Ejercicio 1. Se desea realizar una comunicación de una entidad A a otra entidad B de forma que los servicios de seguridad diseñados garanticen la integridad del mensaje, la autoría del mensaje y la confidencialidad de la transmisión. Para dar estos servicios la entidades A y B disponen cada una de una clave secreta (K_{SA} y K_{SB}) y una clave pública (K_{PA} y K_{PB}) correspondientes al algoritmo RSA.

La información generada por la entidad A es un bloque de 7 bits cuyo valor es 1110110b (76h). La integridad de esta información se garantiza con una función resumen de 5 bits cuyo resultado para el valor de la información mencionado es 01111b (Fh). La firma digital se realiza con 5 bits a partir del valor obtenido en la función resumen.

El mensaje sobre el que se debe garantizar la confidencialidad en el canal de comunicaciones dispondrá de 12 bits. Los 5 bits de mayor peso se corresponden con los 5 bits resultantes de la firma digital y los 7 de menor peso con los 7 de la información.

a) Teniendo en cuenta que:

$$K_{PA} = (e,n) = (17,33) \; ; \; K_{SA} = (d,n) = (13,33)$$

a.1) Determine el valor de la firma digital.

a.2) Exprese en hexadecimal y en decimal el mensaje de 12 bits compuesto por A.

a.3) Demuestre que la elección realizada de las claves K_{PA} y K_{SA} permite que la firma digital sea de sólo 5 bits.

b) Sabiendo que los parámetros elegidos por la entidad B para calcular su clave pública K_{PB} y su clave secreta K_{SB} son:

$$p = 59, \; q = 83, \; e = 11$$

b.1) Si se considera un número primo grande a aquel que es mayor que 3, razone si la elección de p y q es acertada.

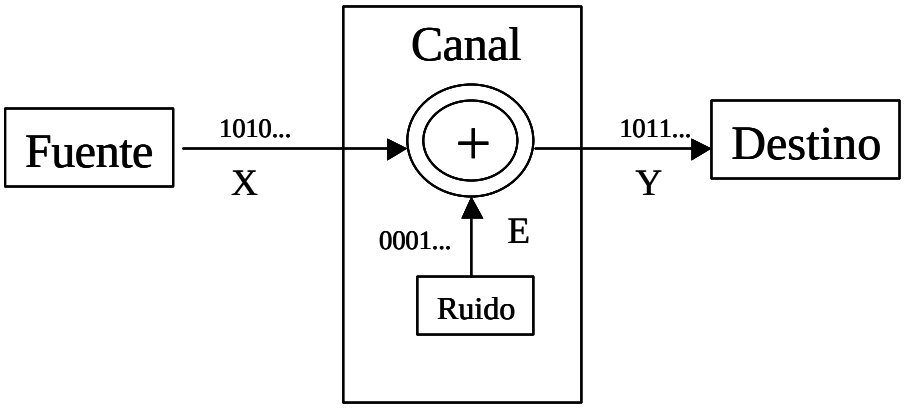
b.2) Razone por qué e tiene un valor adecuado teniendo en cuenta los valores de p y q elegidos.

b.3) Halle la clave secreta K_{SB}= (d, n)

b.4) Calcule cuál es el criptograma enviado por la entidad A a la entidad B. Exprese su valor en hexadecimal.

b.5) Comente cuál es el número de bits que se debe asignar a un criptograma en este sistema deacuerdo con las claves elegidas. (3 líneas)

Ejercicio 2. Una fuente binaria (X) emite símbolos sobre un canal de comunicación el cual se puede modelar a través de un generador de ruido binario (E) y una OR exclusiva. De esta forma, la secuencia binaria (Y) recibida en el destino es el resultado de la operación XOR bit a bit entre las emisiones de la fuente y las de la generación del ruido.



a) Si la fuente emite la secuencia 10110010 y el generador de ruido la secuencia 00001010, determine la secuencia recibida en el destino indicando los bits erróneos.

Sabiendo que la probabilidad de emisión de la fuente del símbolo 1 es p y la probabilidad de emisión del símbolo 1 del generador de ruido es q, calcule:

b) La probabilidad de que se reciba en el destino un 1, Pr(Y=1), y la probabilidad de que se reciba en el destino un 0, Pr(Y=0)
c) La entropía de la fuente, H(X), y la entropía del generador de ruido, H(E), para p=3/4 y q=1/8
d) La entropía de la secuencia recibida, H(Y), para p=3/4 y q=1/8
e) La entropía de la secuencia recibida condicionada al conocimiento de la secuencia emitida, H(Y/X), para p y q en general. Discuta el resultado obtenido (2 líneas)
f) La entropía mutua entre la secuencia enviada y la secuencia recibida, H(X,Y), para p=3/4 y q=1/8
g) La entropía de la secuencia enviada condicionada al conocimiento de la secuencia recibida, H(X/Y), para p=3/4 y q=1/8.
h) La información mutua entre la secuencia enviada y la secuencia recibida, I(X;Y), para p=3/4 y q=1/8.