CONTROL DE TRANSMISIÓN DE DATOS 5/12/02 GRUPO 40

PROBLEMA 1

$n = 499 \cdot 439 = 219061$ e 17 $\phi(n) = (p-1)(q-1) = 218124$

$\lambda(n) = \phi(n) / mcd(p-1, q-1) = 218124/6 = 36353$

a) $\lambda(n) = \dfrac{\phi(n)}{mcd(p-1, q-1)}$ $\left.\begin{array}{l} \cdot p, q \text{ primos impares} \\ p-1 = 2p' \\ q-1 = 2q' \end{array}\right\} \Rightarrow mcd(p-1, q-1) \geq 2 \Rightarrow \geq \dfrac{\phi(n)}{2}$

b) $ed = k\lambda(n) + 1 \Rightarrow$

	353	$0 \cdot 17$	36353
0	353	$+ 1$ 17	17
		$-2138 \cdot 17$	8

$4277 \; 7 = 1 \Rightarrow d_0 = 4277$

$d_i \; d_0 + k\lambda(n) \; i = 0 \ldots 5 \Rightarrow d_i = 4277, 40631, 76985, 113339, 149693, 186047$

c) Solo hay una firma por mensaje (los exponentes privados son equivalentes)

d) $FIRMA = M, h(M)^d \bmod n = M, 12344^{4277} \bmod 219061 \quad M, 138336$

Cálculo $4277 = 1000010110101_b$

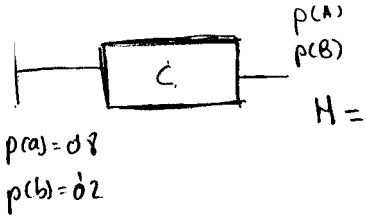
$((((((12344)^{2 \cdot 2222} 12344)^{22} 1234)^2 1234)^{2 \cdot 2} \cdot 1234)^2 1234 = 138336 \mod 219061$

Número esperado de mensajes de 1024 bytes con igual firma $= \dfrac{2^{8 \cdot 1024}}{2^{16}} \; 2^{8176}$

PROBLEMA 2

Si el polinomio de conexiones es irreducible todos los ciclos han de ser divisores de $2^4 - 1 = 2^5 - 1 = 31$. Puesto que es primo sus únicos divisores son 1 (estado "cero") y 31, todos han de ser primitivos.

1 F



$H = 0'8267 \text{ bits/simb} = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}$

$\Rightarrow \quad x = (0'8267 - (1-x) \log_2 \frac{1}{1-x}) / \log_2 1/x \quad \Rightarrow$ Función iterativa

$0'5 \rightarrow 0'3267 \rightarrow 0'274147 \rightarrow 0'2631 \rightarrow 0'26066 \rightarrow \boxed{0'260}$ punto fijo

$P(A) = 1 - 0'26 = 0'74 \; ; \; p(B) = 0'26$

$0'74 = p(A) = p(a)(1-pe) + p(b)pe \qquad 0'8(1-pe) + 0'2\,pe \Rightarrow \underline{pe = 0'1}$