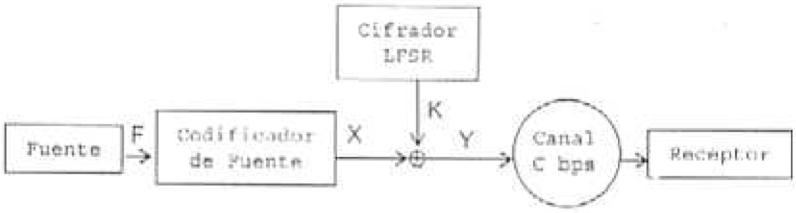
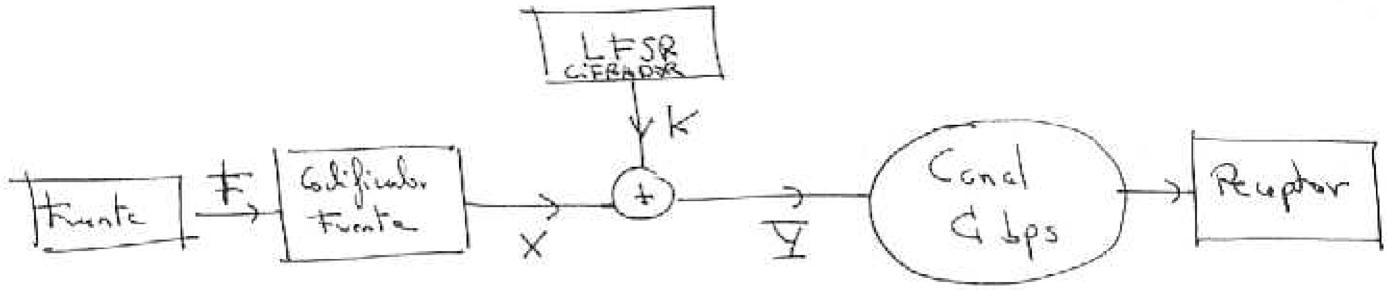
Ejercicio 1. Un sistema de transmisión de datos emplea un codificador de fuente y un cifrador en flujo basado en un simple LFSR. La fuente F que emplea el sistema carece de memoria y emite símbolos del alfabeto { A, B} cuyas probabilidades de generación son $p_A=0.9$ y $p_B=0.1$. La transmisión se realiza sobre un canal cuya capacidad es de C bps. La codificación binaria aplicada utiliza una extensión de fuente de orden 1 (concatenación de símbolos de 2 en 2) y el algoritmo de Huffman. El cifrador en flujo emite una secuencia cifrante K cuyos valores 1 y 0 son equiprobables. El flujo binario de salida del codificador de fuente se ha denominado X y el entregado al canal Y, resultado de X+K.



a) determine la entropia de la fuente H(F)
b) determine la entropia de la fuente extendida $H(F^2)$
c) halle la codificación de Huffman de la fuente extendida y calcule la eficiencia resultante $E_F{}^2$
d) para un canal con C=64Kbps determine la máxima velocidad de emisión de símbolos de la fuente por segundo (v_F) que acepta el sistema
e) calcule las siguientes entropias
   e.1) H(Y/X)
   e.2) H(Y/K)
   e.3) H(X, Y)
f) determine el valor de la información mutua I(X, K)
g) halle el grado mínimo del polinomio de conexiones del LFSR para garantizar en todos los casos la aleatoriedad de los mensajes cifrados de hasta 60 símbolos generados por F

Ejercicio



a) Fuente $\{A, B\}$ $\quad P_A = 0'9 \; ; \; P_B = 0'1$

$$H(F) = P_A \log_2 \frac{1}{P_A} + P_B \log_2 \frac{1}{P_B} = 0'469 \text{ bits/símbolo}$$

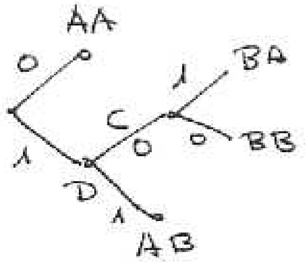
b) Fuente extendida $\quad F^2 = \{AA, AB, BA, BB\}$

$$H(F^2) = 2 \cdot H(F) = 0'938 \text{ bits/simb. ext.}$$

c) Huffman de F^2

$AA \rightarrow 0'81$
$AB \rightarrow 0'09$
$\left.\begin{array}{l} BA \rightarrow 0'09 \\ BB \rightarrow 0'01 \end{array}\right\} \rightarrow C \rightarrow 0'1$

$AA \rightarrow 0'81$
$\left.\begin{array}{l} C \rightarrow 0'1 \\ AB \rightarrow 0'09 \end{array}\right\} \rightarrow D \rightarrow 0'19$



Codificación:

$AA \rightarrow 0$
$AB \rightarrow 11$
$BA \rightarrow 101$
$BB \rightarrow 100$

$$L_{F^2} = 0'81 \cdot 1 + 0'09 \cdot 2 + 0'09 \cdot 3 + 0'01 \cdot 3 = 1'29 \text{ bits/s.e}$$

$$E_{F^2} = \frac{H(F^2)}{L_{F^2}} = \frac{0'938}{1'29} = 0'727 \qquad >> E_F = 0'4$$

d) $v_F = 1/T_F$, T_F = tiempo de símbolo de fuente.

$$\frac{L_{F^2}}{2T_F} = C \Rightarrow \frac{L_{F^2}}{2} \cdot v_F = C \Rightarrow v_F = \frac{2C}{L_{F^2}} = 992$$

Observación $\Rightarrow$ Con Huffman sin extensión $v_F = 64000$ sim/sg

e) Entropías, dado que X y K son independientes:

e.1) $H(Y/X) = H(K) = 1$ bit/símbolo binario

e.2) $H(Y/K) = H(X) = \frac{H(F^2)}{2} = H(F) = 0'469$ bits/si

Si se desea expresar en símbolos binarios:

$$H(Y/K) = H(F) = 0'469 \text{ bits/sim F} \cdot \frac{1 \text{ sim F}}{0'65 \text{ simb bin}}$$

$$H(Y/K) = 0'72 \text{ bits/sim binarios}$$

e.3) $H(X,Y) = H(X) + H(Y/X) = H(X) + H(K$

En las mismas unidades se suma:

$H(X,Y) = H(X) + H(K) = 0'72 + 1 = 1'72$ bits/po de símb binari

d) Información mutua.

$I(X,K) = H(X) - H(X/K) = 0$ (independientes)

f) - En el peor de los casos:

60 símbolos de fuente $\Rightarrow$ 90 bits

- El periodo del LFSR $\geq$ 90 bits

- El grado mínimo de $G(D)$ se obtiene cuando es primitivo y cumple:

$$2^m - 1 \geq 90 \Rightarrow m = 7$$

Ejercicio 2. Un sistema de firmas digitales utiliza RSA y como función resumen el algoritmo denominado El Gamal. Este algoritmo mantiene un valor x en secreto que debe ser custodiado de igual forma que la clave secreta K_s^{RSA} por la entidad firmante. La verificación de la firma de un mensaje m se lleva a cabo utilizando la clave pública K_P^{RSA} junto con una terna (g, y, p) que facilita la comprobación del mensaje recibido en concordancia con el resumen. En este sistema será necesario que se hagan públicas las claves K_P^{RSA} y las ternas (g, y, p) asociadas a cada entidad firmante. Considere que el resumen r se concatena a continuación del mensaje m de la forma m | r.
Complete el cálculo y la validación del resumen obtenido con el algoritmo El Gamal que se expone con los siguientes pasos:

1) Se determina un número primo p = 23 y dos números aleatorios g = 15 y x = 2.
2) Se deriva un valor y de la siguiente forma:

$$y = g^x \bmod p$$

a) determine el valor de y

3) Para hallar el resumen r de un mensaje m = 6 se genera un número aleatorio, coprimo con p-1, de valor z = 3. A partir de este número se deriva una primera parte del resumen, denominada a, mediante la expresión:

$$a = g^z \bmod p$$

b) calcule el valor de a

4) Se determina un valor auxiliar b' que es elemento inverso de z en el anillo Z_{p-1}

c) halle el valor de b'

5) Se completa el cálculo del resumen con un valor b en Z_{p-1} que verifica:

$$m = (x\,a + z\,b) \bmod (p-1)$$

el cual se obtiene de forma inmediata a través de su relación con b':

$$b = [(m - x\,a)\,b'] \bmod (p-1)$$

d) halle el valor de b

6) Se forma el resumen con la concatenación de los dos valores anteriores, r = a | b
7) La comprobación de un mensaje m se lleva a cabo en el receptor con el resumen r asociado, verificando la igualdad:

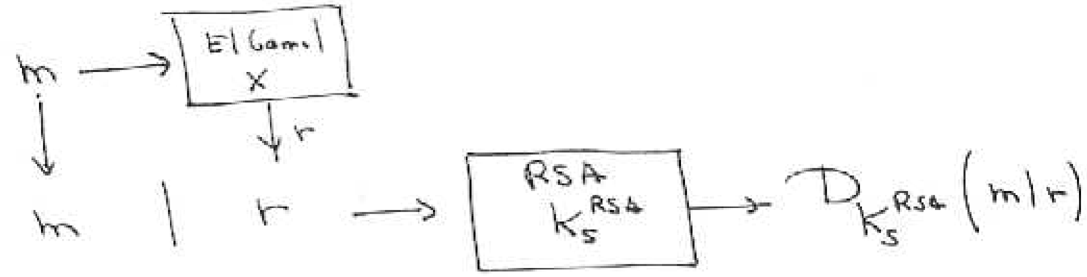
$$y^a a^b = g^m \bmod p$$

e) compruebe que los cálculos anteriores han sido correctos utilizando el mecanismo de comprobación del algoritmo
f) describa gráficamente el procedimiento de firma realizado por el emisor y por el receptor
g) razone brevemente (15 líneas) la validez de la función resumen propuesta

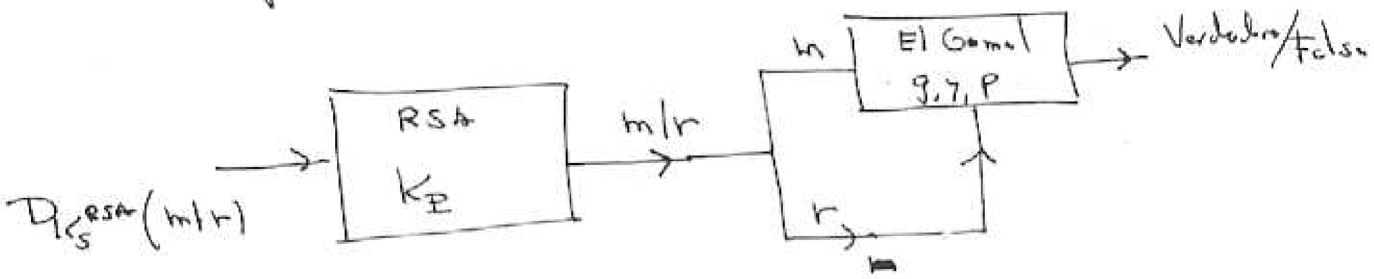
Ejercicio

①

Emisor



Receptor



- Se genera un número primo $p = 23$
- Se hallan dos números aleatorios $g = 15$ y $x = 2$
- Se deriva

$$y = g^x \bmod p$$

a) Determinar la terna pública (g, y, p)

$$y = 15^2 \bmod 23 = 18$$

Mensaje $m = 6$

- Se obtiene un aleatorio $z = 3$ coprimo con $p-1 = 22$
- Se deriva un valor

$$a = g^z \bmod p$$

- Se halla $b \in Z_{p-1}$ que verifica

$$m = (xa + zb) \bmod p-1$$

b) Calcular a:

$$a = 15^3 \bmod 23 = 17$$

c) Halle b' tal que

$$1 \equiv z \cdot b' \mod p-1$$

De forma equivalente:

$$1 = z \cdot b' + k(p-1)$$

$$1 = 3 \cdot b' + 22 \cdot k \Rightarrow \begin{cases} k = 1 \\ b' = -7 \equiv 15 \mod 22 \end{cases}$$

d) Dado que $b = (m - xa) \cdot b' \mod p-1$,

entonces, $b = (6 - 2 \cdot 17) \cdot 15 \mod 22 = 20$

e) $r = a | b = 17 | 20$

Comprobación, si se verifica $y^a a^b = g^m \mod p$ el resumen es correcto.

f) Comprobación

$$y^a a^b \equiv g^m \mod p$$

$$18^{17} \cdot 17^{20} \equiv 15^6 \mod 23$$

$$18^{17} = 18^{10001_2} = ((18^2)^2)^2 \cdot 18 \equiv 8 \mod 23$$

$$17^{20} = 17^{10100_2} = (((17^2)^2 \cdot 17)^2)^2 \equiv 16 \mod 23$$

Se verifica

$$\left.\begin{aligned} y^a \cdot a^b &\equiv 8 \cdot 16 \mod 23 = 13 \\ g^m &\equiv 15^6 \mod 23 = 13 \end{aligned}\right\} \underline{\text{OK}}$$

g) Validez de la función resumen propuesta

3

i) El resumen es de longitud fija con valor de bits necesario para concatenar a||b

ii) Dado m es fácil calcular r, aunque la exponenciación empleada puede ser computacionalmente lenta en algunos casos.

iii) Dado r es imposible en la práctica hallar m si no se conoce x

iv) Es poco probable que dos mensajes m y m' dé ~~a~~ lugar al mismo r. Se puede controlar la probabilidad en función del tamaño de m máx. y del valor de P.

v) Dado un m es prácticamente imposible hallar otro m' que cumpla $r(m) = r(m')$ si no se conoce x.