Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona UNIVERSITAT POLITÈCNICA DE CATALUNYA **DEPARTAMENT D'ENGINYERIA TELEMÀTICA**	**Transmissió de dades, grupo 50** Fecha: 23 Nov 2006 Notas provisionales: 30 Nov Período de alegaciones: 5 Dic Fecha notas revisadas: 11 Dic

Información adicional:

- Duración de la prueba: 2 HORAS
- Cualquier error conceptual grave puede anular todo el problema

PROBLEMA 1 (35%)

Sea una función de hash H(M), con una salida de k bits, que se calcula de la siguiente forma:

- 1. Se añade al final del mensaje el número de ceros necesario para que la longitud el mensaje sea múltiplo de k
- 2. Se divide el mensaje en n bloques de k bits, m_i $0 = i = n-1$
- 3. H(M) se calcula iterativamente de la siguiente manera:
  - $h_0=m_0$
  - $h_{i+1}=h_i \oplus m_{i+1}$ $0= i= n-2$
  - $H(M)=h_{n-1}$

a) Indique las propiedades que debe cumplir una función de hash criptográficamente robusta, y diga cuales de ellas cumple la función propuesta.
b) Sea el mensaje M= 10101010101010101010. Calcule H(M) para k=6.
c) Sea un sistema de RSA en el que todos los usuarios usan e=23. Genere un par de claves RSA con p=11, q=13. Indique cual sería la clave privada y la pública, utilizando el algoritmo extendido de Euclides.
d) Firme digitalmente el mensaje del apartado b con el sistema de claves generado en el apartado c y la función de hash propuesta (considere siempre que los bits de menor peso son los de la derecha). Indique qué servicios de seguridad ofrece la firma digital.
e) Suponga que un atacante quiere modificar un mensaje firmado digitalmente con el sistema anterior. Indique la forma más eficiente de hacerlo y genere un mensaje que tenga la misma firma que M.

PROBLEMA 2 (40%)

Sea F_A una fuente equiprobable y ternaria con alfabeto {-1, 0, 1}, y F_B otra fuente cuya salida en el instante i-ésimo es $F_B(i)= F_A(i) + F_A(i-1)$

a) Determine un modelo markoviano de F_B y calcule la entropía de F_B (asúmase que F_B tiene memoria 1)
b) Calcule la eficiencia de una codificación de Huffman de F_B

PROBLEMA 3 (25%)

Un generador de secuencias pseudoaleatorias LFSR tiene un polinomio de conexiones *c(D)* de grado 4. Se inicializa con el estado 1, y al cabo de 12 iteraciones vuelve a alcanzar el mismo estado. ¿Pueden asegurarse las siguientes afirmaciones?

a) c(D) es un polinomio primitivo
b) c(D) es un polinomio irreducible
c) c(D) es divisor de $D^{24}+1$