J. Mata

# Control de Transmisión de Datos

25/05/07

**Ejercicio 1.** En un sistema de comunicaciones inalámbrico los terminales se autentican utilizando un servidor central. Los terminales intercambian entre sí mensajes cortos de forma confidencial, utilizando el algoritmo RSA. Dado que los terminales no disponen de claves públicas, se genera de forma dinámica para cada sesión entre teminales A y B una clave $K_{P_{AB}} = (e_{AB}, n_{AB})$, donde $e_{AB}$ es de valor constante 11 y $n_{AB}$ es el producto de dos primos, $p_{AB}$ y $q_{AB}$. Los valores de dichos números primos se derivan utilizando, para cada uno de ellos, el mecanismo de operación Diffie-Hellman para compartir un secreto.

El intercambio de mensajes entre los terminales A y B para la compartición de un secreto ($p_{AB}$ y $q_{AB}$) se realiza utilizando el servidor central como intermediario. De esta forma, se garantiza la identidad entre los terminales. Los mensajes intercambiados se envían desde el terminal al servidor de forma confidencial utilizando la clave pública del servidor, $K_{\text{Serv}}$, correspondiente al algoritmo RSA. Cuando el servidor recibe el criptograma enviado por un terminal, lo descifra y lo retransmite al otro terminal.

Considerando que:

1) La operación del mecanismo Diffie-Hellman utiliza: $a = 5$ y $p = 97$

2) Los valores aleatorios generados por los terminales para el secreto compartido de cada número primo son:

- $p_{AB}$: Terminal A genera $x_1 = 2$ ; Terminal B genera $y_1 = 5$
- $q_{AB}$: Terminal A genera $x_2 = 7$ ; Terminal B genera $y_2 = 10$

3) La clave pública del servidor es: $K_{\text{Serv}} = (e, n) = (3, 319)$

determine:

a) El valor de los mensajes cifrados con RSA que se envían desde el terminal A al servidor para la generación de $p_{AB}$ y $q_{AB}$ respectivamente

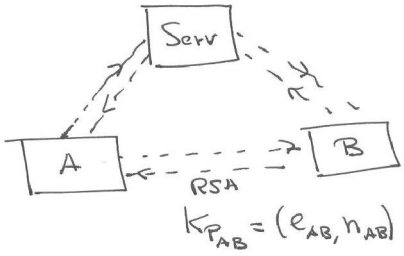
b) Los mensajes enviados en claro desde el servidor al terminal A para la generación de $p_{AB}$ y $q_{AB}$ respectivamente

c) La clave pública $K_{P_{AB}}$ de la sesión RSA entre los terminales A y B a partir de los mensajes recibidos por el terminal A y los números aleatorios generados por dicho terminal

d) La clave secreta de la sesión RSA entre los terminales

e) El criptograma enviado del terminal A al B cuando el mensaje en claro es 9

# Ejercicio 1




$e_{AB} = 11$

$n_{AB} = p_{AB} \cdot q_{AB}$

$p_{AB}$, $q_{AB}$ } Diffie-Hellman

1) Diffie-Hellman $a = 5$ y $p = 97$

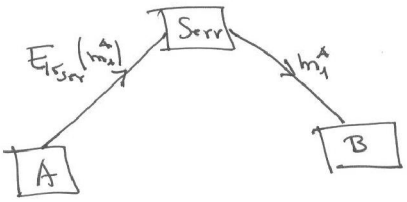
2)

| | $p_{AB}$ | $q_{AB}$ |
|---|---|---|
| A | $x_1 = 2$ | $x_2 = 7$ |
| B | $y_1 = 5$ | $y_2 = 10$ |

3) $K_{Serv} = (e, n) = (3, 319)$

a) Mensajes cifrados RSA desde A al servidor

Para $p_{AB}$:




$$m_1^A = a^{x_1} \bmod p = 5^2 \bmod 97 = 25$$

Para $q_{AB}$:

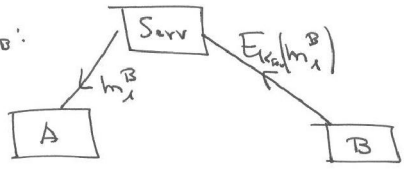
$$m_2^A = a^{x_2} \bmod p = 5^7 \bmod 97 = 40$$

Criptogramas:

$$c_1^A = (m_1^A)^e \bmod n = 25^3 \bmod 319 = 313$$

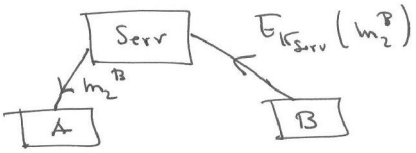
$$c_2^A = (m_2^A)^e \bmod n = 40^3 \bmod 319 = 200$$

b) Para $p_{AB}$:



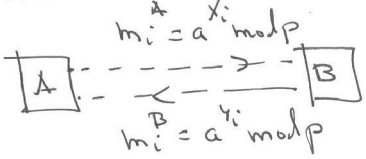

$$m_1^B = a^{y_1} \bmod p = 5^5 \bmod 97 = 21$$

Para $q_{AB}$:




$$m_2^B = a^{y_2} \bmod p = 5^{10} \bmod 97 = 53$$

c) Indirectamente entre A y B se ha hecho el intercambio




El secreto compartido es:

$$S_i = \left(m_i^A\right)^{y_i} \bmod p = \left(m_i^B\right)^{x_i} \bmod p = a^{x_i \cdot y_i} \bmod p$$

$$S_1 = p_{AB} = \left(m_1^B\right)^{y_1} \bmod p = 21^2 \bmod 97 = 53$$

$$S_2 = q_{AB} = \left(m_2^B\right)^{y_1} \bmod p = 53^7 \bmod 97 = 3$$

$$n_{AB} = p_{AB} \cdot q_{AB} = 53 \cdot 3 = 159$$

$$K_{P_{AB}} = (e_{AB}, n_{AB}) = (11, 159)$$

d) $K_s = (d, n)$

$e \cdot d + k \cdot \phi(n) = 1$

$\phi(n) = (p_{AB} - 1)(q_{AB} - 1) = 52 \cdot 2 = 104$

$11 \cdot d + 104 \cdot k = 1$

Algoritmo de Euclides extendido:

(1) $104 \cdot 1 + 11 \cdot 0 = 104$ | $104 = 11 \cdot 9 + 5$

(2) $104 \cdot 0 + 11 \cdot 1 = 11$ | $11 = 5 \cdot 2 + 1$

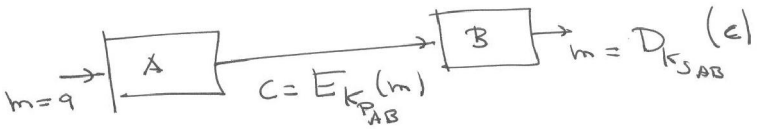
(3) $104 + (-9) \cdot 11 = 5$ ← (1) − (2) · 9

(4) $(-2) \cdot 104 + (1 + 18) \cdot 11 = 1$ ← (2) − (3) · 2

$k = -2$

$d = 19 \bmod 104 = 19 \Rightarrow K_{S_{AB}} = (19, 159)$

e)




$C = m^{e_{AB}} \bmod n_{AB} = 9^{11} \bmod 159 = 123$

**Ejercicio 2.** Un fuente binaria con memoria 1 se modela con una cadena de Markov. La fuente emite símbolos del alfabeto $\{0, 1\}$ y las probabilidades de transición entre estados son:

$$p_{0/1} = 0.3; p_{1/0} = 0.4$$

La fuente transmite los símbolos sobre un canal binario simétrico con ancho de banda $W = 1\,\text{KHz}$ y $P_e = 0.06$. La relación S/N a la salida del canal es 3 (en lineal).

a) Determine la entropía de la fuente con memoria.

b) Calcule la entropía a la salida del canal.

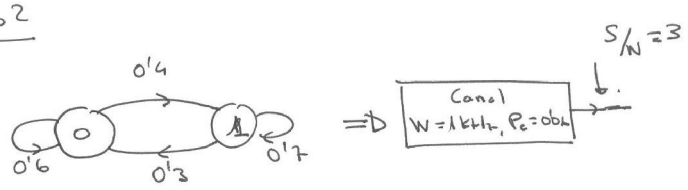
c) Suponiendo un codificador de fuente ideal, halle el máximo número de símbolos que la fuente puede transmitir de forma fiable por el canal durante un tiempo de observación, $T_{\text{obs}}$, de 5 segundos cuando se explota toda la capacidad del enlace.

d) Definiendo la eficiencia de explotación del canal cuando se emplea la mayor velocidad de transmisión fiable como:

$$\nu = \frac{\text{número de simbolos transmitidos en un } T_{\text{obs}}}{\text{máximo número de simbolos transmitidos en un } T_{\text{obs}}}$$

determine el valor de la eficiencia definida para un codificador de fuente cuya longitud media de codificación es $L = 0.95$. (Utilice los valores del apartado anterior como referencia.)

## Ejercicio 2




a) Definiendo $S_{n-1}$ el último estado de la fuente.

$$H(F) = H\left(F/_{S_{n-1}=0}\right)\cdot P(0) + H\left(F/_{S_{n-1}=1}\right)\cdot P(1)$$

$$H\left(F/_{S_{n-1}=0}\right) = H(0'6) = \frac{1}{0'6}\log_2\frac{1}{0'6} + \frac{1}{0'4}\log_2\left(\frac{1}{0'4}\right) = 0'97$$

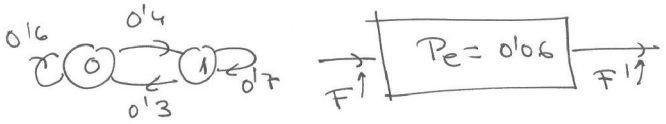
$$H\left(F/_{S_{n-1}=0}\right) = H(0'7) = \frac{1}{0'7}\log_2\frac{1}{0'7} + \frac{1}{0'3}\log_2\left(\frac{1}{0'3}\right) = 0'88$$

Balance de flujos y suma de probabilidades

$$\begin{cases} 0'4\cdot P(0) = 0'3\,P(1) \Rightarrow P(0) = \frac{3}{4}P(1) \\ P(0)+P(1)=1 \Rightarrow P(1)=\frac{4}{7},\ P(0)=\frac{3}{7} \end{cases}$$

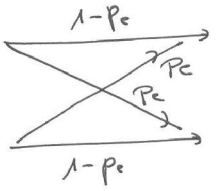
$$H(F) = \frac{3}{7}\cdot 0'97 + \frac{4}{7}\,0'88 = 0'9185 \ \text{bits/simb.}$$

b)




$$H(F') = H\left(F'/_{S_{n-1}=0}\right)P(0) + H\left(F'/_{S_{n-1}=1}\right)\cdot P(1)$$

Para $S_{n-1}=0$

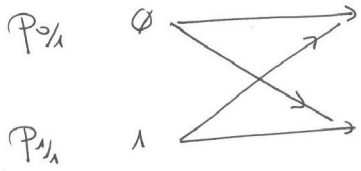



$P_{0/0}$ → 0: $P_{0/0}(1-P_e) + P_{1/0}P_e = 0'588$

$P_{1/0}$ → 1: $P_{1/0}(1-P_e) + P_{0/0}P_e = 0'412$

$$H\left(F'/_{S_{n-1}=0}\right) = H(0'588) = 0'9647$$

Para $S_{n-1} = 1$



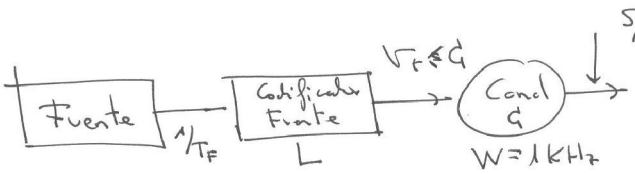

$P_{0/1}(1-p_e) + P_{1/1}p_e = 0'324$

$P_{1/1}(1-p_e) + P_{0/1}p_e = 0'676$

$$H\left(F'/_{S_{n-1}=1}\right) = H(0'324) = 0'9087$$

$$H(F') = \frac{3}{7}\,0'9647 + \frac{4}{7}\,0'9087 = 0'9327 \text{ bits/símb.}$$

c)




$L = H$ codificador ideal

$T_{obs} = 5$ s.

$V_t = C = W \log_2(1 + S/N) = 1000 \cdot 2 = 2000$ bit/s.

↑ máxima velocidad.

$$T_{F\,mínimo} = \frac{L}{V_t} = \frac{H}{C}$$

$$\text{Nº de símbolos máximo} = \frac{T_{obs}}{T_{F\,min}} = \frac{T_{obs}}{H/C} = \frac{C \cdot T_{obs}}{H} = 10887'31$$

d)

$$\eta = \frac{\text{nº de símbolos en } T_{obs}}{\text{máximo número de símbolos}} = \frac{T_{obs}/L/v_t}{T_{obs}/H/c}$$

$$\eta = \frac{v_t/L}{c/H} = \frac{H}{L} \cdot \frac{v_t}{c}$$

Si: $v_t = c$ para mayor velocidad física.

$$\eta\Big|_{v_t=c} = \frac{H}{L} = \frac{0'9185}{0'95} = 0'9668$$

eficiencia del codificador