Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
27 de Mayo de 2005

NOTAS IMPORTANTES:

1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
2.- *Se valorará la justificación, discusión y claridad de los resultados.*
3.- ***Los resultados no reflejados en la hoja de resultados anexa no serán tenidos en cuenta.***
4.- *Un **error conceptual grave** puede anular todo el problema.*
5.- *Nótese que **los problemas constan de distintas partes que pueden resolverse por separado**. Se recomienda saltar aquellas partes que no sepan resolverse.*

Problema 1 (20%)

Una fuente emite dos símbolos (A y B) quedando completamente caracterizada por las siguientes probabilidades de emisión condicionadas:

$$p(B/A) = 0.3$$
$$p(A/B) = 0.7$$

Dicha fuente atraviesa un canal binario simétrico con una tasa de error de 0.7
Se pide:

a) ¿Cuál es la entropía de la fuente? **(3 puntos)**
b) ¿Cuál es la entropía a la salida del canal? Coméntese el resultado. **(4 puntos)**
c) Si se cambia el canal por otro (tambien binario simétrico) la entropía a su salida es de 1 bit/símbolo ¿Cuál es la tasa de error del nuevo canal? **(2 puntos)**
d) ¿Cuál de los dos canales es mejor? ¿por qué? **(1 punto)**

Problema 2 (20%)

Suponga que dispone de un algoritmo que dado un valor arbitrario x le proporciona otro valor y de forma que:

$$x^2 \equiv y^2 \bmod(n) \quad con\ y \neq \pm x \mod(n)$$

donde n es el producto de dos primos impares distintos ¿Cómo utilizaría dicho algoritmo para romper un sistema RSA que trabajase módulo n?

Problema 3 (20%)

El módulo de un sistema Diffie-Hellman es $p=2q+1$, donde q es un número primo. La base de dicho sistema es α.

Se pide:

a) ¿Qué propiedad debe cumplir α?¿por qué?**(2 puntos)**

Para un valor X aleatorio

b) ¿Qué valores puede tomar $X^{(p-1)/2} \bmod p$? **(3 puntos)**
c) Para un cierto valor β, se tiene que $\beta^q \bmod p \neq p-1$. ¿puede ser β primitivo?¿por qué? **(5 puntos)**

SIGUE DETRÁS

Problema 4 (40%)

Sabiendo que la función Phi de Euler es multiplicativa, esto es:

$$\Psi(mn) \equiv \Psi(m)\Psi(n) \quad si \quad mcd(m,n) = 1$$

si en un sistema de clave pública (análogo a RSA) se tiene por módulo $n = 385$
Se pide:

a) ¿Cuánto vale $\Psi(385)$? **(2 puntos)**
b) ¿Qué exponente público (*e*) elegiría, el 3 o el 7? **(2 puntos)**
c) ¿Calcule un exponente privado (*d*) válido? **(3 puntos)**
d) Se dispone de una función de "hash" de 8 bits. Se desea firmar un archivo M de 1024 bytes, donde hash(M)=3. ¿Cómo debe construirse la firma de M? ¿Cuál es el número esperado de mensajes de la misma longitud de M que tienen la misma firma? **(3 puntos)**