

Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
CONTROL DE TRANSMISIÓN DE DATOS (GRUPO 40)
 24 de Mayo de 2002

NOTAS IMPORTANTES:

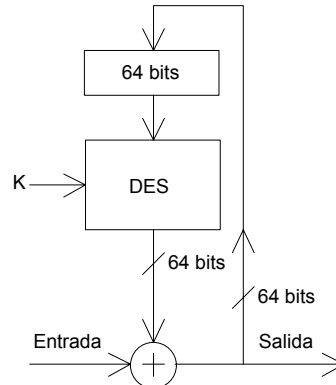
- 1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
- 2.- *Se valorará la justificación, discusión y claridad de los resultados.*
- 3.- ***Los resultados no reflejados en 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 sólo es factible un ataque pasivo por parte del enemigo. Los comunicantes confían el uno en el otro.

Se ha estudiado la fuente que emite 4 símbolos independientes (A, B, C y D) siendo sus probabilidades de emisión :

$$p(A) = P(B), \quad p(C) = 0.2, \quad P(D) = 0.1$$

Como mecanismo de cifrado de sesión se usa el mostrado en la figura y como función de hash se dispone del algoritmo SHA1.

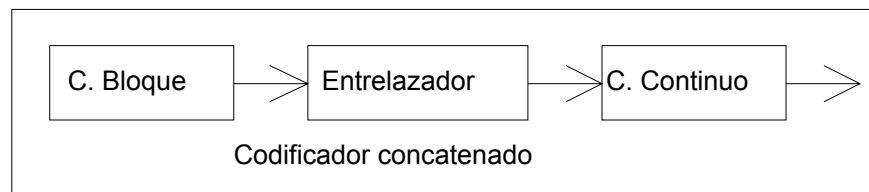


Para implementar la gestión de claves *deben utilizarse los parámetros que se consideren convenientes de la siguiente tabla*, fijando la longitud del bloque a 20 bits y eligiendo entre Diffie-Hellman o RSA con el objetivo de proporcionar una mayor protección global al sistema (recuérdese que, a igualdad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

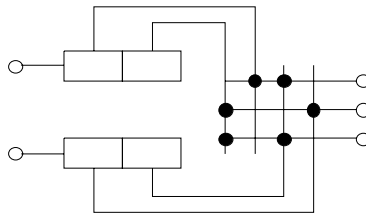
Parámetros seleccionables para la gestión de claves	
Primo	Elemento Primitivo GF(p)
1048573	2
1048447	6
1019	53
997	7
Clave pública del receptor a utilizar (e)	Elegir el adecuado entre 3, 5 y 25

SIGUE DETRÁS

El canal no tiene memoria y presenta una tasa de error de bit nativa de $P_e = 10^{-2}$. Como protección se pretende utilizar un código bloque conjuntamente con un código continuo según el siguiente esquema:



El codificador continuo es el siguiente:



Se pide:

- Entropía de la fuente, su codificación de Huffman y la longitud media de codificación. **(10%)**
- ¿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? **(20%)**
- 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 $X_A=23$ y $X_B=66$ para establecer la clave de sesión conjunta. **(30%)**
- Dibuje el diagrama de enrejado del codificador continuo (sólo es necesario especificar la relación *entrada/salida* para el primer estado). Si el modulador utilizado sin el codificador continuo era 4PSK, ¿cuál debe ser el nuevo modulador para que la introducción del código continuo no suponga una pérdida en la velocidad de transmisión al usuario? ¿Cómo se denomina esta técnica y explique brevemente en qué consiste? ¿Por qué se usa el entrelazador entre los dos codificadores? **(20%)**
- El código bloque opera con bloques de 204 octetos y es capaz de corregir 8 octetos erróneos en por bloque. Teniendo esto en cuenta, ¿el entrelazado debe hacerse a nivel de bit o a nivel de octeto? Suponiendo que la tasa de octetos erróneos a la salida del desentrelazador es de $P_E = 2 \cdot 10^{-4}$ y que resulta suficientemente profundo ¿cuál será la probabilidad de error de bit al usuario? **(20%)**