CONTROL DE TRANSMISIÓN DE DATOS. 25 de Mayo de 2006

Notas Importantes:

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Los problemas se entregan **juntos**, ponga su nombre y apellidos en cada hoja, enumerándolas.
3. Un error conceptual grave, puede anular todo el problema.
4. Lista de los números primos hasta el 1103:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103

1. Sean X e Y dos variables aleatorias tales que $X=\{X_1, X_2\}$ y $Y=\{Y_1, Y_2\}$. Se sabe que $p(Y_1\backslash X_1)=3/4$, $p(Y_2\backslash X_2)=1/2$, $p(X_1)=(1/2)\cdot p(X_2)$. Obtenga H(Y).

2. Una fuente emite 2 símbolos con probabilidades p(A)=1/4 y p(B)=3/4. Se usa un código aritmético. Descodifique la palabra código 0'04 sabiendo que la longitud de la secuencia emitida es 3.

3. Sabiendo que $91537=383\cdot239$, demuestre que $1021^{90916} \bmod 91537=74682$.

4. Calcule $\Phi(7875)$.

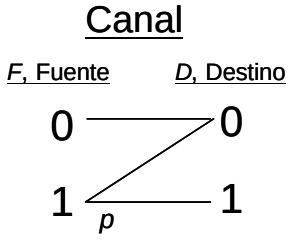
5. Sean F_1 y F_2 dos fuentes equiprobables cuyos elementos pertenecen al conjunto {1, 2, 3, 4}. Sea F otra fuente cuya salida es el *mcm* de los símbolos emitidos por F_1 y F_2. Calcule H(F).

6. Sea una fuente binara con probabilidades p(0)=0,4 y p(1)=0,6. Emite sobre un canal BSC (*Binary Symmetric Channel*) con probabilidad de error en el bit p_E=0,1. Calcule la entropía a la salida.

7. Sabiendo que $(D^{256}+D^{255}) \bmod C(D)=D+1$, siendo C(D) un polinomio primitivo, ¿de qué grado puede ser C(D)?

8. Sea una fuente que emite los símbolos {A, B, C}. Codifique el mensaje AABBCBCBABA según el código fuente LZW.

9. Calcule en función de *p*, la capacidad de canal que tiene el canal discreto binario definido por el siguiente diagrama de transiciones.



Nota: Para mayor comodidad en las operaciones, utilice: $H(p)=p\cdot\log_2\frac{1}{p}+(1-p)\cdot\log_2\frac{1}{(1-p)}$

SIGUE DETRÁS

10. Sea un sistema de clave pública RSA. Considere dos usuarios A y B y una entidad CA que expende certificados para autenticar el origen de los mensajes. Los usuarios del sistema utilizan criptografía asimétrica **RSA** para **intercambiar una clave de sesión**, utilizada a su vez para **codificar mensajes** mediante **cifrado de flujo síncrono implementado con LFSR**. Las secuencias binarias se consideran con más peso a la izquierda (MPI).

Parámetros RSA de los usuarios y de la entidad certificadora, e identificadores de cada usuario:

Usuario A	p_A=7, q_A=17, e_A=11, d_A=35	ID_A=0001
Usuario B	p_B=3, q_B=11, e_B=7, d_B=3	ID_B=0010
Entidad certificadora CA	p_{CA}=7, q_{CA} =11, e_{CA}=37, d_{CA}=13	ID_{CA}=0011

La función de *Hash* H(M) correspondiente a un mensaje M, que se emplea en dicho sistema es la siguiente:

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden al inicio del mensaje tantos unos como sea necesario para que la longitud sea múltiplo de **4**.
- Se divide el mensaje resultante desde la izquierda en *n* bloques de **4** bits, m_i $0 = i = n-1$.
- $h_0=DCI(m_0)$, siendo **DCI** = Desplazamiento Circular a Izquierda.
- $h_{i+1}=DCI(h_i Å m_{i+1})$, $0 = i = n-2$.
- $H(M)=h_{n-1}$
- $H(M)$ debe ocupar **4 bits**.

La autoridad certificadora CA sigue el siguiente esquema para expender los certificados (**en hexadecimal**): Un usuario *i* entrega a la CA el certificado en claro correspondiente a la concatenación (||) de su identificador ID_i y de su clave pública K_{Pi}. La CA firma digitalmente dicho certificado en claro y añade la firma detrás: *Certificado firmado = certificado en claro* || *firma digital.*

El algoritmo de cifrado en flujo se realiza mediante un LFSR con polinomio de conexiones $C(D)=D^3+D^2+D+1$. La $\mathbf{K_{SESIÓN}}$ **es el estado inicial** del LFSR. La secuencia pseudoaleatoria generada se utiliza para cifrar el mensaje. Considere que el primer bit de salida del LFSR es el bit de mayor peso MPI (más peso a la izquierda) de la secuencia pseudoaleatoria generada.

a) B recibe de A su certificado (**en hexadecimal**), que previsiblemente fue firmado previamente por CA: **1B7740**. Realice las operaciones que hace B para autenticar su procedencia.

b) Si el certificado es falso, obtenga el certificado auténtico que hubiera enviado el usuario A.

c) Si el certificado es auténtico, proceda a calcular qué envía B a A para comunicarle la **clave de sesión**, $\boldsymbol{k_{sesión} = 7}$.

d) Codifique el mensaje 10010110 que B envía a A.