Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS

17 de mayo de 2006

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.- *Un **error conceptual grave** puede anular todo el problema.*
4.- *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%)

Sabiendo que se satisface que:

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

Se pide:

a) Encuentre el número público y privado para un criptosistema análogo a RSA cuyo modulo sea 2717. Cómo número público ha de emplearse uno de los siguientes{ 3, 5, 7 , 9} (**6 puntos**)
b) Encuentre el criptograma correspondiente al mensaje M=22 (**1.5 puntos**)
c) Sabiendo que el hash de un fichero F es H(F)=277, indique si la firma {F,30} es válida para el sistema anterior (**2.5 puntos**)

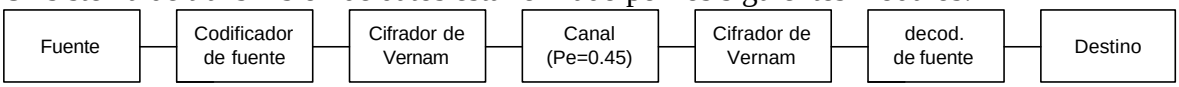
PROBLEMA 2 (15%)

Indique, de forma justificada, cuáles de los siguientes polinomios de coeficientes binarios son primitivos, sabiendo que todos son irreducibles:

$$D^3+D+1, \quad D^5+D^2+1, \quad D^7+D+1$$

PROBLEMA 3 (35%)

Un sistema de transmisión de datos está formado por los siguientes módulos:



La **fuente** emite dos símbolos quedando totalmente determinada por las probabilidades P(A|A)=0.1 y P(B|B)=0.4

Se pide:

a) Entropía de la fuente **(2 puntos)**
b) Capacidad del canal **(2 puntos)**
c) Capacidad que observa un atacante si desconoce la clave de cifrado. **(1 puntos)**

Si la fuente emite la secuencia A, B, A, B

d) ¿Qué secuencia decidirá el receptor legítimo con mayor probabilidad? **(2.5 puntos)**
e) ¿Qué secuencia decidirá un atacante si desconoce la clave de cifrado con mayor probabilidad? **(2.5 puntos)**