Criptografía

28 / 06 / 2013

Alumno:_____ **DNI:**_____

Ingeniería Informática

Ejercicio 1.
Contesta razonadamente a las siguientes cuestiones:

1. Descifra el siguiente criptograma

   ukcñu ñmmry wñczk xyukn ñoedl yuñcu kmkvz ñywñn ññeby zkinñ uvewn y

   que ha sido cifrado usando un criptosistema clásico.

2. Un criptosistema contiene cuatro posibles mensajes en claro $\{m_0, m_1, m_2, m_3\}$ y todos ellos aparecen con la misma probabilidad. Contiene también cuatro posibles claves $\{k_0, k_1, k_2, k_3\}$ y seis posibles mensajes cifrados $\{c_0, c_1, c_2, c_3, c_4, c_5\}$. La función de cifrado, para una clave k_i es $E_{k_i}(m_j) = c_l$, donde $l = (i + j)$ mód 6. ¿Cuál es la cantidad de información que contiene, en media, un criptograma, sobre el mensaje claro?

3. Para generar una clave en un cifrado en flujo, vamos a utilizar dos LFSR de tres y cuatro celdas respectivamente, cuyos polinomios característicos son $x^3 + x + 1$ y $x^4 + x + 1$, y las semillas 110 y 1011. Luego, las dos salidas se conectan a una puerta XOR, y así se obtiene la secuencia clave. ¿Es periódica esta secuencia?. En caso afirmativo, indica la longitud del periodo.

4. En el cifrado DES, antes de realizar la S-transformación tenemos los 48 bits siguientes:

   001010 101011 101010 001011 110011 000110 110010 001010

   ¿Cuál es el resultado de la transformación?

5. ¿Podría ser $(1073, 5)$ la clave pública de un criptosistema RSA? En caso afirmativo, ¿cuántos mensajes no cifrables existen?.

6. Una empresa tiene cinco accionistas. Hay dos accionistas que poseen el 10 % de las acciones cada uno, otros dos que poseen el 30 % cada uno y el que queda posee el 20 %. Diseña un protocolo de secreto compartido en el que para tener acceso al secreto, los usuarios participantes deban poseer, al menos, el 60 % de las acciones.

Ejercicio 2.
La clave pública de un criptosistema ElGamal es $(113, 3, 17)$.
El mensaje $(105, 87)$ ha sido cifrado con dicho criptosistema.
Descifra el mensaje.

Ejercicio 3.
Definimos la siguiente función resumen. Para esto, sea m un mensaje formado por n bits.
Si $n = 1$, añadimos un 1 a la derecha, y vamos al paso siguiente.
Si $n < 4$, añadimos a la derecha la suma (XOR) de los dos últimos bits. Este proceso lo repetimos hasta que tengamos 4 bits.
Si $n = 4$ lo dejamos tal cual.

Si $n \geq 5$, sumamos los dos primeros bits. El resultado lo colocamos al final, y los dos bits que hemos sumado, los eliminamos. De esta forma, hemos reducido en 1 el tamaño de la sucesión. Este proceso lo repetimos hasta que nos queden 4 bits.

Sean ahora $p = 103$, $q = 17$, $\alpha = 72$ e $y = 8$.

- Comprueba que los parámetros (p, q, α, y) pueden ser los parámetros públicos necesarios para un sistema de firma DSS (salvo en lo referente al tamaño de los números primos), y calcula el parámetro x (privado).
- Firma el mensaje 10110101110101011011 (Nota: puesto que el resumen del mensaje tiene 4 bits, podemos verlo como un número comprendido entre 0 y 15).
- Sea el mensaje 10101. Comprueba si $(0, 14)$ es una firma válida.

Ejercicio 4. Juan y Miguel han acordado usar el siguiente sistema de cifrado por bloques.

El sistema trabaja con bloques de 5 bits (o lo que es lo mismo, números comprendidos entre 0 y 31). La función de cifrado es $E_{a,b}(m) = a \cdot m + b$, donde $a, b \in \mathbb{Z}_{32}$ (en este caso, el par (a, b) sería la clave).

Para representar los mensajes, utilizan la siguiente codificación. Las 27 letras del alfabeto las representan como los números del 1 al 27, siguiendo el orden natural, el espacio lo representan como 0, y los números 28,29,30,31 los utilizan para los signos de puntuación *coma*, *punto*, *punto y coma*, *dos puntos* respectivamente. De esta forma, cada uno de los símbolos es representado como una cadena de 5 bits.

Juan va a enviar un mensaje a Miguel. Para ello, elige una clave de sesión (a, b) y la cifra usando la clave pública de Miguel (Miguel tiene un criptosistema RSA cuya clave pública es $(85, 43)$). El resultado de cifrar la clave de sesión es $(46, 81)$.

Una vez establecida la clave de sesión, Juan agrupa el mensaje en bloques de cinco bits, y los cifra, operando en modo CBC. El vector de inicialización es 11111.

El mensaje recibido por Miguel es `ih;d uuv`

Descifra el mensaje.

Criptografía

10 / 09 / 2012

Alumno:_____ **DNI:**_____

Ingeniería Informática

Ejercicio 1.
Contesta razonadamente a las siguientes cuestiones:

1. El siguiente texto

   LMBAXRU APAWECH NFZHWEÑ UYPÑXRV O

   Se ha obtenido después de cifrar una frase usando el criptosistema de Vigenère, con una clave de 7 caracteres.

   Sabemos que la primera letra de la clave es una A, y la última, una D. Además, se conocen cuales son los caracteres del texto plano que van en las posiciones que son múltiplos de 6, y son RLOI repectivamente.

   Descifra la frase original.

2. De un número n queremos saber si es o no primo. Para eso, aplicamos el test de Miller-Rabin. Tomamos $a = 125$, realizamos una serie de cálculos (módulo n) y obtenemos los siguientes resultados:

   $$a^{41} = 2478; \quad a^{82} = 4403; \quad a^{164} = 1852; \quad a^{328} = 2307; \quad a^{656} = 5012; \quad a^{1312} = 3679; \quad a^{2624} = 3119.$$

   Suponiendo que hemos aplicado el test correctamente, ¿podrías decir quien es n, y la conclusión a la que llegamos sobre él?

3. Una variable puede toma cuatro vales, A, B, C y D. La probabilidad de que tome el valor A es $\frac{1}{8}$, la misma que de que tome el valor B, y la probabilidad de que tome el valor C es $\frac{1}{4}$.

   Para representar esta variable, utilizamos el siguiente código binario: $A \mapsto 01$, $B \mapsto 10$, $C \mapsto 0$, $D \mapsto 1$.

   Calcula la entropía de esta variable y estudia si este código es un buen código para representarlo. Caso de no serlo, diseña un código instantáneo óptimo y halla el número medio de bits necesarios para representar cada uno de los datos de esta variable.

4. Tenemos un LFSR de 7 celdas, y con polinomio generador $x^7 + x^5 + x^2 + x + 1$ (que es irreducible) y semilla 1011010. ¿Qué podemos decir del periodo de la secuencia que genera?

5. Intentamos un ataque por fuerza bruta de un mensaje cifrado con AES, con una clave de 128 bits. Supongamos que somos capaces de analizar un billón de claves por segundo, y que necesitamos explorar únicamente una octava parte del espacio total de claves. ¿Podrías dar una estimación del tiempo necesario para descifrar el mensaje?

6. La cuarta clave de ronda de un sistema de cifrado AES de 128 bits es

2A	54	04	F2
87	19	37	BB
D2	1E	46	90
35	C6	71	22

   Calcula la quinta clave de ronda.

7. Formas parte de un grupo de 35 personas. Indica qué es más probable: que en esas 35 personas haya dos que hayan nacido el mismo día del año (aunque posiblemente en años diferentes), o que no se encuentren esas dos personas.

   Indica también si es más probable que haya alguien que celebre el cumpleaños el mismo día que tú, o que no lo haya.

   ¿Cómo se conoce este hecho?

Ejercicio 2.

Un mensaje se ha cifrado con un LFSR de 4 celdas. El mensaje cifrado es 10000 00101 01000 11000 11001 0(
Para cifrarlo, se ha usado la siguiente codificación:

–	00000	H	01000	O	10000	W	11000
A	00001	I	01001	P	10001	X	11001
B	00010	J	01010	Q	10010	Y	11010
C	00011	K	01011	R	10011	Z	11011
D	00100	L	01100	S	10100	,	11100
E	00101	M	01101	T	10101	.	11101
F	00110	N	01110	U	10110	;	11110
G	00111	Ñ	01111	V	10111	:	11111

Sabemos que los dos caracteres centrales del mensaje son AM.

Descifra el mensaje.

Ejercicio 3.

Una empresa tiene en su plantilla diez trabajadores divididos en dos grupos. El primero, con 4 trabajadores y el segundo con los seis restantes. Una información, que representaremos mediante el número $s = 25$, deseamos repartírsela a los trabajadores, de forma que sólo puedan acceder a ella si se ponen de acuerdo, bien dos trabajadores del primer grupo, bien cuatro trabajadores del segundo, bien un trabajador del primero con dos del segundo.

Diseña un protocolo de secreto compartido para guardar esta información, y explica la participación que darías a cada uno de los trabajadores.

Ejercicio 4.

Definimos la siguiente función resumen:

> Tomamos una cadena de bits. Si la longitud no es múltiplo de 4, añadimos los unos necesarios al final para que la longitud sea múltiplo de 4.
>
> Una vez hecho esto, seleccionamos los 8 bits más a la izquierda, lo que nos da un número comprendido entre 0 y 255. Lo multiplicamos por 3 (módulo 256), y del resultado (en binario) nos quedamos con los bits que ocupan posición impar (empezando a contar por la izquierda). De esta forma, hemos reducido el tamaño de la cadena en cuatro unidades.
>
> Con la cadena resultante repetimos el proceso hasta quedarnos con una cadena de 4 bits, es decir, un número comprendido entre 0 y 15.

Supongamos que Roberto quiere enviar a María cierta información m. Para ello, hace uso del criptosistema que tiene María. Este es un sistema de cifrado RSA de clave pública $(187, 107)$. Y firma el resumen del mensaje m (obtenido con la función descrita anteriormente). Para ello emplea un sistema de firma DSS de parámetros $p = 191$, $q = 19$, $\alpha = 69$ e $y = 136$.

Roberto envía a María el mensaje cifrado, y la firma.

María recibe $(152, (12, 17))$. Es decir, el mensaje cifrado y la firma.

Descifra el mensaje recibido por María y comprueba si la firma es válida.

Criptografía

15 / 06 / 2012

Alumno:_____ **DNI:**_____

Ingeniería Informática

Ejercicio 1.
Contesta razonadamente a las siguientes cuestiones:

1. Ciframos el Quijote siguiendo un criptosistema de Vigènere con clave AIFARGOTPIRC (antes de eso, hemos eliminado los espacios, signos de puntuación, etc.). Cada carácter del texto cifrado ocupa una posición en el texto que denotaremos por n (empezamos por 1). De todo el texto, elegimos:

   - Aquellos que ocupan una posición n tal que $n \equiv 3$ (mód 12).
   - Aquellos que ocupan una posición n tal que $n \equiv 2$ (mód 6).
   - Aquellos que ocupan una posición n tal que $n \equiv 1$ (mód 3).
   - Aquellos que ocupan una posición n tal que $n \equiv 5$ (mód 24).
   - Aquellos que ocupan una posición n tal que $n \equiv 5$ (mód 6).

   Indica en cada caso si el índice de coincidencia del texto seleccionado es mayor o menor que 0'06.

2. A continuación se indican los resultados obtenidos después de aplicar el test de Miller-Rabin a varios números. En cada caso, explica que conclusión podemos sacar de estos resultados.

   - Probamos con $n = 1729$.
     Elegimos $a = 5522$, y nos da $a^{27} = 1728$; Si elegimos $a = 5476$, nos da $a^{27} = 1$.
   - Probamos otra vez con $n = 1729$.
     Elegimos $a = 69$, y nos da $a^{27} = 1728$; elegimos $a = 201$ y nos da $a^{27} = 1217$, $a^{54} = 1065$, $a^{108} = 1$.
   - Probamos con $n = 6601$.
     Elegimos $a = 100$, y nos da $a^{825} = 1$. Elegimos $a = 65$ y nos da $a^{825} = 1954$, $a^{1650} = 2738$, $a^{3300} = 4509$.

3. Tenemos un dado irregular, de forma que la probabilidad de que salga 1 es $\frac{1}{20}$. La probabilidad de que salga 2 y de que salga 3 es $\frac{1}{10}$. La probabilidad de que salga 4 es $\frac{1}{5}$, la misma que de que salga 5. Y la probabilidad de que salga 6 es $\frac{7}{20}$.

   Sea X la variable que representa los resultados del lanzamiento del dado. Calcula la entropía de la variable X y diseña, usando el algoritmo de Hufman, un código instantáneo óptimo. Halla el número medio de bits necesarios para representar cada uno de los datos de la variable X.

4. ¿En que medida afecta a la seguridad de la función SHA1 el que se encuentren colisiones? ¿Piensas que esto comprometería seriamente su uso? Razona la respuesta.

5. En el cuerpo AES realiza los siguientes cálculos:

   AB^{-1}; $25 \cdot C1$; $37 + 2A$; $37 \oplus 2A$.

6. Dispones de un criptosistema ElGammal de clave pública (p, α, y) y clave privada x. Sea m un mensaje (sin cifrar), y h su resumen. Sea (r, s) el resultado de firmar h, siguiendo el sistema de firma ElGammal.

   Si envías el mensaje m, junto con la firma (r, s), explica:

- Cómo puede el receptor comprobar que la firma es válida.
- Porqué puede el receptor estar seguro que el mensaje ha sido enviado por quien dice ser (tú en este caso).
- Porqué puede el receptor estar seguro de que nadie ha modificado el mensaje que has enviado.
- Porqué tú no puedes negar que has sido tú quien ha enviado dicho mensaje firmado.

7. Dado el criptosistema RSA de clave pública $(91, 11)$, calcula la clave privada.

   ¿Cuántos exponentes de descifrado existen? Calcúlalos.

Ejercicio 2.

Consideramos el siguiente sistema de cifrado en bloque:

El criptosistema trabaja con bloques de seis bits. Para cifrar un bloque, se expresa en decimal el correspondiente número binario, se multiplica por 13, y se reduce módulo 64. El resultado, se expresa como un número binario con 6 cifras.

Tenemos ahora un mensaje m, y usamos el criptosistema descrito para cifrarlo, operando según el modo CBC, con vector de inicialización 000000.

El mensaje cifrado es 010101 101001 000001 111111 010010 (donde lo hemos separado en bloques de 6 para facilitar su lectura).

1. Descifra el mensaje.

   Para descifrar el mensaje, ten en cuenta que el espacio lo representamos como 00000, las letras desde la A a la Z como los números del 1 al 27 en binario (y con cinco cifras), mientras que los signos de puntuación . , : ; los representamos como los números 28, 29, 30 y 31 respectivamente.

   Le aplicamos ahora la siguiente función resumen.

   Agrupamos el mensaje en bloques de 6. A cada bloque le aplicamos la S caja 5 del DES (si hubiera bits sobrantes, se dejan como están para la siguiente ronda). A la cadena resultante, le aplicamos lo mismo. Así hasta que nos quede una cadena de 4 bits (si llegáramos a una cadena de 5 bits, le añadimos el bit 0 a la izquierda, y continuamos).

   Por ejemplo, si tenemos el mensaje 10110101, agrupamos en un bloque de 6 bits (101101) y dos bits sobrantes (01). Después de aplicar la S-caja 5 al bloque 101101 nos queda 0111. Por tanto, la cadena resultante después de la primera ronda es 011101, que es un bloque de 6 bits. Le aplicamos la S-caja 5, y el resultado es 1000. Este es el resumen.

2. Calcula el resumen del mensaje obtenido en el apartado anterior.

   Firmamos el resumen con un criptosistema ElGammal de clave pública $(p = 19, \alpha = 2, y = 17)$.

3. Comprueba si la firma $(13, 13)$ es válida.

Ejercicio 3.

01100110101111011111011101000011 es la información con las 10 cifras del número de cuenta que Eva te ha enviado. Esa información ha sido cifrada usando un LFSR, cuya semilla y cuyo polinomio generador han sido cifrados con tu criptosistema RSA, cuya clave pública es $(77381, 30725)$. La semilla (cifrada) es 40276, mientras que el polinomio (cifrado) es 50461.

Determina el número de cuenta que te ha sido enviado.

Algunas consideraciones.

1. La semilla es un número en binario. Lo que se ha cifrado es en realidad ese número (en decimal), y el resultado es el que se te indica (40276).
2. Para el polinomio, lo que se ha cifrado es el resultado de evaluar el polinomio en $x = 2$. Por ejemplo, si el polinomio fuera $x^3 + x^2 + 1$, al evaluarlo en $x = 2$ nos queda 13, que es el número que se ha cifrado. Observa como la expresión binaria de 13 es 1101, que se corresponde con los coeficientes del polinomio.
3. Tu clave RSA la ha distribuido Jesús, así que si necesitas conocer tu clave privada, él puede facilitarla. Esto lo hará de forma trascordada, siguiendo el protocolo de Rabin. Puedes intercambiar información con él, siguiendo este protocolo, cuantas veces sea necesario.

Criptografía

Ingeniería Informática (1- 09-2011)

Alumno:_____ **D.N.I.:**_____

Preguntas de respuesta corta

1. Para un NLFSR de 8 celdas, el periodo de la secuencia que genera

   a) es $2^8 - 1$.

   b) es 2^8.

   c) es un divisor de $2^8 - 1$.

   d) no puede determinarse previamente.

a)	b)	c)	d)

2. La secuencia de periodo:

   0011010101100011010110

   a) Tiene 15 rachas, 9 de longitud 1, 5 de longitud 2 y 1 de longitud 3, por lo que no cumple el segundo postulado de Golomb.

   b) Tiene 14 rachas, 8 de longitud 1, 4 de longitud 2 y 2 de longitud 3, así que cumple el segundo postulado de Golomb.

   c) No puede cumplir simultáneamente el primer y el segundo postulado de Golomb puesto que las cantidades de ceros y unos deben diferir en exactamente una unidad.

   d) No cumple el primer postulado de Golomb.

a)	b)	c)	d)

3. Señala la frase **falsa**.

   a) DES es una red de Feistel.

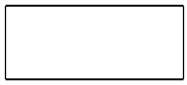
   b) DES es seguro con cualquier clave inicial.

   c) La entrada de una S-caja de DES es un subbloque de 6 bits y la salida son 4 bits.

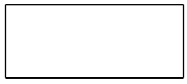
   d) TDES (TripleDES) tiene una clave de longitud doble a la de DES, pero es 3 veces más lento.

a)	b)	c)	d)

4. Para un criptosistema RSA con parámetros $(p = 61, q = 113)$ (y $n = 6893$) una clave privada pareja con la clave pública $d = 11$ es



5. En el cuerpo de AES el resultado de la operación $(B3 \times 07) \oplus A1$ es



6. Elige la frase **verdadera**.

   a) Si existen dos mensajes que producen el mismo resumen para una determinada función hash debemos despreciar esta función por insegura.

   b) Es imposible que una buena función hash obtenga el mismo resumen para dos mensajes distintos.

   c) Independientemente de la función hash que utilicemos siempre existen mensajes que tienen el mismo resumen.

   d) Si dos mensajes tienen la misma longitud es más probable que los resúmenes sean muy parecidos.

7. 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)

8. En un protocolo de secreto compartido utilizando el método umbral de Shamir, en el que se ha elegido un polinomio de grado 5 sobre $\mathbb{Z}_{53}$

   a) No pueden repartirse más de 5 porciones de secreto.

   b) Es posible recuperar el secreto con 5 porciones.

   c) Para recuperar el secreto son necesarias al menos 6 porciones.

   d) Pueden repartirse tantas porciones de secreto distintas como se desee.

a)	b)	c)	d)

Problemas

1. Desarrolla el test de Miller-Rabin para determinar si el número 6313 es primo con probabilidad mayor o igual que $0,98$.

2. El mensaje

   11011 10000 00000 01001 11011 10000 11010 10000 00001 01100 10011 00101 10100

   ha sido cifrado mediante un cuaderno de uso único usando la secuencia cifrante que se obtiene como salida del LFSR con polinomio $D(x) = x^4+x^3+1$ y semilla $s_0 = 1$, $s_1 = 1$, $s_2 = 0$, $s_3 = 1$. Descifra el mensaje. Puedes encontrar su traducción al alfabeto latino usando la tabla del código utilizado que se adjunta al examen; se trata del nombre de un escritor granadino.

3. La clave pública para un criptosistema ElGammal es $(p = 887, \alpha = 17, y = 67)$. Cifra el mensaje $m = 555$.

Puntuación: cada pregunta de respuesta corta 0,5 puntos (sin puntuaciones intermedias); cada problema 2 puntos.

Criptografía

Ingeniería Informática (7- 11-2011)

Alumno:_____ **D.N.I.:**_____

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.

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

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

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)

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.

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:

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

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

Criptografía

Ingeniería Informática (29- 06-2010)

Alumno:_____ **D.N.I.:**_____

Preguntas de respuesta corta

1. Para un LFSR de 5 celdas con polinomio $D(x) = x^5 + x + 1$ que es irreducible pero no primitivo, ¿cúal es el periodo de la secuencia que genera?

2. Cuenta el número de rachas y decide si verifica el segundo postulado de Golomb la secuencia de periodo:

$$00110101011000110101 10$$

3. Para un criptosistema RSA con parámetros $(p = 61, q = 113)$ (y $n = 6893$) determina una clave privada pareja con la clave pública $d = 11$.

4. En el cuerpo de AES calcula el resultado de la operación $(B3 \times 07) \oplus A1$.

5. En el protocolo de Diffie-Hellman hay quien dice que las operaciones se hacen en el cuerpo $\mathbb{Z}_n$, siendo n el módulo de la clave pública. ¿Es cierto?

Problemas

6. En un protocolo de secreto compartido (utilizando el método umbral de Shamir) se utiliza el cuerpo $\mathbb{F}_{53}$ ($\mathbb{Z}_{53}$) y se distribuyen las porciones de secreto:

$$(3,9)$$
$$(7,-1)$$
$$(8,28)$$
$$(11,21)$$

   Calcula el secreto original y determina el número mínimo de porciones necesarias para reconstruirlo.

7. Utiliza el test de Miller-Rabin para determinar si el número 6313 es primo con probabilidad mayor o igual que $0,98$.

8. El mensaje

$$11011\ 10000\ 00000\ 01001\ 11011\ 10000\ 11010\ 10000\ 00001\ 01100\ 10011\ 00101\ 10100$$

   ha sido cifrado mediante un cuaderno de uso único usando la secuencia cifrante que se obtiene como salida del LFSR con polinomio $D(x) = x^4 + x^3 + 1$ y semilla $s_0 = 1$, $s_1 = 1$, $s_2 = 0$, $s_3 = 1$. Descifra el mensaje. Puedes encontrar su traducción al alfabeto latino usando la tabla del código utilizado que se adjunta al examen; se trata del nombre del autor de la novela "El viajero del siglo".

9. La clave pública para un criptosistema ElGammal es $(p = 887,\ \alpha = 17,\ y = 67)$. Cifra el mensaje $m = 555$.

Puntuación: cada pregunta de respuesta corta 0,4 puntos (sin puntuaciones intermedias); cada problema 2 puntos.

Criptografía

Ingeniería Informática (22- 06-2009)

Alumno:_____ **D.N.I.:**_____

Preguntas de respuesta corta

1. Para un LFSR de 10 celdas con polinomio $D(x) = X^{10} + x^3 + 1$ que es irreducible y primitivo, ¿cúal es el periodo de la secuencia que genera?

2. Calcula la salida por la primera S-caja de DES de la entrada 111001.

3. Para el criptosistema ElGamal de clave pública $(p = 47, \alpha = 2, y = 32)$ ¿Hay más de una clave privada posible?

4. En el cuerpo de AES calcula el resultado de la operación $(A3 \times 70) \oplus 31$.

5. Comprueba si el número $n = 217$ pasa el test de Miller-Rabin para $a = 3$.

Problemas

6. Descifra el siguiente criptograma

   HAQSC HMIQM CEESS ZACUT HAEZU ECSCE F_YOE AOCFY EAIOO RE_US
   DMDEE ESLOB MML_N AIUER LSEEN ROAI_

   Pista 1 Se trata del primer párrafo de un libro titulado "La naturaleza de la felicidad".

   Pista 2 Observa que hay espacios en blanco en algunos bloques de 5 letras, que se han incluido para facilitar el trabajo.

   Pista 3 Javier Molina comió conmigo el lunes pasado.

7. La clave pública de mi criptosistema RSA es $(43289, 17)$. El mensaje que he firmado con este criptosistema es $c = 9072$, léelo y tendrás una pista más sobre el texto a descifrar en el primer criptograma.

8. El mensaje

   01101 11011 00001 00111 00101 00100 10001 01010 11000 11010 00110 11001 11100 11110

   ha sido cifrado mediante un cifrado en flujo usando la secuencia cifrante que se obtiene como salida del NLFSR que se muestra en la Figura 1; la semilla utilizada para la generación de secuencia ha sido 01001 ($c_0 = 0, c_1 = 1, c_2 = 0, c_3 = 0, c_4 = 1$). Descifra el mensaje. Puedes encontrar su traducción al alfabeto latino usando la tabla del código utilizado que se adjunta al examen; se trata del nombre del autor del texto cifrado en el ejercicio 6.

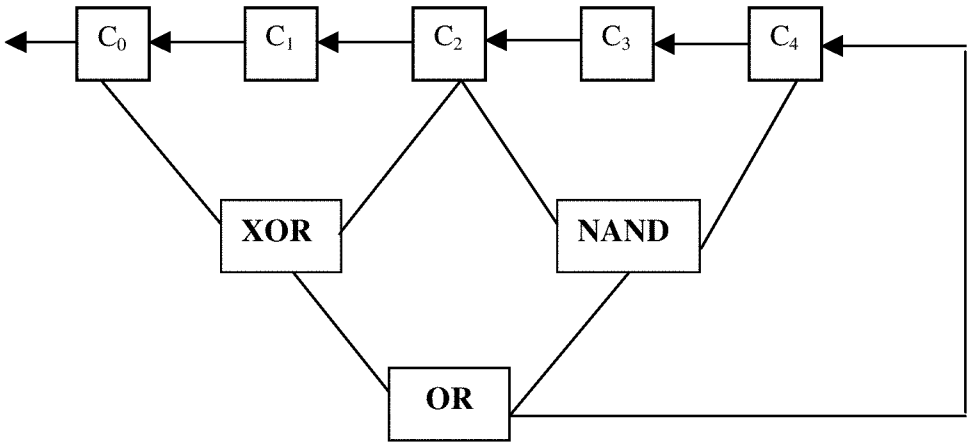


Figura 1: Esquema del NLFSR

9. El mensaje

0000000
1101111
1000001
1110111
0000110
0110010
1011111
1001101
1100010
1100011

ha sido cifrado con un cifrado en bloque de longitud de bloque 7, con función de cifrado $D(B) = B \oplus K$, es decir, XOR bit a bit, donde B es un bloque y $K = 0110101$ es la clave de cifrado. Este cifrado en bloque se ha montado en modo CBC, utilizando como vector de inicialización $IV = 0100101$. Descífralo.

Puntuación: cada pregunta de respuesta corta 0,4 puntos (sin puntuaciones intermedias); cada problema 2 puntos.

Criptografía

Ingeniería Informática (15- 09-2008)

Alumno:_____ **D.N.I.:**_____

Preguntas tipo test:

1. Un texto español cifrado en el que cada símbolo del alfabeto, junto con los signos . , ! ? - (en total 32 símbolos) se ha sustituido por una secuencia de 5 bits es más difícil de descifrar que el mismo texto cifrado en el que cada símbolo se ha sustituido por uno del mismo alfabeto.
2. La secuencia de periodo

   0011010101100110011111

   no puede ser obtenida mediante un LFSR para ninguna elección de polinomio y semilla.
3. El modo de cifrado CFB puede ser considerado como un sistema de cifrado en flujo.
4. El transformado de los bits 101101 011011 111000 por la quinta S-caja de DES es 0111 1001 0100.
5. En el cuerpo de AES el resultado de la operación $(B7 \times 71) + A5 = A4$.
6. La clave privada del criptosistema RSA puede ser obtenida conociendo la clave pública (n, e) si se tiene también $\varphi(n)$.

Respuestas a las preguntas test

1	2	3	4	5	6

Problemas cortos:

7. Descifra el siguiente criptograma

   JP HWNUYTXNXYJQF WXF JX, XNR PZLFW F IZIFX, JP XNXYJQF IJ HNKWFIT FXNQJYWNHT QFX HTRTHNIT D YFQGNJR JP QFX JQUPJFIT. JP RTQGWJ UWTANJRJ IJ PFX NRNHNFPJX IJ PTX FUJPPNITX IJ XZX HWJFITWJX.
8. Para el criptosistema ElGammal de clave pública $(p = 47, \alpha = 5, y = 11)$

   a) Calcula la clave privada.

   b) Firma el mensaje $m = 41$.
9. Sea $n = 1729$. Estudia si n supera los test de primalidad de Fermat y Miller-Rabin para los números $a = 9, 10, 11$.

   ¿Qué conclusiones sacas?. ¿Es n primo o compuesto?. ¿Con que probabilidad?.

Problema:

10. Consideramos el criptosistema RSA de clave pública $(n, e) = (55822831, 7972447)$. La clave privada la poseen los profesores. Ellos, usando el protocolo de Rabin, te transmiten de forma trascordada (o inconsciente) la factorización de n.

    A partir del intercambio de información con los profesores, encuentra la clave privada.

Criptografía

Ingeniería Informática (16- 06-2008)

Alumno:_____ **D.N.I.:**_____

Preguntas tipo test

1. En un texto cifrado con el criptosistema de Vigenère con clave **FULANITA**, el índice de coincidencia del subtexto formado por las posiciones $i \equiv 3 \text{mód } 4$ (se comienza a numerar por 0) es menor que 0'05.

2. La siguiente secuencia

   0 1 0 0 0 1 1 1 1 0 1 0 1 1 0

   satisface los postulados de Golomb

3. 467 es un exponente de descifrado para un criptosistema RSA de clave pública $(1189, 3)$.

4. $(29, 8)$ es una firma válida para el mensaje $m = 25$ que se firma con un criptosistema ElGammal de clave pública $(p = 41, \alpha = 6, y = 35)$.

5. Para dos claves cualesquiera k_1, k_2 y sus respectivas funciones de cifrado DES existe una tercera clave k_3 tal que
$$E_{k_1} \circ E_{k_2}^{-1} \circ E_{k_1} = E_{k_3}$$

6. Para ver si el número 3215031751 es primo, le pasamos el test de Miller-Rabin para $a = 2$ y $a = 8$, y en ambos casos nos sale que el número pasa el test. Entonces podemos asegurar que p es primo con probabilidad mayor que $0'9$.

1	2	3	4	5	6

Problemas cortos

7. Se considera la variable aleatoria X con distribución de probabilidad
$$\left\{p_1 = \frac{1}{21}\ p_2 = \frac{2}{21}\ p_3 = \frac{3}{21}\ p_4 = \frac{2}{21}\ p_5 = \frac{5}{21}\ p_6 = \frac{4}{21}\ p_7 = \frac{4}{21}\right\}$$

   a) Calcula la entropía de esta variable. ¿Cuántos bits se necesitan como media para representar cada uno de los sucesos de esta variable?

   b) Mediante el algoritmo de Huffman construye un código instantáneo óptimo (binario) que nos permita representar los sucesos de esta variable.

8. Calcula la transformada de la columna

A1
03
31
25

   por la transformación MIXCOLUMNS de AES.

9. En un protocolo de secreto compartido (utilizando el método umbral de Shamir) se utiliza el cuerpo $\mathbb{F}_{41}$ y se distribuyen las porciones de secreto:

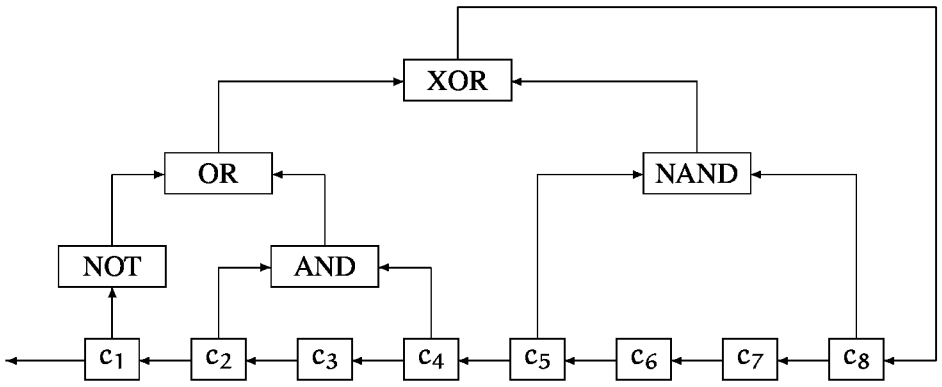
$$(7,13)$$
$$(8,30)$$
$$(11,11)$$
$$(40,31)$$

Calcula el secreto original y determina el número mínimo de porciones necesarias para reconstruirlo.

Problema:

10. Hemos recibido el mensaje 00100111100000001101000011010010001100 10. Este mensaje viene cifrado, con un cifrado en flujo en el que la secuencia cifrante se ha obtenido como la suma de dos secuencias generadas por dos registros de desplazamiento con retroalimentación L_1 y L_2.

L_1 es un registro de desplazamiento con retroalimentación no lineal (NLFSR), donde la función que genera la secuencia viene dada por:



Se recomienda dar la expresión de la función como un polinomio y trabajar con ella

L_2 es un LFSR de 8 celdas.

La semilla para L_1 y L_2, así como el polinomio generador de la secuencia de L_2 vienen cifrados con un criptosistema RSA de llave pública $(1081, 675)$ respectivamente 449, 4 y 314[1]

Para el mensaje se ha usado la siguiente codificación:

B 0011 D 0010 E 11 N 0100 O 0101 S 10 T 0000 U 0001 Esp 011

Descifra el mensaje.

[1]Si el valor de la semilla fuera, por ejemplo 38, significa que $s_0 = 0$, $s_1 = s_2 = 1$, $s_3 = s_4 = 0$, $s_5 = 1$, $s_6 = s_7 = 0$

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.

Criptografía

11 / 06 / 2007

Alumno:_____ **DNI:**_____

Ingeniería Informática **Grupo:**

Ejercicio 1.
Contesta razonadamente a las siguientes cuestiones:

1. Disponemos de un alfabeto de 256 caracteres (caracteres ASCII). ¿Es viable un ataque por fuerza bruta a una sustitución monoalfabética?.
2. La matriz $\begin{pmatrix} 10 & 4 & 7 \\ 5 & 19 & 20 \\ 17 & 14 & 8 \end{pmatrix}$ puede ser la matriz de cifrado de un criptosistema de Hill de 27 caracteres.
3. ¿Es cierto que en $\mathbb{Z}_{1081}$ se verica que $125^{1011} = 467$?
4. ¿Qué característica(s) del criptosistema DES lo hacen apropiado para una implementación en Hardware?.
5. Consideramos la siguiente columna de un estado en un proceso de cifrado AES.

a1
35
ce
20

   Calcula el resultado de aplicarle la transformación *Subbytes* seguida de la transformación *Mixcolumns*
6. ¿Qué ventajas tiene en un criptosistema RSA que los números $\frac{p-1}{2}$ y $\frac{q-1}{2}$ sean primos?.
7. ¿Cuál de estas cuatro características se garantizan con la firma digital?.
   - No repudio.
   - Ingegridad.
   - Confidencialidad.
   - Autenticidad.

   ¿Cuál o cuales se vería afectada por una mala elección de la función resumen?.

Ejercicio 2.
Javier quiere enviar un mensaje a Jesús. Para esto, han decicido usar un criptosistema de cifrado en flujo con un Registro de Desplazamiento Retroalimentado Linealmente (LFRS) con diez celdas. Para establecer la comunicación, Javier envía previamente un par formado por el polinomio generador y la semilla. Para esto, y puesto que Jesús dispone de un criptosistema RSA, utiliza la clave pública de Jesús (que es $(1537, 1165)$) y le envía ambos valores cifrados.
Para cifrar el mensaje, cada carácter se representa mediante una cadena 5 bits como sigue:

- La cadena 00000 se corresponde con el espacio.

- Las cadenas correspondientes a los números 1 - 27 se corresponden con las 27 letras del alfabeto español (A,B,...,Z).
- Las cadenas correspondientes a los números 28 - 31 se corresponden respectivamente con los signos: "punto"; "dos puntos"; "coma" y "punto y coma".

Los pasos seguidos entonces por Javier para crear el mensaje que envía a Jesús son:

- Toma el polinomio generador $p(x)$. Calcula $p(2)$ y cifra el valor obtenido con la clave pública de Jesús. Por ejemplo, si $p(x) = 1+x^2+x^5+x^9$ lo que cifra es $549 = 2^9+2^5+2^2+1 = (1000100101)_2$.
- Toma la semilla, la considera como un valor binario y cifra el valor decimal correspondiente. Así, si $S = (s_0,\ s_1,\ s_2,\ s_3,\ s_4,\ s_5,\ s_6,\ s_7,\ s_8,\ s_9)$ lo que se cifra es el valor (decimal) de $(s_9 s_8 s_7 s_6 s_5 s_4 s_3 s_2 s_1 s_0)_2$
- A partir de la semilla y el polinomio genera la clave de sesión, y con ella cifra el mensaje propiamente dicho.

Jesús recibe el siguiente mensaje:

403
957
01111100110101101101000010101O

Descifra el mensaje que recibe Jesús.

Ejercicio 3. Tema: Protocolos de transferencia inconsciente.

Criptografía

13 / 12 / 2006

Alumno:_____ **DNI:**_____

Ingeniería Informática **Grupo:**

Ejercicio 1.
Contesta Verdadero o Falso (V o F) a las siguientes cuestiones:

1. En $\mathbb{Z}_{3763}$ se verifica que $1325^{3641} = 1325$.
2. Para cualquier $a \in \mathbb{F}_{256}$, con $a \neq 0$, y puesto que $\varphi(256) = 128$, se verifica que $a^{128} = 1$.
3. El protocolo de intercambio de Diffie-Hellman está basado en el problema de la factorización de números grandes.
4. Las redes de Feistel son empleadas en el algoritmo DES.
5. Un certificado $X509$ tiene que ir firmado digitalmente.
6. Es computacionalmente muy costoso el cálculo de raíces cuadradas módulo un primo.
7. En un criptosistema RSA de llave pública (n, e) y llave privada (n, d) se verifica que $ed \equiv 1 (mód\ n)$.
8. Para firmar digitalmente un documento es necesario conocer la clave pública del destinatario.
9. Si en un criptosistema RSA elegimos los primos próximos entre sí, entonces facilitamos su ruptura.
10. Si (p, g, h) es la clave pública de un criptosistema ElGamal, entonces g tiene que ser un elemento primitivo de $\mathbb{Z}_p$.

1	2	3	4	5	6	7	8	9	10

Ejercicio 2.
Miguel quiere enviar un mensaje a María. Antes han decidio usar un criptosistema simétrico de cifrado por bloques, que consiste en dividir el mensaje a cifrar en bloques del tamaño de la clave (13 en este caso) y hacer un XOR de la clave con cada bloque.

Para establecer esta comunicación, necesitan previamente establecer una clave de sesión: un número de 13 bits.

Para cifrar el mensaje, cada carácter se representa mediante una cadena 5 bits como sigue:

- La cadena 00000 se corresponde con el espacio.
- Las cadenas correspondientes a los números 1 - 27 se corresponden con las 27 letras del alfabeto español (A,B,...,Z).
- Las cadenas correspondientes a los números 28 - 31 se corresponden respectivamente con los signos: "punto"; "dos puntos"; "coma" y "punto y coma".

Miguel entonces elige una clave de sesión y la cifra con la clave pública de María (María dispone de un criptosistema RSA de clave pública $(7571, 2957)$).

Miguel manda a María un mensaje en el que incluye la clave de sesión, cifrada con la llave pública de María, y el mensaje, cifrado con la clave de sesión.

María recibe un mensaje que contiene:

5524.

1101111101001 1101010011000 1011001110111 1101000011000 1110010011011
1101000100100 0011001101111 1101001000111 1011001110010 1111110101001

Descifra el mensaje que recibe María.

Ejercicio 3. Tema: Cifrado en flujo.

Criptografía

04 / 09 / 2006

Alumno:_____ **D.N.I.:**_____

Ingeniería Informática **Grupo:**

Ejercicio 1.

Contesta Verdadero o Falso (V o F) a las siguientes cuestiones:

1. En $\mathbb{Z}_{3763}$ se verifica que $1325^{3641} = 1325$.
2. Para cualquier $a \in \mathbb{F}_{256}$, con $a \neq 0$, y puesto que $\varphi(256) = 128$, se verifica que $a^{128} = 1$.
3. El protocolo de intercambio de Diffie-Hellman está basado en el problema de la factorización de números grandes.
4. Las redes de Feistel son empleadas en el algoritmo DES.
5. Un certificado X.509 tiene que ir firmado digitalmente.
6. Es computacionalmente muy costoso el cálculo de raíces cuadradas módulo un primo.
7. Todo cifrado por bloques en modo CBC puede ser visto como un cifrado en flujo.
8. Para firmar digitalmente un documento es necesario conocer la clave pública del destinatario.
9. Si en un criptosistema RSA elegimos los primos próximos entre sí, entonces facilitamos su ruptura.
10. Si (p, g, h) es la clave pública de un criptosistema ElGammal, entonces g tiene que ser un elemento primitivo de $\mathbb{Z}_p$.

1	2	3	4	5	6	7	8	9	10

Ejercicio 2.

Jesús quiere enviar un mensaje a Javier. Dicho mensaje lo va a enviar cifrado, usanndo la clave pública de Javier. Dicha clave pública es la terna $(41, 7, 11)$, que se corresponde con un criptosistema ElGammal.

Puesto que pueden trabajar con números comprendidos entre 0 y 40, previamente han decidido representar los números 0-9 tal cual. Las letras del alfabeto A-Z se corresponden con los números 10-36. Mientras que los símbolos "punto"; çoma"; "punto y comaτ "dos puntos"los representan mediante los números 37-40 respectivamente:

Javier recibe el mensaje siguiente:

$$(17,22)\ (8,30)\ (14,18)\ (10,40)\ (16,28)\ (37,37)\ (12,9)\ (23,18)$$

Descifra el mensaje que recibe Javier.

Ejercicio 3. Tema: Certificados digitales.

Criptografía

05 / 07 / 2006

Alumno:_____ **D.N.I.:**_____

Ingeniería Informática **Grupo:**

Ejercicio 1.

Contesta Verdadero o Falso (V o F) a las siguientes cuestiones:

1. La matriz $\begin{pmatrix} 15 & 2 & 13 \\ 1 & 0 & 22 \\ 13 & 1 & 0 \end{pmatrix}$ puede ser la matriz de cifrado de un criptosistema de Hill de 33 caracteres.
2. La longitud de la clave del criptosistema TDES es el triple que la del criptosistema DES.
3. El criptosistema AES no posee claves débiles, a diferencia del DES.
4. No es cierto que en $\mathbb{Z}_{132}$ se verifica que para cualquier $a \neq 0$, $a^{120} = 1$.
5. Los criptosistemas simétricos, en general, son poco seguros en comparación con los asimétricos.
6. Cualquier persona puede emitir un certificado digital.
7. En un criptosistema RSA de llave pública (n, e) y llave privada (n, e) se verifica que $ed \equiv 1 (\text{mód } n)$.
8. La firma digital garantiza la c onfidencialidad de una comunicación.
9. El resumen de un documento garantiza su autenticidad.
10. La dificultad del cálculo de raíces cuadradas modulares es la base de algunos protocolos criptográficos.

1	2	3	4	5	6	7	8	9	10

Ejercicio 2.

Miguel quiere enviar un mensaje a María. Antes han decidido usar un criptosistema simétrico de cifrado por bloques, que consiste en dividir el mensaje a cifrar en bloques del tamaño de la clave (13 en este caso) y hacer un XOR de la clave con cada bloque.

Para establecer esta comunicación, necesitan previamente establecer una clave de sesión: un número de 13 bits.

Para cifrar el mensaje, cada carácter se representa mediante una cadena de 5 bits como sigue:

- La cadena 00000 se corresponde con el espacio.
- Las cadenas correspondientes a los números 1-27 se corresponden con las 27 letras del alfabeto español (A,B,...,Z).
- Las cadenas correspondientes a los números 28-31 se corresponden respectivamente con los signos: "punto"; "dos puntos"; çomaτ "punto y coma".

Miguel entonces elige una clave de sesión y la cifra con la clave pública de María (María dispone de un criptosistema RSA de clave pública $(2957, 7571)$,

Miguel manda a María un mensaje en el que incluye la clave de sesión, cifrada con la llave pública de María, y el mensaje, cifrado con la clave de sesión.

María recibe un mensaje que contiene:
3790

1101111101001	1101010011000	1011001110111	110100001100	1110010011011
1101000100100	0011001101111	1101001000111	1011001110010	1111010101001

Descifra el mensaje que recibe María.
Ejercicio 3. Tema: Protocolos de secreto compartido.