Jorge Mata

Ejercicio 1. Un sistema simple de clave pública utiliza una Entidad de Certificación (EC) para obtener las claves RSA de los servidores. Todas las claves empleadas en el sistema utilizan el mismo valor n = 33 por lo que las claves quedan definidas por el valor e que se expresa con 5 bits. La función resumen R(.) se obtiene a través de un LFSR cuyo polinomio de conexiones es $C(D)= D^5+D^4+D^3+D^2+1$. El resumen se deriva inicializando el LFSR con el valor binario de la clave e y se le hace operar un número de veces igual al valor de dicha clave.

$$R(e)=P^{(e)}(D) \quad \text{con } P^{(0)}(D)=e_4D^4+e_3D^3+e_2D^2+e_1D^1+e_0 \text{ y } e=e_4e_3e_2e_1e_0 \text{ en base 2}$$

El proceso para acceder desde un terminal a un servidor se inicia solicitando desde el terminal a la EC un certificado de 10 bits. El certificado se compone con los 5 bits de la clave pública del servidor y con los 5 bits de la firma generada por la EC del resumen de dicha clave. Una vez el terminal verifica la validez de la clave pública del servidor, la autenticación del usuario frente al servidor se realiza a través de login y password. El password es un número de identificación personal (PIN) de 4 dígitos que se envía cifrado al servidor dígito a dígito. El cifrado de cada dígito se lleva a cabo con su valor numérico incrementado en 2 unidades y aplicando RSA con la clave pública del servidor.

Para las claves:

1) Clave secreta del servidor: $Ks_{serv}=(d,n)=(3,33)$
2) Clave pública de la EC: $Kp_{EC}=(e,n)=(13,33)$

a) Halle la clave pública del servidor Kp_{serv} utilizando el algoritmo de Euclides extendido.
b) Calcule el valor decimale del resumen R(e) de la clave pública hallada Kp_{serv}.
c) Halle la clave secreta de la EC utilizando el algoritmo de Euclides extendido.
d) Determine el valor del certificado emitido por la EC correspondiente Kp_{serv} (exprese el resultado en binario y hexadecimal).
e) Obtenga los cuatro criptogramas enviados por un terminal para el PIN: 7007.

Ejercicio 2. Un sistema de transmisión de datos está compuesto por una fuente binaria X y un canal binario con borrados cuya salida denominaremos Y. La fuente emite el símbolo 0 con probabilidad α y el símbolo 1 con probabilidad $1-\alpha$. El canal se caracteriza por la matriz estocástica:

$$Q=\begin{pmatrix} 1-\rho & \rho & 0 \\ 0 & \rho & 1-\rho \end{pmatrix}$$

donde ρ es la probabilidad de recibir un borrado (B) a la salida del canal cuando se emite un símbolo binario (0, 1).

a) Halle la relación entre H(Y) y H(X). Razone el resultado obtenido para los casos $\rho=0$ y $\rho=1$.
b) Calcule H(X/Y).
c) Determine H(Y/X).
d) Indique cuál es el valor de la información mutua I(X;Y).
e) Especifique el cuál es el valor de la capacidad del canal con borrados en bits por símbolo.

Nota: Intente expresar los resultados utilizando la siguientes definiciones:

$$H(\alpha)\triangleq\alpha\log_2\left(\frac{1}{\alpha}\right)+(1-\alpha)\log_2\left(\frac{1}{1-\alpha}\right)$$

$$H(\rho)\triangleq\rho\log_2\left(\frac{1}{\rho}\right)+(1-\rho)\log_2\left(\frac{1}{1-\rho}\right)$$

Ejercicio 1

$K_{S_{Serv}} = (d, n) = (3, 33)$

$K_{P_{Ec}} = (e, n) = (13, 33)$

a) ¿ $K_{P_{Serv}}$?

$K_{P_{Serv}} = (e, n)$

$n = 3 \cdot 11 \Rightarrow \Phi(n) = 2 \cdot 10 = 20$

$de = 1 + k\,\Phi(n)$

$3e - 20k = 1$

Alg. Euclides

20	3	3	2
2	6	1	1

1) $20 \cdot 1 + 3 \cdot 0 = 20$

2) $20 \cdot 0 + 3 \cdot 1 = 3$

3) $20 \cdot 1 + 3 \cdot (-6) = 2$

4) $20(-1) + 3 \cdot (1 \cdot 6) = 1 \Rightarrow \begin{cases} k = +1 \\ e = 7 \end{cases} \Rightarrow \boxed{K_{P_{Serv}} = (7, 33)}$

b) $R(e) = P^{(e)}(D)$

$P^{(e)}(D) = D^e\, P^{(0)}(D) \bmod C(D)$

$P^{(0)}(D) = D^2 + D + 1$

$P^{(7)}(D) = D^7 \cdot (D^2 + D + 1) \bmod D^5 + D^4 + D^3 + D^2 + 1$

$e = 7$

$D^9 + D^8 + D^7 \;\big|\; D^5 + D^4 + D^3 + D^2 + 1$

$D^5 + D^4 + D^3 + D^2 + D \quad | \quad D^4 + D + 1$

$D^6 + D^4$

$D^6 + D^5 + D^4 + D^3 + D$

$D^5 + D^3 + D$

$D^5 + D^4 + D^3 + D^2 + 1$

$D^4 + D^2 + D + 1$

$\boxed{R(e) = 1\,0\,1\,1\,1_2 = 23}$

c) $K_{Sec} = (d, n)$ $K_{Pec} = (e, n) = (13, 33)$ (2)

$n = 3 \cdot 11 \Rightarrow \varphi(n) = 2 \cdot 10 = 20$

$13d - 20k = 1$

Alg. Euclides $20 = 1 \cdot 13 + 7$ $13 = 1 \cdot 7 + 6$ $7 = 1 \cdot 6 + 1$

(4) $20 \cdot 1 + 13 \cdot 0 = 20$
(3) $20 \cdot 0 + 13 \cdot 1 = 13$
(2) $20 \cdot 1 + 13 \cdot (-1) = 7$
(1) $20 \cdot (-1) + 13 \cdot (1+1) = 6$
(5) $20 \cdot (1+1) - 13 \cdot (-1-2) = 1 \Rightarrow$ $k = -2$, $d = -3 \equiv 17 \bmod 20$

$K_{Sec} = (17, 33)$

d) $Certificado = K_{P_{Serv}} \mid F_{K_{Sec}}(R(K_{P_{Serv}}))$

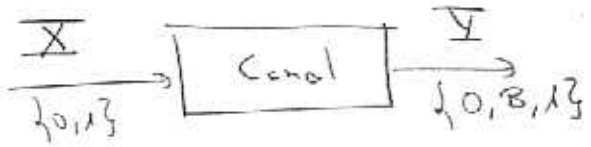
$F_{K_{Sec}}(23) = 23^{17} \bmod 33 = (((23^2)^2)^2) \cdot 23 \bmod 33 = 23 = 10111_B$

$Cert_{K_{P_{Ser}}} = F7h$

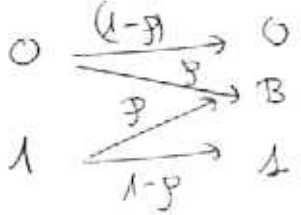
e) $PIN = 7007$ $C_i = (n+4)^e \bmod n = (n+4)^7 \bmod 33$

$C_1 = 9^7 \bmod 33 = 15$
$C_2 = 2^7 \bmod 33 = 29$
$C_3 = C_2 = 29$
$C_4 = C_1 = 15$

Ejercicio 2



$$Q = \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}$$



a) $H(X) = \alpha \log \frac{1}{\alpha} + (1-\alpha) \log \frac{1}{1-\alpha} = H(\alpha)$

$$H(Y) = \sum_{i \in \{0,B,1\}} P(Y=i) \log \frac{1}{P(Y=i)}$$

$P(Y=0) = (1-p) P(X=0) + 0 \cdot P(X=1) = (1-p)\alpha$

$P(Y=B) = p \cdot P(X=0) + p \cdot P(X=1) = p$

$P(Y=1) = 0 \cdot P(X=0) + (1-p) P(X=1) = (1-p)(1-\alpha)$

$$H(Y) = (1-p)\alpha \log \frac{1}{(1-p)\alpha} + p \log \frac{1}{p} + (1-p)(1-\alpha) \log \frac{1}{(1-p)(1-\alpha)}$$

$$H(Y) = (1-p)\alpha \left[\log \frac{1}{1-p} + \log \frac{1}{\alpha} \right] + p \log \frac{1}{p} +$$

$$(1-p)(1-\alpha) \left[\log \frac{1}{1-p} + \log \frac{1}{1-\alpha} \right] =$$

$$\alpha \left[(1-p) \log \frac{1}{1-p} \right] + (1-p) \left[\alpha \log \frac{1}{\alpha} \right] + p \log \frac{1}{p} +$$

$$+ (1-\alpha) \left[(1-p) \log \frac{1}{1-p} \right] + (1-p) \left[(1-\alpha) \log \frac{1}{1-\alpha} \right] = H(p) + (1-p) H(\alpha)$$

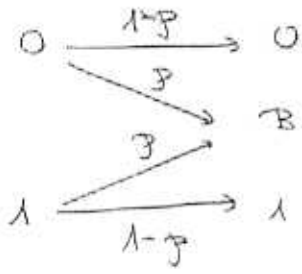
$$\boxed{H(Y) = H(p) + (1-p) H(\alpha)}$$

Si $p = 0 \Rightarrow H(Y) = H(\alpha) = H(X)$ canal sin errores

Si $p = 1 \Rightarrow H(Y) = \emptyset$ canal sin capacidad de transmisión
Siempre se recibe un borrón

b) $$H(X/Y) = \sum_{i \in \{0,B,1\}} P(Y=i) \sum_{j \in \{0,1\}} P(X=j/Y=i) \log \frac{1}{P(X=j/Y=i)}$$

$H(X/Y=i)$



$P(X=0/Y=0) = 1$
$P(X=1/Y=0) = 0$
$\Rightarrow H(X/Y=0) = \emptyset$

$P(X=0/Y=B) = \alpha$
$P(X=1/Y=B) = 1-\alpha$
$\Rightarrow H(X/Y=B) = H(\alpha)$

$P(X=\emptyset/Y=1) = 0$
$P(X=1/Y=1) = 1$
$\Rightarrow H(X/Y=1) = \emptyset$

$$\boxed{H(X/Y) = P(Y=B) \cdot H(\alpha) = p\,H(\alpha)}$$

c) $$H(Y/X) = \sum_{j \in \{0,1\}} P(X=j) \sum_{i \in \{0,B,1\}} P(Y=i/X=j) \log \frac{1}{P(Y=i/X=j)}$$

$H(Y/X=j)$

$$H(Y/X=0) = P(Y=0/X=0) \log \frac{1}{P(Y=0/X=0)} + P(Y=B/X=0) \log \frac{1}{P(Y=B/X=0)}$$

$$H(Y/X=0) = (1-p) \log \frac{1}{1-p} + p \log \frac{1}{1-p} = H(p)$$

$H(Y/X=1) = H(p)$ por simetría.

$$H(Y/X) = \alpha \cdot H(p) + (1-\alpha) H(p) = H(p)$$

$$\boxed{H(Y/X) = H(p)}$$

d) $I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X)$

Utilizando la primera expresión

$I(X;Y) = H(X) - H(X/Y) = H(\alpha) - p\,H(\alpha) = (1-p)\,H(\alpha)$

Con la segunda expresión también se obtiene:

$I(X;Y) = H(Y) - H(Y/X) = H(p) + (1-p)H(\alpha) - H(p)$

$$\boxed{I(X;Y) = (1-p)\,H(\alpha)}$$

e) $C = \max_{\alpha} (1-p)\,H(\alpha) = (1-p)\,H_{max}$

$H_{max} = 1$ cuando $\alpha = 1/2$

$$\boxed{C = (1-p) \text{ bits/simb}}$$