1} \bmod \Phi(n)$.

Calcular el mensaje m original y verificar si la firma es correcta. La función de Hash es H(m)=m.

El originador de m lo ha encriptado con nuestra clave pública y deberemos desencriptar con nuestra clave privada:

$m = c^d \bmod n;\ m = 16^7 \bmod 22 = 14.$

El originador ha firmado H(m) con su clave privada. Para verificar la firma, hemos de desencriptar s con su clave pública y ver si el resultado coincide con m:

$m = s^e \bmod n;\ s = 14^{11} \bmod 35 = 14.$

PROBLEMA 5

En un entorno RSA, queremos hacer una suplantación firmando un mensaje m=14 como si fuéramos la víctima.

La clave pública de la víctima es: (e, n) = (11, 35)

Nuestras claves pública y privada son: (e, n) = (3, 22) d = 7

Nota: Ejemplo de operaciones RSA: $x = y^d \bmod n;\ y = x^e \bmod n;\ d = e^{-1} \bmod \Phi(n)$.

Calcular la clave privada de la víctima y el resultado de la firma.

Calculamos la clave privada d de la víctima:

$n=p*q;\ 35=5*7.\ \Phi(n)=(p-1)*(q-1)=4*6=24.$

$d = e^{-1} \bmod \Phi(n) = 11^{-1} \bmod 24.$ Con magic box:

b	d	k
0	24	-
1	11	2
-2	2	5
11	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

$d = 11 \bmod 24 = 11.$

Ahora firmamos con su clave privada:

$s = m^d \bmod n;\ m = 14^{11} \bmod 35 = 14.$

EXERCISE 6

Using RSA, B sends to A the result c=11 of encrypting a message m, together with the result s=18 of signing the same message with a hash function H(m)=m/2.

The public and private keys of A and B are: $(e_A, n_A) = (11, 35)$, $d_A = 11$; $(e_B, n_B) = (3, 22)$, $d_B = 7$

Note: Examples of RSA operations: $x = y^d \bmod n;\ y = x^e \bmod n;\ d = e^{-1} \bmod \Phi(n)$.

1) **Calculate (with the information that the recipient could have) the original message m.**

B has encrypted m with the public key from A, and A must decrypt with his/her private key:

$m = c^{dA} \bmod n_A$; $m = 11^{11} \bmod 35 = 16$.

2) **Verify (with the information that the recipient could have) if the signature is correct.**

B has signed H(m) with his/her private key. To verify the signature, A needs to decrypt s with the public key from B, and check if the result coincides with H(m), i.e. if $H(m)=s^{eB} \bmod n_B$.

$s^{eB} \bmod n_B = 18^3 \bmod 22 = \mathbf{2}$.

$H(m)=m/2$, $H(16)=\mathbf{8}$.

Therefore, the signature is not correct!

PROBLEMA 7

Usando RSA, A envía a B el resultado c=5 de encriptar un mensaje m, y el resultado s=4 de firmar el mismo mensaje con una función de Hash H(m)=m/3.

Las claves pública y privada de A y B son: $(e_A, n_A) = (11, 35)$, $d_A = 11$; $(e_B, n_B) = (3, 22)$, $d_B = 7$

Nota: Ejemplo de operaciones RSA: $x = y^d \bmod n$; $y = x^e \bmod n$; $d = e^{-1} \bmod \Phi(n)$.

1) **Calcular (con los datos que pueda tener el receptor) el mensaje m original.**

A ha encriptado m con la clave pública de B, y B debe desencriptar con su clave privada:

$m = c^{dB} \bmod n_B$; $m = 5^7 \bmod 22 = 3$.

2) **Verificar (con los datos que pueda tener el receptor) si la firma es correcta.**

A ha firmado H(m) con su clave privada. Para verificar la firma, B ha de desencriptar s con la clave pública de A, y ver si el resultado coincide con H(m):

H(m) vale $H(m)=m/3$, $H(3)=1$.

Calculamos H(m) desencriptando s:

$H(m) = s^{eA} \bmod n_B$; $s = 4^{11} \bmod 35 = 9$.

Como la desencriptación de s es distinta al cálculo de H(m), la firma no es correcta!

EXERCISE 8

We encrypt using ElGamal with a generator $\alpha=3 \in Z_{31}$. The secret key of the sender is 14 and the one for the recipient is 10. To encrypt, v=2 is chosen.

Note: ElGamal expressions: Encrypt: $c = m*(\alpha^a)^v \in G$ Decrypt: $m = c*(\alpha^{va})^{-1} \in G$

If the encrypted message c=27 is received, **calculate the original message m**.

$\alpha^v = 3^2 \bmod 31 = 9$.

$m = 27 * (9^{10})^{-1} \bmod 31 = 27 * 5^{-1} \bmod 31$, ya que $9^{10} \bmod 31 = 5$

We calculate $5^{-1} \bmod 31$ with "magic box":

b	d	k
0	31	-
1	5	6
-6	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

Therefore, the result of the *magic box* is 31-6=25

$m = 27 * 25 \bmod 31 = 24$

PROBLEMA 9

Encriptamos usando ElGamal con un generador $\alpha=3 \in Z_{31}$. Nuestra clave secreta es 10. Como resultado de la encriptación, enviamos los valores c y 9.

Nota: Fórmulas ElGamal: Encriptar: $c = m*(\alpha^a)^v \in G$ Desencriptar: $m = c*(\alpha^{va})^{-1} \in G$

Calcular el mensaje encriptado c que enviamos si nuestro mensaje en claro es m=24.

$\alpha^v = 9$. Por tanto, como $3^v \bmod 31 = 9$, quiere decir que v=2.

$c= 24*(9^{10}) \bmod 31 = 24 * 5 \bmod 31 = 27$

PROBLEMA 10

Suponer que encriptamos usando ElGamal con un generador $\alpha=3 \in Z_{31}$. La clave secreta de un usuario A es a=17 y la de un usuario B es b=10. B recibe de A: $(\alpha^v, c) = (13, 5)$.

Nota: Fórmulas ElGamal: Encriptar: $c = m*(\alpha^a)^v \in G$ Desencriptar: $m = c*(\alpha^{va})^{-1} \in G$

Calcular el valor del mensaje m que A ha enviado.

$m= 5*(13^{10})^{-1} \bmod 31 = 5 * 5^{-1} \bmod 31 = 5 * 25 \bmod 31 = 1$

ya que $13^{10} \bmod 31 = 5$, y $5^{-1} \bmod 31 = 31-6 = 25$ con magic box.

b	d	k
0	31	-
1	5	6
-6	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

PROBLEMA 11

Encriptamos usando ElGamal con un generador $\alpha=2 \in Z_{31}$. La clave secreta del emisor es a=14 y la del receptor es a=9. Para encriptar se elige v=3.

Nota: Fórmulas ElGamal: Encriptar: $c = m*(\alpha^a)^v \in G$ Desencriptar: $m = c*(\alpha^{va})^{-1} \in G$

Si se recibe el mensaje encriptado c=3, **CONTESTAR RAZONADAMENTE A LAS SIGUIENTES PREGUNTAS:**

1) **¿Qué otro valor recibiremos además de c?**

   $\alpha^v = 2^3 \bmod 31 = 8$.

2) **¿Cuál es la clave pública del receptor que se habrá usado para enviar el mensaje cifrado?**

   $\alpha^a = 2^9 \bmod 31 = 16$.

3) **Calcular el mensaje original m.**

   $m= 3 * (8^9)^{-1} \bmod 31 = 3 * 4^{-1} \bmod 31$, ya que $8^9 \bmod 31 = 4$

   Calculamos $4^{-1} \bmod 31$ con "magic box":

b	d	k
0	31	-
1	4	7
-7	3	1
8	1	

$b_i = b_{i-2} - (k_{i-1} * b_{i-1})$

Por tanto el resultado del magic box es 8

$m = 3 * 8 \bmod 31 = 24$