Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
15 de diciembre 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 (50%)

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

$$p(B/A) = 0.1$$
$$p(A/B) = 0.4$$

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

a) ¿Cuál es la entropía de la fuente? **(3 puntos)**
b) Plantee la ecuación que ha de satisfacer el valor máximo de p_e ($p_e = 0.5$) que permite que por el canal pueda trasmitirse la información emitida por la fuente de manera fiable. Suponga que la solución de la ecuación es $p_e = 0.0883$ **(3 puntos)**
c) ¿Cuál es el valor de la entropía observada a la salida del canal? **(2 puntos)**
d) Realice la codificación de Huffman de la fuente extendida en agrupaciones de dos símbolos? **(2 puntos)**

Problema 2 (50%)

El objetivo del problema es establecer, de forma guiada, un protocolo de pago por cheques electrónicos que permita el anonimato del comprador.
El principio fundamental es la "*firma a ciegas*" es decir, el banco emisor firma un cheque desconociendo su contenido ya que confía plenamente en el cliente que le solicita la firma. Con posterioridad se entenderá por qué el banco tiene tal confianza.

Se pide:

a) Justifique que, para el método RSA (e, d, n), se satisface que "el cifrado del producto es el producto de los cifrados, todo ello módulo n" **(1 punto)**
b) El objetivo del cliente es obtener la firma de cheque M sin que el banco sepa cuál es el valor de M. Para ello el cliente solicita la exponenciación al número secreto del banco de tM donde tanto t como M son desconocidos para el banco. Una vez obtenido $(tM)^d$ lo multiplica por r. ¿Qué relación deben guardar t y r para que $(tM)^d\, r = M^d$? **(3 puntos)**
c) Supóngase que el significado de cada cheque es "*páguese al primer portador del presente cheque la cantidad de 100 €*". Para que el sistema funcione, cada cheque debe

SIGUE DETRÁS

tener un número de serie distinto y desconocido a priori por el banco. Supongamos que el número de serie consta de 128 bits. Especifique cómo compondría el valor de M en la expresión anterior (recuerde utilizar un mecanismo de hash para dar consistencia a la firma). Determine la probabilidad de que accidentalmente dos usuarios distintos generen dos cheques idénticos. **(3puntos)**

Para que el banco tenga confianza en el cliente puede procederse mediante el siguiente símil:

- El cliente presenta al banco mil sobres cerrados con el cheque solicitado
- El banco solicita al cliente la apertura de 999 de los sobres y verifica que todos son correctos
- El banco firma el sobre cerrado que resta

d) Establezca el símil anterior en términos criptográficos. Recalcule con estos parámetros la probabilidad de que accidentalmente dos usuarios distintos generen dos cheques idénticos **(2puntos)**

e) Recapitule todo el procedimiento **(1 punto)**