Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS (GRUPO 50)

24 de Mayo de 2002

NOTAS IMPORTANTES:

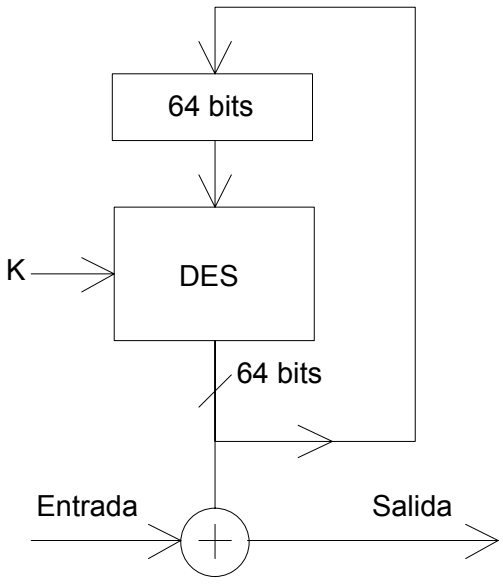
1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
2.- *Se valorará la justificación, discusión y claridad de los resultados.*
3.- ***Los resultados no reflejados en la hoja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

Se pretende diseñar un sistema de transmisión de datos, que realice compresión, cifrado y codificación de canal. Se ha realizado un estudio de los ataques posibles y se considera que es factible un ataque activo por parte del enemigo. Los comunicantes confían el uno en el otro.

Se ha estudiado la fuente que emite dos símbolos (A y B), quedando completamente caracterizada por las siguientes probabilidades de emisión condicionadas:

$$p(A/A) = 0.8$$
$$p(B/B) = 0.25$$

El canal no tiene memoria y presenta una tasa de error de bit nativa de $Pe=0.6\ 10^{-4}$. Como protección se pretende utilizar un código corrector (7,4) conjuntamente con un CRC de 32 bits.
Como mecanismo de cifrado de sesión se usa el mostrado en la figura y como función de hash se dispone del algoritmo SHA1.



SIGUE DETRÁS

Para implementar la gestión de claves *deben utilizarse los parámetros que se consideren convenientes de la siguiente tabla*, fijando la longitud del bloque a 20 bits y eligiendo entre Diffie-Hellman o RSA con el objetivo de proporcionar una mayor protección global al sistema (recuérdese que, a igualdad de tamaño, la complejidad del logaritmo discreto es mayor que la de la factorización).

Parámetros seleccionables para la gestión de claves	
Primo	**Elemento Primitivo GF(p)**
1048573	2
1048447	6
1019	53
997	7
Clave pública del receptor a utilizar (e)	Elegir el adecuado entre 3, 5 y 25

Se pide:

a) Entropía de la fuente, la codificación de Huffman de su extensión de orden 1 (agrupaciones de dos símbolos) y la longitud media de codificación que se obtendría. ¿Es conveniente realizar la extensión? ¿por qué? (**25%**)

b) ¿Debe utilizarse la función SHA1? ¿Y la firma digital? Dibújese el esquema del descifrador adecuado. El sistema de cifrado, ¿es síncrono o autosincronizante? Determínese la longitud efectiva máxima de la clave de sesión. Si el canal introduce un error, ¿cuántos errores se producen en media al descifrar? (**15%**)

c) Realice la elección de los parámetros adecuados de la tabla para la gestión de claves. Si se ha seleccionado RSA elija la clave pública del receptor de entre las que se proponen (si hay varias posibles seleccione la más pequeña), calcule la correspondiente clave secreta, realice los cálculos necesarios en el emisor para adoptar como clave de sesión 1234, dejando indicada la operación en el receptor. Si se ha seleccionado Diffie-Hellman use como semillas aleatorias $X_A=12$ y $X_B=6$ para establecer la clave de sesión conjunta. (**30%**)

d) Determine el formato y la longitud máxima de la trama de codificación si se exige que la tasa de retransmisiones sea como máximo de 10^{-6}. Especifique la estrategia de tratamiento de errores que debe llevarse a cabo. (**30%**)