Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
5 de Diciembre de 2002

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 (60%)

Es sabido que la base del sistema RSA es el teorema de Euler

$$m^{\Phi(n)} \equiv 1 \bmod n \quad si \quad mcd(m,n) = 1$$

Sin embargo para $n = pq$ se satisface también que

$$m^{\lambda(n)} \equiv 1 \bmod n \quad si \quad mcd(m,n) = 1$$

donde $\lambda(n) = mcm(p-1, q-1)$.

Este hecho conlleva que, en realidad, existe más de un exponente privado que deshace la operación realizada por una clave pública.

Para el siguiente sistema RSA

$$n = 499 * 439; e = 17$$

Se pide:

a) Demuestre que $\lambda(n) \le \Phi(n)/2$ para cualquier elección de p y q como primos impares distintos(**10%**)
b) Encuentre TODOS los valores de d, en el rango [$0..n$], que pueden ser utilizados como exponente privado si se utiliza como exponente público $e=17$(**50%**)
c) ¿Cuántas firmas distintas existen para un mensaje dado? (**10%**)
d) Se dispone de una función de "hash" de 16 bits. Se desea firmar un archivo M de 1024 bytes, donde hash(M)=12344. ¿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?(**30%**)

PROBLEMA 2 (20%)

Justifique que todo polinomio de coeficientes binarios de grado 5 que sea irreducible, también ha de ser primitivo.

PROBLEMA 3 (20%)

Una fuente emite dos símbolos independientes con probabilidades 0.8 y 0.2. Al atravesar un canal binario simétrico la entropía a la salida del mismo vale 0.8267 bits/símbolo ¿Cuánto vale la tasa de error del canal?