APELLIDOS: .....

NOMBRE: ..... D.N.I.: .....

Criptografía

10 de septiembre de 2007

Ejercicio 1. Responde razonada y brevemente a las siguientes preguntas.

(a) Tras cifrar un texto mediante un criptosistema de Vigenère, el criptograma obtenido es

GNLUG UTZSK VAWOK FEGOT CCSDE GS

Sabemos que la clave tiene longitud 5 y es de la forma C-L--, y que el texto original contiene los caracteres

----- ----- -A--- ----- ---O- --

Descifra el mensaje.

(b) ¿Cuántas posibles claves hay en un cifrado afín monoalfabético de 27 caracteres?

(c) ¿Cuál o cuáles de los siguientes modos de operación de un criptosistema simétrico de cifrado por bloques puede ser considerado como un cifrado por flujo?

ECB CBC CFB OFB

(d) Dado el criptosistema RSA cuya llave pública es $(1804, 21)$, calcula la llave privada.

(e) Consideremos un sistema de firma digital DSA con parámetros $p = 233$, $q = 29$ y $g = 37$, llave pública $y = 142$ y llave privada $x = 4$. El resultado de firmar un mensaje cuyo valor resumen es $h = 20$ es el par $(r, s) = (1, 12)$, donde hemos utilizado un valor aleatorio $k = 2$. ¿Cuáles de los números anteriores es necesario conocer para verificar la validez de la firma?.

(f) ¿Qué es un protocolo de conocimiento cero?

Ejercicio 2. Una empresa tiene 5 accionistas, y la distribución de acciones en tanto por ciento es $(30, 30, 20, 10, 10)$. Diseña un protocolo de secreto compartido en el que para acceder al secreto sea necesario que los usuarios participantes posean al menos el 60 por ciento de las acciones de la empresa.

Ejercicio 3. Consideremos el siguiente criptosistema. Codificamos los caracteres mediante 5 bits, el 0 corresponde al espacio, los números del 1 al 27 son los 27 caracteres del alfabeto latino incluyendo la letra Ñ, los números del 28 al 31 son los signos de puntuación .,;: respectivamente. Este sistema nos permite convertir los caracteres a una cadena de bits y de cadena de bits a lista de caracteres.

Dada una cadena de bits utilizamos un criptosistema de cifrado por bloques consistente en realizar la suma lógica XOR bit a bit, operando en modo CBC, sobre bloques de 7 bits. La clave empleada se cifra mediante un criptosistema de ElGamal de llave pública $(131, 2, 16)$. El resultado obtenido es la pareja de números $(62, 15)$ y la cadena de caracteres JM,R,AH

Descifra el mensaje.

Examen del 10/9/2007

Ejercicio 1.-

Comparando el mensaje cifrado con la clave

CALQ-	CALQ-	CALQ-	CALQ-
GNLUG	UTZSK	VAWOK	FEGOT
-----	-----	-A---	-----

CALQ-	CA
CCSDE	GS
---O-	--

podemos obtener que el 2º elemento de la clave es A y el cuarto cambia la O por D

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

(15 saltos → 15+1 posic).

entonces la clave ocupa la posic 16. ó 0

La intuición hace el resto:

clave CALOR

mensaje: En agosto estamos de vacaciones

(hay una letra en el cifrado -el.

(d) RSA

clave pública $(1804, 21)$

$$1804 = 2^2 \cdot 11 \cdot 41$$

$$\varphi(1804) = 2 \cdot 10 \cdot 40 = \underline{800}$$

$$e \cdot d \equiv 1 \mod 800$$

$$21 \cdot d \equiv 1 \mod 800$$

$$\boxed{d = 381}$$

Ejemplo:

$$21 \cdot d = (-x) \cdot 800 + 1. \quad \text{ó bien}$$

$$800 \cdot x + 21 \cdot d = 1$$

Algoritmo de la división

$$800 = 38 \cdot 21 + 2 \qquad 2 = 800 - 38 \cdot 21$$

$$21 = 10 \cdot 2 + 1$$

Paso atrás:

$$1 = \boxed{21} - 10 \cdot \boxed{2}^{*} =$$

$$= 21 - 10\left[800 - 38 \cdot 21\right] =$$

$$= (-10)\cdot 800 + \frac{(1+380)\cdot 21}{d}$$

$\boxed{d = 381}$ solución

(e) Firma DSA (p, q, g, y) ; x privada $k = 2$ aleat.

$h = 20$ firma $(r, s) = (1, 12)$

Para la comprobación de firma se necesita:

solución $\begin{cases} \rightarrow \text{clave pública } (p, q, g, y) \\ \rightarrow \text{hash } (h) \\ \rightarrow \text{valor de la firma } (r, s) \end{cases}$

Se ejecuta

$$u = h \cdot s^{-1} \bmod q$$

$$v = r \cdot s^{-1} \bmod q$$

Comprueba:

$$(g^u y^v \bmod p) \bmod q \overset{?}{=} r$$

Ejercicio 2.-

El protocolo puede diseñarse usando el método umbral de Shamir.

↳ 6 participaciones recuperan el secreto.

ind 1	ind 2	ind 3	ind 4	ind 5
3 part.	3 part	2 part	1 part.	1 part.

Se debe tomar un polinomio de grado 5. (6 coeficientes).

Ejercicio 3.-

Cálculo de la clave de sesión

ElGamal → clave pública (131, 2, 16)

o sea, cl. priv. es $x = 4$ inmediato.

el mensaje cifrado es

$(62, 15)$
$r \quad s$

descifrado:

$$s \cdot r^{-x} = s \cdot r^{p-1-x}$$

$$15 \cdot 62^{[131-1-4]} = 15 \cdot 62^{[126]} \text{ mód } 131$$

$62^{126} \bmod 131 = 107$

$15 \cdot 107 \bmod 131 = 33 = \underline{100001}$

¡NO! 6 bits.

$7 \times 5 = 35$.

J = 01010

M = 01101

) = 11101

R = 10011

A = 00001

H = 01000

Al revés

$r = 15$
$s = 62$

$62 \cdot 15^{(131-5)} = 62 \cdot 20 = \underline{61}$

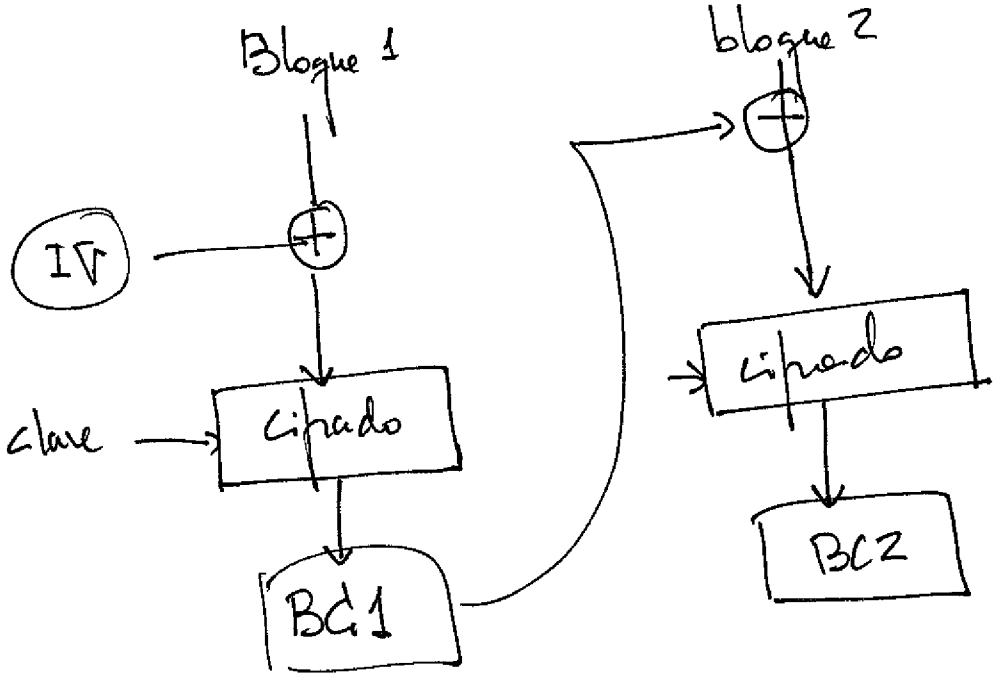
111101

6 bits

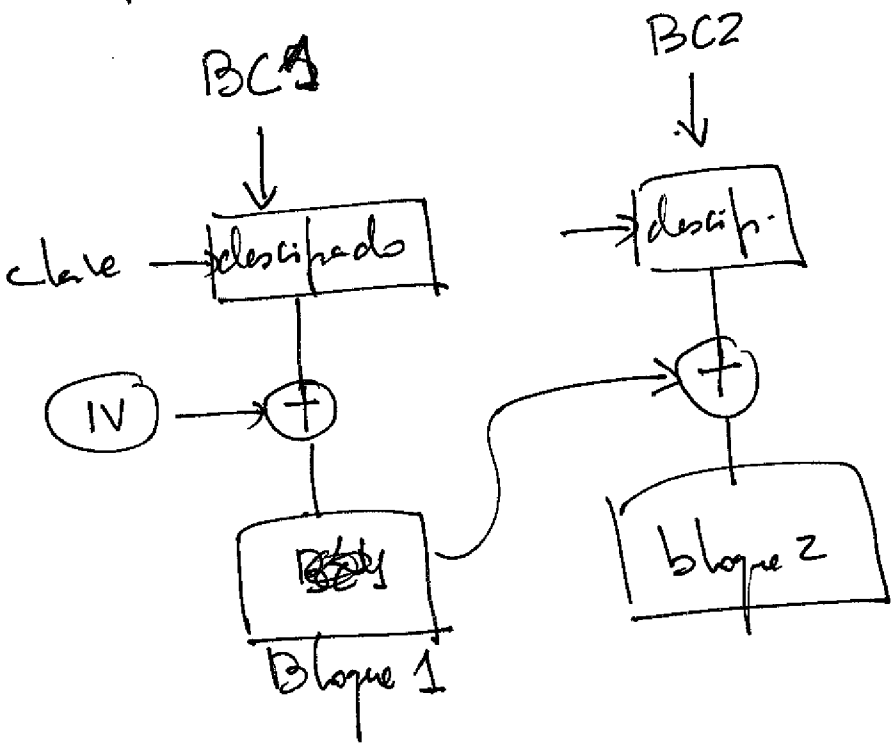
tampoco

tiene que ser ≥ 64

Modo CBC. se necesita una clave de inicialización. ??



descifrado



Criptografía

Ingeniería Informática (7- 11-2011)

SOLUCIONES

Preguntas de respuesta corta

1. De una secuencia de ceros y unos se conoce que contiene el mismo número de ceros que de unos y un número impar de rachas. Señala la afirmación **verdadera**:

   a) Cumple el primer postulado de Golomb, pero no cumple el segundo.

   b) Cumple el primer postulado de Golomb, pero no podemos afirmar nada acerca del segundo.

   c) Cumple el primer y el segundo postulado de Golomb.

   d) No se cumple el primer postulado de Golomb puesto que las cantidades de ceros y unos deben diferir en exactamente una unidad.

a)	b)	c)	d)
✓			

2. En cuanto a los modos básicos de composición de un cifrador en bloque: ECB, CBC, CFB,OFB, elegir la afirmación que es **falsa**:

   a) En modo ECB dos bloques idénticos de texto claro quedan cifrados del mismo modo.

   b) En todos los modos excepto ECB es necesario utilizar un vector de inicialización.

   c) En todos los modos el cifrador de bloque actúa sobre el bloque a cifrar o bien sobre el bloque cifrado anterior.

   d) El modo OFB puede considerarse un cifrador en flujo.

a)	b)	c)	d)
		✓	

3. Para el cifrado con DES escribir las salidas correspondientes por las S-cajas que se señalan:

   a) La salida por la S-caja número 1 (S_1) de la entrada 011010.

1	0	0	1

   b) La salida por la S-caja número 3 (S_3) de la entrada 100101.

1	1	0	1

4. Señala la respuesta **verdadera**:

   a) AES es una red de Feistel de 10 rondas.

   b) AES sólo puede operar sobre bloques de 128 bits.

   c) AES realiza transformaciones sobre cada byte y sobre las filas y las columnas de la matriz de estado.

d) Todas las rondas de AES son idénticas, sólo cambia la clave de ronda que se utiliza.

a)	b)	c)	d)
		✓	

5. Elige la respuesta **correcta** sobre el resultado de aplicar Miller-Rabin al número 561.

   a) Para $a = 103$ como $a^{35} = 1$, pasa el test, así que es primo.

   b) Como para $a = 103$ se tiene $a^{35} = 1$ no pasa el test, así que podemos asegurar que no es primo.

   c) Como para $a = 103$ se tiene $a^{35} = 1$ pasa el test, así que tendríamos que es probable primo.

   d) La base $a = 103$ debe descartarse para la realización del test, puesto que $a^{35} = 1$.

a)	b)	c)	d)
		✓	

6. Una tarjeta inteligente trata de identificarse ante un lector utilizando el protocolo de conocimiento cero de Fiat-Shamir con parámetro $n = 1313$. La tarjeta proporciona el número de identificación $ID = 1212$ y envía como testigo $r^2 = (91)^2 = 403 = t$ módulo n. Elegir la respuesta **falsa**:

   a) La tarjeta superará la prueba de identificación con el testigo anterior si el lector le envía como reto el bit 0.

   b) La tarjeta no superará la prueba de identificación con el testigo anterior si el lector le envía como reto el bit 1.

   c) La tarjeta puede superar un reto aún siendo falsa, pero es improbable que supere un número elevado de retos.

   d) La tarjeta superará el reto con el testigo anterior en cualquier caso, puesto que conoce r.

a)	b)	c)	d)
			✓

7. El resultado de la operación $(A3 \times 21) \oplus 32$ en AES es

36

8. Empareja cada protocolo con el problema inabordable computacionalmente en el que se basa

   a) Diffie-Hellman de intercambio de claves.

   b) cifrado RSA.

   c) Cifrado ElGamal.

   d) Protocolo de conocimiento cero de Fiat-Shamir.

   FP Factorización de números grandes en primos.

   LD Cálculo del logaritmo discreto.

   RD Cálculo de raices cuadradas modulares.

a)	b)	c)	d)
LD	FP-LP	LD	RD

Ejercicios

9. El mensaje

01000 00110 01011 01010 10000 00001 00001 11010 11001 00000

ha sido cifrado mediante un cuaderno de uso único usando la secuencia cifrante que se obtiene como salida del LFSR con polinomio $D(x) = x^5 + x^3 + 1$ y semilla $s_0 = 0$, $s_1 = 1$, $s_2 = 0$, $s_3 = 1$, $s_4 = 1$.

a) Calcula el periodo de la secuencia que genera el LFSR.

b) ¿Es el polinomio dado irreducible? (la respuesta está en los apuntes, pero también puede comprobarse sin consultarlos) ¿Es primitivo? (la respuesta no está en los apuntes explícitamente).

c) Descifra el mensaje. Puedes encontrar su traducción al alfabeto latino usando la tabla del código utilizado que se adjunta al examen, es una locución en latín.

Solución

a) Para calcular la secuencia se considera la fórmula

$$s_5 = a_5 s_0 + a_4 s_1 + a_3 s_2 + a_2 s_3 + a_1 s_4$$

y como $6a_5 = 1$ (coeficiente de grado 5), $a_4 = 0$ (coeficiente de grado 4), $a_3 = 1$ (coeficiente

de grado 3), $a_2 = 0$ (coeficiente de grado 2), $a_1 = 0$ (coeficiente de grado 1), queda

s_0	s_1	s_2	s_3	s_4	s_5
0	1	0	1	1	0
1	0	1	1	0	0
0	1	1	0	0	1
1	1	0	0	1	1
1	0	0	1	1	1
0	0	1	1	1	1
0	1	1	1	1	1
1	1	1	1	1	0
1	1	1	1	0	0
1	1	1	0	0	0
1	1	0	0	0	1
1	0	0	0	1	1
0	0	0	1	1	0
0	0	1	1	0	1
0	1	1	0	1	1
1	1	0	1	1	1
1	0	1	1	1	0
0	1	1	1	0	1
1	1	1	0	1	0
1	1	0	1	0	1
1	0	1	0	1	0
0	1	0	1	0	0
1	0	1	0	0	0
0	1	0	0	0	0
1	0	0	0	0	1
0	0	0	0	1	0
0	0	0	1	0	0
0	0	1	0	0	1
0	1	0	0	1	0
1	0	0	1	0	1
0	0	1	0	1	1
0	1	0	1	1	0

como la semilla ha vuelto a aparecer, ya se ha completado un periodo, que tiene longitud 31.

b) El periodo no depende de la semilla (todas las semillas posibles están en la tabla, y generarían el mismo periodo) y además es máximo: 2^5-1 así que el polinomio es irreducible y primitivo.

c) Haciendo un XOR con la secuencia generada (y repitiendo el periodo la longitud necesaria), aparece el mensaje **CARPE_DIEM**

10. Alice quiere enviar un mensaje a Bob y utiliza un doble sistema de seguridad basado en sus respectivos criptosistemas RSA. En primer lugar cifra el mensaje para que sólo Bob pueda leerlo, para ello usa las claves públicas de Bob: $(n_B = 3431, e_B = 17)$. Además, firma el resultado para que su interlocutor esté completamente seguro de que es ella quien lo ha enviado. Sabiendo que la clave pública de Alice es $(n_A = 3589, e_A = 5)$ y que Bob recibe 468, calcula el mensaje que Alice ha enviado. **Observación:** es probable que necesites romper el/los criptosistemas, como ayuda la descomposición en primos de los módulos es:

$$n_A = 3589 = 37 \cdot 97;\ n_B = 3431 = 47 \cdot 73$$

Solución

El proceso que ha seguido Alice es

$$m \rightarrow_{\text{cifrado\_cpubBob}} c_1 \rightarrow_{\text{cifrado\_cprivAlice}} c$$

Así que tendremos que deshacer este procedimiento mediante

$$c \rightarrow_{\text{cifrado\_cpubAlice}} c_1 \rightarrow_{\text{cifrado\_cprivBob}} m$$

Puesto que necesitamos calcular la clave privada de Bob, usamos la información dada para calcular $\phi(n_B) = (47-1)(73-1) = 3312$.

La clave privada de Bob satisface la ecuación

$$e_B d_B \equiv 1 (\mathrm{mod}\, \phi(n_B))$$

que puede resolverse usando el algoritmo de Euclides extendido y se obtiene $d_B = 1169$.

El procedimiento de calcular una potencia modular puede llevarse a cabo usando el algoritmo de potenciación rápida que solo requiere el cálculo del producto de dos números de la magnitud del módulo.

Quedaría:

$$468 \rightarrow_{\text{cifrado\_cpubAlice}} 468^5 = 3036 (\mathrm{mod}\, 3589) \rightarrow_{\text{cifrado\_cprivBob}} 3036^{1169} = 1001 (\mathrm{mod}\, 3431)$$

Solución: 1001

Puntuación: cada pregunta de respuesta corta 0,7 puntos (sin puntuaciones intermedias); cada problema 2,2 puntos.