TEST

ETSETB
Curso 2008-09 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
22 de enero de 2009

PUBLICACIÓN DE NOTAS PROVISIONALES: 26/01/2009 A LAS 19:00 HORAS
FECHA LÍMITE PARA LAS ALEGACIONES: 27/01/2009 a las 14:00 horas
PUBLICACIÓN DE NOTAS DEFINITIVAS: 29/01/2009

NOTAS IMPORTANTES:

- Toda hoja de respuestas que no esté completamente identificada será anulada.
- La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
- No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere oportunas por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales y hasta el plazo arriba indicado. En ellas debe consignarse OBLIGATORIAMENTE el DNI y el código de la prueba.
- QUEDA EXPRESAMENTE PROHIBIDO EL USO DE CUALQUIER DISPOSITIVO DE COMUNICACIÓN. EL INCUMPLIMIENTO DE ESTA NORMA SUPONDRÁ LA EXPULSIÓN DEL EXAMEN.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

1. Sea un sistema RSA para dos usuarios A y B y una autoridad certificadora CA, con los parámetros de la **Tabla 1**. El formato del certificado de un usuario i consta de su identificador ID_i (1 byte), seguido de su clave pública $K_{Pi} = (e_i, N_i)$ (2 bytes, uno para e y otro para N), y de la firma de la CA (1 byte). B recibe el siguiente certificado: 00001111000000110010000101011100. La función de Hash $H(M)$ que se emplea en dicho sistema es la siguiente:
   - Las secuencias binarias se consideran con más peso a la izquierda (MPI).
   - Se añaden a la izquierda del mensaje tantos ceros como sea necesario para que la longitud sea múltiplo de 6.
   - Se divide el mensaje resultante desde la izquierda en n bloques de 6 bits, m_i $0 \leq i \leq n-1$.
   - $h_0 = DCD(m_0)$, siendo DCD = Desplazamiento Circular a Derecha.
   - $h_{i+1} = DCD(h_i \oplus m_{i+1})$, $0 \leq i \leq n-2$.
   - $H(M) = h_{n-1}$

   Qué afirmación es cierta:

   a) B concluye que quien ha enviado ese certificado es A
   b) B concluye que el certificado no es auténtico
   c) El certificado de A sirve para que B sepa cuál es la clave privada de A
   (d) Ninguna de las anteriores

Certificado A = 00 10 111 | 00 00 00 11 | 00 10 00 00 | 10 10 11 00

ID_A | $e_A = 3$ | $N_A = 33$ = $p_A \cdot q_A = 3 \cdot 11$ | $FD(H_A) \equiv 92$

M_2

$FD(H_A) = H(H_A)^{d_{CA}} \bmod N_{CA} \Rightarrow H(H_A) = FD(H_A)^{e_{CA}} \bmod N_{CA}$

$H(H_A) = 92^{77} \bmod 119 = 57$

00 00 11 | 11 00 00 | 00 11 00 | 10 00 01

m_0 | m_1 | m_2 | m_3 $\quad n = 4$ bloques

$h_0 = 100001$

$h_1 = DCD(h_0 + m_1) = DCD(010001) = 101000$

$h_2 = DCD(h_1 + m_2) = DCD(100100) = 010010$

$h_3 = DCD(h_2 + m_3) = DCD(110011) = 111001 = H(M) \equiv 57$

El certificado es auténtico, lo generó la CA, esa clave pública de A es auténtica. Pero ello no implica que su poseedor sea A!

2. Sea un código (90, 78) binario lineal sistemático. Qué afirmación es correcta:

(a) Puede ser un código 2-perfecto

b) El subespacio vectorial ortogonal al código tiene dimensión 78

c) Hay 2^{12} errores no nulos detectables

d) Ninguna de los anteriores

a) $2^r = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} = 1 + n + \frac{n(n-1)}{2}$

$\left.\begin{matrix} n=90 \\ k=78 \end{matrix}\right\} r = n-k = 12$ $\qquad 2^{12} = 1 + 90 + \frac{90 \cdot 89}{2}$

$4096 = 4096$

b) Tiene dimensión $r = 12$

c). nº errores no nulos $= 2^n - 1$

• nº errores no nulos NO detectables =

$=$ nº palabras código (excepto $\emptyset$) $= 2^k - 1$

• nº errores no nulos detectables $= 2^n - 1 - (2^k - 1) = 2^n - 2^k$

Pero $2^n - 2^k \neq 2^r$!!

3. Sea c(D)=$D^3 + D + 1$ el polinomio de conexiones de un LFSR. Qué afirmación es correcta:

a) c(D) divide a $D^{12} + 1$
b) c(D) divide a $D^{15} + 1$
c) c(D) divide a $D^{21} + 1$
d) Ninguna de las anteriores

a) Un c(D) completo de grado m, divide a $D^{K(m+1)} + 1$
(con K natural positivo) $m=3, K=3 \rightarrow D^{12} + 1$
Pero este c(D) no es completo.

Un c(D) primitivo grado m, divide a $D^{k \cdot L} + 1$
(k natural positivo) con $L = 2^m - 1$,
y no divide a ningún $D^\lambda + 1$, $\lambda = m, m+1 \ldots L-1$.

$m=3 \rightarrow L=7 \rightarrow$ c(D) divide a $D^{3 \cdot 7} + 1 = D^{21} + 1$

4. Sea un código sistemático (5, 2) caracterizado por el polinomio generador $g(D) = D^3 + 1$.Qué afirmación es correcta:

(a) El número de vectores de error no nulos detectables es 28

b) El error $e(D) = D^4 + D^3 + 1$ no se detecta

c) El errore$(D) = D^3 + 1$ se detecta con probabilidad 75 %

d) Ninguna de las anteriores

a) $2^n - 2^k = 2^5 - 2^2 = 32 - 4 = 28$

b) $g(D) = (D+1) \cdot (D^2 + D + 1)$ → Detecta todos los errores impares (con nº impar de unos, nº impar de términos)

(primitivo)

$e(D) = D^{20} + D^{15} + 1$ se detecta.

c) $e(D) = D^3 + 1$

$g(D) = D^3 + 1 \rightarrow r = 3$

Como $e(D) \bmod g(D) = 0$, ese error NO se detecta, con total seguridad.

Error → $e(D) = D^r + \boxed{D^{r-1} + \dots + D + 1}$

$g(D) = D^r + \boxed{D^{r-1} + \dots + D + 1}$

prob. coincidencia $= \frac{1}{2^{r-1}}$;; prob. detección $= 1 - \frac{1}{2^{r-1}} =$

$= 1 - \frac{1}{4} = 75\%$

5. Sean A y B dos fuentes discretas cada una con un alfabeto de 8 símbolos. Si $H(A|B) = 3$, puede afirmarse que:

   a) $H(A) > 3$

   b) $H(B) \leq H(A)$

   c) $H(B) = H(A)$

   d) Ninguna de las anteriores

$0 \leq H(A) \leq \log_2 8 = \log_2 2^3 = 3$

$0 \leq H(B) \leq 3$

$H(A) \geq H(A|B) = 3$

$H(A) \leq 3$

$H(A) \geq 3$

$\Rightarrow H(A) = 3$

$H(B) \leq H(A)$

6. Descodifique la secuencia 21357 si fue generada con el algoritmo de compresión LZW. El código está inicialmente cargado como 1 A, 2 B, 3 C.

   a) BACACA
   b) BACAACAC
   c) BACACACA
   d) Ninguna de las anteriores

1	A
2	B
3	C
4	BA
5	AC
6	CA
7	

2 1 3 5 7

B A C AC ?

4 5 6

AC = → ACA

BACAC ACA

Esto sucede cuando al codificar se codificó una palabra justo metida en el diccionario.

7. Un usuario genera un mensaje M y lo firma, usando una función de Hash de 160 bits. Posteriormente quiere repudiar dicho mensaje, y para ello pretende generar otros mensajes distintos que tengan firma idéntica al original. ¿Cuál es el número de mensajes necesarios para *garantizar* que lo consiga?

   a) 2^{160}

   b) 2^{159}

   c) 2^{80}

   d) Ninguno de los anteriores

Solución: No se puede garantizar que dos mensajes tengan el mismo Hash → d)

8. Sea un código de canal lineal sistemático (5, 2) con palabras código Y1=10110 y Y2=11101. Si se recibe Z=01100 puede afirmarse que:

   a) El mensaje estimado es 11

   b) Hay dos palabras código igual de verosímiles

   c) Se han producido 3 bits erróneos

   d) Ninguna de las anteriores

X	Y	d(Z, Y)
00	$00000 = Y_0$	2
01	$01011 = Y_1 + Y_2$	3
10	$10110 = Y_1$	3
11	$11101 = Y_2$	2

Y_0 e Y_2 son igual de verosímiles, están a la misma distancia de Z. $\hat{X} = \begin{cases} 00 \\ 11 \end{cases}$ de forma equiprobable.

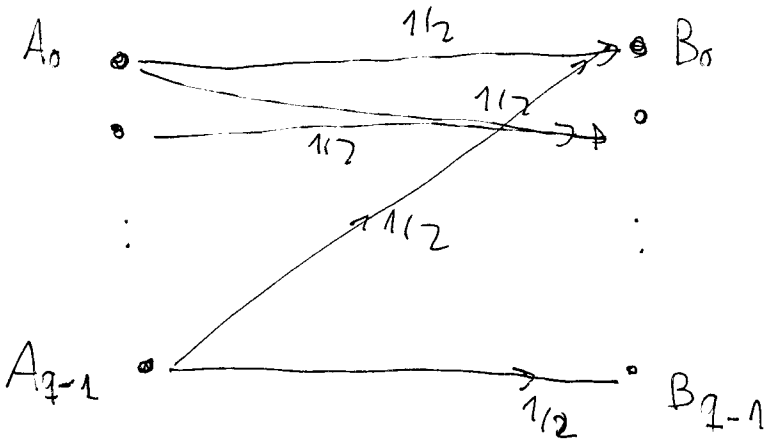
9. Sea un canal con un alfabeto q-ario ($q \geq 2$) a su entrada y salida. Para cada símbolo a la entrada del canal (A_i), la salida puede tomar dos valores de forma equiprobable (B_i y $B_{(i+1) mod q}, 0 \leq i < q$). Calcule la capacidad de canal (en bits por símbolo enviado al canal).

(a) $log_2(q/2)$

b) $log_2\ q$

c) 1

d) Ninguna de las anteriores



$$C = \max \{ I(A;B) \} = H(B) - H(B/A) =$$

$$H(B/A) = H(1/2) = 1$$

$$= \max \{ H(B) \} - 1 = \log_2 q - 1 =$$

$$= \log_2 \left(\frac{q}{2} \right)$$

10. Sea una fuente que emite 4 símbolos con probabilidades P(A)=1/2, P(B)=1/4, P(C)=P(D)=1/8. Para una codificación aritmética de la secuencia ABACABADA, ¿Cuánto vale la longitud del intervalo de codificación?

   a) 2^{-15}
   b) 2^{-9}
   c) 2^{-18}
   d) Ninguna de las anteriores

LA LONGITUD DEL INTERVALO DEPENDE EXCLUSIVAMENTE DE LAS PROBABILIDADES DE LOS SIMBOLOS DE LA SECUENCIA (5A, 2B, 1C, 1D)

$$\text{long} = \left(\frac{1}{2}\right)^5 \cdot \left(\frac{1}{4}\right)^2 \cdot \frac{1}{8} \cdot \frac{1}{8} = \frac{1}{2^{15}} = 2^{-15}$$

11. Sabiendo que N=137*193=26441 es una clave RSA, calcule $X=4^{52227}$ mod 26441.

(a) 64

b) 4096

c) 18724

d) Ninguna de las anteriores

como 137 y 193 son primos (al ser clave RSA)

$\phi(N) = 136 \cdot 192 = 26112$

$52227 = 2 \cdot 26112 + 3$ $\quad 4^{k\phi(N)} \bmod N = 1$

$X = 4^{52227} \bmod 26441 = 4^{2\cdot\phi(N)+3} \bmod N =$

$= 4^3 \bmod 26441 = 64$

12. Sea un sistema RSA con los parámetros indicados en la **Tabla 1**. La función de hash empleada se calcula como H(M)=M. A desea enviar el mensaje M=12 a B protegiendo la transmisión frente a ataques pasivos. ¿Qué criptograma debe transmitir?

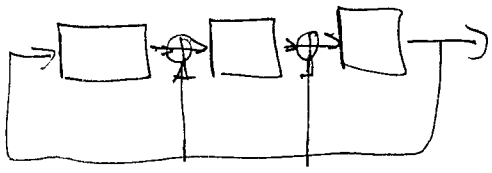
   a) 23
   b) 12
   c) 31
   d) Ninguna de las anteriores

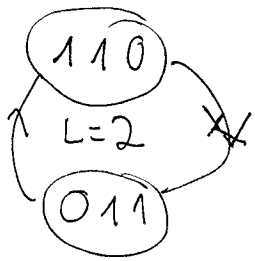
PARA PROTEGER CONTRA ATAQUES PASIVOS HAY QUE OFRECER CONFIDENCIALIDAD, CIFRANDO CON LA CLAVE PÚBLICA DE B.

$$C = M^{e_B} \bmod N_B = 12^3 \bmod 55 = 23$$

13. Sea un LFSR caracterizado por el polinomio de conexiones $C(D) = D^3 + D^2 + D + 1$ y con estado inicial $S(D) = D + 1$. El estado al cabo de 339 iteraciones vale:

a) $S(D) = D^2 + D$
b) $S(D) = D + 1$
c) $S(D) = 1$
d) Ninguna de las anteriores





PERIODO 2 PARA ESTE ESTADO INICAL $\{1+D ; D+D^2\}$

AL CABO DE CUALQUIER Nº IMPAR DE ITERACIONES, EL ESTADO SERÁ $D+D^2$

14. Sea un código lineal sistemático (6, 3) que garantiza la corrección de un error. Se sabe que la palabra Y1=(100110) pertenece al código. ¿Cuál de las siguientes palabras puede ser palabra código?

a) (111111)
b) (010010)
c) (110111)
(*d*) Ninguna de las anteriores

$$\begin{pmatrix} 100\ 110 \\ 010\ xyz \\ 001\ abc \\ 011001 \\ 111111 \\ 101\ \bar{a}\bar{b}c \\ 110\ \bar{x}\bar{y}\bar{z} \end{pmatrix}$$

$$\begin{array}{l} 100\ 110 \\ \oplus\ 010\ xyz \\ \oplus\ 001\ abc \\ \hline (1,1,1,\ 1\oplus x\oplus a,\ 1\oplus y\oplus b,\ z\oplus c) \end{array}$$

Para que sea (1,1,1,1,1,1) debe pasar que [x=a, y=b, z≠c]

Las combinaciones a probar son:

$$\begin{pmatrix} x=0 & y=0 & z=1 \\ a=0 & b=0 & c=0 \end{pmatrix} \begin{pmatrix} 000 \\ 001 \end{pmatrix} \begin{pmatrix} 110 \\ 111 \end{pmatrix} \begin{pmatrix} 111 \\ 110 \end{pmatrix} \begin{pmatrix} 101 \\ 100 \end{pmatrix} \begin{pmatrix} 100 \\ 101 \end{pmatrix} \begin{pmatrix} 011 \\ 010 \end{pmatrix} \begin{pmatrix} 010 \\ 011 \end{pmatrix}$$

(A) $\begin{pmatrix} 001 \\ 000 \end{pmatrix}$ tendríamos 010001 y 011001 a dmin=1. NO

(B) $\begin{pmatrix} 000 \\ 001 \end{pmatrix}$ tendríamos 001001 y 011001 a dmin=1. NO

(C) $\begin{pmatrix} 110 \\ 111 \end{pmatrix}$ tendríamos 001111 y 111111 a dmin=2. NO

(D) $\begin{pmatrix} 111 \\ 110 \end{pmatrix}$ tendríamos 010111 y 111111 a dmin=2. NO

(E) $\begin{pmatrix} 101 \\ 100 \end{pmatrix}$ tendríamos 010101 y 011001 a dmin=2. NO

(F) $\begin{pmatrix} 100 \\ 101 \end{pmatrix}$ tendríamos 001101 y 011001 a dmin=2. NO

(G) $\begin{pmatrix} 011 \\ 010 \end{pmatrix}$ tendríamos 110101 y 111111 a dmin=2. NO

(H) $\begin{pmatrix} 010 \\ 011 \end{pmatrix}$ tendríamos 101101 y 111111 a dmin=2. NO

En conclusión, no hay ninguna combinación de la base de un código lineal con (100110), (111111) y que corrija 1 error $C_c = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor \leftrightarrow d_{min}=3$.

15. Se dispone de un LFSR constituido por un número de celdas $n \geq 5$, y un polinomio de conexiones completo ($c(D) = \sum_{i=0}^{n} D^i$). Si el estado inicial es D^3, indique cuál de los siguientes puede ser el estado al cabo de 137 iteraciones.

a) $D^3 + D + 1$

b) $D^4 + D^2 + D + 1$

c) $D^2 + 1$

d) Ninguna de las anteriores

Respuesta correcta: d.

Si el estado inicial es D^3, el siguiente será D^4, ... hasta D^{n-1}, luego $\sum_{i=0}^{n-1} D^i$, luego 1, D, y D^2. Es decir, o es una potencia de D, o el polinomio $\sum_{i=0}^{n-1} D^i$, y por tanto ninguno de ellos puede serlo.

16. Todos los empleados de una empresa usan RSA con N de 10
que e no es divisor de $\phi(N)$, indíquese cuál es la respuesta cor

(a) El uso de esta solución permite ganar velocidad al realizar la e

b) El uso de esta solución facilita la tarea de un criptoanalista

c) Dicho valor no se puede escoger para ningún usuario

d) Todas las anteriores son incorrectas.

Solución: El valor de e es pequeño (comparado con N), por lo que las funcion rápidas (verificar firmas, codificar), que son las mayoría. En cambio, la clave pr mayor por lo que las operaciones que la usan (firmar, descodificar) son más largas.

17. En la recepción de palabras que han sido codificadas mediante un código lineal, se reciben dos Z_1 y Z_2 que dan lugar al mismo síndrome. Se puede afirmar que:

   a) El vector de error en ambas puede ser distinto

   b) La distancia de Hamming entre ambas puede ser inferior a la distancia mínima del código

   c) El código no se puede utilizar como corrector de errores

   d) Ninguna de las anteriores

18. La variable aleatoria de una fuente Y es $Y = X^2 + 3$, donde X es la variable aleatoria de otra fuente con entropía no nula. Puede afirmarse que:

a) $H(X,Y) > H(X)$
b) $H(X,Y) > H(Y)$
c) $I(X;Y) = 0$
d) Ninguna de las anteriores

$H(Y \setminus X) = 0$ $\quad H(X,Y) = H(X) + H(Y \setminus X) = H(X)$

$H(X \setminus Y) \geq 0$ Si el alfabeto de X contiene elementos TODOS POSITIVOS o TODOS NEGATIVOS, a partir de Y la X queda totalmente determinada (unívocamente determinada). Entonces $H(X \setminus Y) = 0$

En el resto de casos, $H(X \setminus Y) > 0$ y por tanto $H(X,Y) = H(Y) + H(X \setminus Y) > H(Y)$

Por tanto, solo podemos afirmar que $H(X,Y) \geq H(Y)$.

19. Sea M el mensaje en claro (m bits), C el criptograma (n bits) y k la clave de cifrado (r bits). Indíquese cuál es la respuesta correcta.

a) $H(M|C) > n$

b) $H(M|C) > r$

c) $H(M|C) \leq m$

d) Ninguna de las anteriores

Solución:
H(M/C)<=H(M)<=m → H(M/C)<=m

20. Un código lineal polinómico codifica mensajes de usuario de 28 bits usando como polinomio generador $g(D) = p(D)(D + 1)$, siendo $p(D)$ un polinomio primitivo de grado 4. ¿Cuál es la probabilidad p, que habiendo dos errores, **no** sean detectados?

a) $1{,}89\ 10^{-2}$

b) $3{,}41\ 10^{-2}$

c) $3{,}98\ 10^{-2}$

d) Ninguna de las anteriores

Tabla 1

Usuario	p	q	e	d	ID
A	3	11	3	7	00001111
B	5	11	3	27	11110000
CA	7	17	77	5	-

Respuesta correcta c.

El polinomio g(D) tiene grado r=5.
Las palabras código tienen k+r=28+5=33 bits.
Para hallar la probabilidad, calculamos los casos posibles y los favorables.

- Casos posibles: contar cuántas palabras código hay con 2 bits erróneos, de entre 33 bits.
- Casos favorables: No serán detectados aquellos e(D) múltiplos de g(D). Con dos errores, e(D) tiene dos componentes.
  - p(D) es primitivo de grado 4, por lo que divide a $(D^{15}+1)^* D^j$, con $j \in (0, \ldots, 17)$, ya que e(D) no puede tener un grado mayor que 32 (hay 33 bits) → Hay 18 casos
  - Además, p(D) también es factor de $(D^{30}+1)^* D^j$, con $j \in (0, \ldots, 2)$, por el mismo motivo. → Hay 3 casos
  - Casos favorables = 21
  -

Hay 21 casos favorables y $\binom{33}{2}$ casos posibles.
Probabilidad = p = 3,977 * 10^{-2}