UNIVERSITAT POLITÈCNICA DE CATALUNYA

E.T.S. d'Enginyeria de Telecomunicació de Barcelona
E.T.S. d'Enginyers de Camins, Canals i Ports de Barcelona
Facultat d'Informàtica de Barcelona

Titulació
Assignatura
Cognoms
Nom
Pàgina 1 de 2
DNI

① $0<m_1<n_1$; $0<m_2<n_1$

$am_1+b \equiv_{n_1} am_2+b$, $am_1 \equiv_{n_1} am_2$ (no hay condición para b)

$a(m_1-m_2) \equiv_{n_1} 0$, $n_1 \mid a(m_1-m_2)$, $n_1 \mid (m_1-m_2)$ si mcd $(a,n_1)=1$.

y $(m_1-m_2)<n_1$ por ser m_1, m_2 inferiores a $n_1 \Rightarrow m_1=m_2$. Un criptograma concreto es generado a partir de un único mensaje.

② $a \in CRR_{n_1}$, $\phi(n_1)=58\cdot 96=5568$ diferentes
$b \in \mathbb{Z}_{n_1}$, $n_1=5723$ diferentes
} $n_1\,\phi(n_1)=31865664$ claves

③ $(545\cdot 55+4460) \bmod 5723 = 97$

④ $n_2=s\cdot t^e$, mcd $(s,t^e)=1$, s un número compuesto

$t^{\phi(n_2)} \bmod s = t^{\phi(s)\phi(t^e)} \bmod s = (\underbrace{t^{\phi(s)} \bmod s}_{\text{como mcd}(t,s)=1\text{, por Euler vale } 1})^{\phi(t^e)} \bmod s = 1.$

$\Rightarrow t^{\phi(n_2)} = Ks+1$ (algún K).

$t^e t^{\phi(n_2)} \bmod n_2 = t^e(Ks+1) \bmod n_2 = (K\underbrace{t^e s}_{n_2}+t^e) \bmod n_2 = t^e \bmod n_2$
$= t^e$ ∎

⑤ $\phi(59^2\cdot 97)=328512$, $c_1 \equiv_{n_2} 97^{328517} \equiv_{n_2} 97^{\phi(n_2)+15} \equiv_{n_2} 97^{\phi(n_2)+1}\cdot 97^4$

$\equiv_{n_2} 97\cdot 97^4 \equiv_{n_2} 97^5 \equiv_{n_2} 47433$

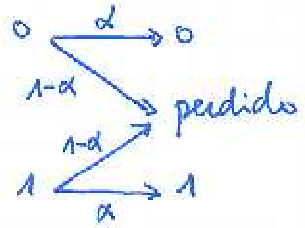
⑥ c_A múltiplo de t^e, c_A^e múltiplo de t^e, ¿ $c_A^e \bmod n_2 = c_1$ múltiplo de t^e?

Sea $c_A^e = k_2 t^e$ y $k_2 = k_3 s + (k_2 \bmod s)$, entonces:

$c_A^e \equiv_{n_2} k_2 t^e \equiv_{n_2} k_3\underbrace{t^e s}_{n_2} + (k_2 \bmod s)t^e = \underbrace{(k_2 \bmod s)}_{\text{menor a } s} t^e \Rightarrow$ múltiplo de t^e.

		7	2	3	8	
337657	47433	5626	2425	776	$\boxed{97}$	0

(7)



$C = \max_{p(x)} H(Y) - H(Y/X)$

$H(Y/X) = H(Y/X=0) = H(Y/X=1) = H(\alpha)$.

$P(Y=0) = \alpha p_0$, $P(Y=1) = \alpha p_1$, $P(Y=\text{perdido}) = (1-\alpha)$

con $P(X=0) = p_0$ y $P(X=1) = p_1$.

$\to H(Y) = -(\alpha p_0 \log \alpha p_0 + \alpha p_1 \log \alpha p_1 + (1-\alpha)\log(1-\alpha))$

$= -(\underbrace{\alpha p_0 \log p_0 + \alpha p_1 \log p_1}_{-\alpha H(p_0)} + \underbrace{\alpha p_0 \log \alpha + \alpha p_1 \log \alpha + (1-\alpha)\log(1-\alpha)}_{-H(\alpha)})$

$= \alpha H(p_0) + H(\alpha) = \alpha + H(\alpha)$ si $p_0 = p_1 = 1/2$, $H(p_0) = 1$ para $H(Y)|_{\text{máx}}$.

$\to C = \alpha + H(\alpha) - H(\alpha) = \alpha$. Se pueden recuperar los α bits correctos que llegan.

(8)

328517	328512	1	131405	-131407
328512	5	65702	-2	131405
5	2	2	1	-2
2	$\boxed{1}$	2	0	1
	0			

$\to ed = K\phi(n_2) + 1$

$d = 131405$, $K = 131407$.

$(t^{\ell})^{ed} \equiv_{n_2} t^{\ell K \phi(n_2) + \ell} \equiv_{n_2} (t^{\ell K \phi(n_2)} \bmod s)\, t^{\ell}$ (ver apartado 4)

$\equiv_{n_2} ((\underbrace{t^{\phi(s)} \bmod s}_{1 \text{ por EULER}})^{\ell K \phi(t^{\ell})} \bmod s)\, t^{\ell} \equiv_{n_2} t^{\ell}$ ∎

(9) $c_1 \equiv_{n_1} am + b \to a^{-1}(c_1 - b) \equiv_{n_1} m \equiv_{n_1} 1873(97 - 4460) \equiv_{n_1} -8171899$

5723	55	104	-18	1873
55	3	18	1	-18
3	$\boxed{1}$	3	0	1
	0			

$\equiv_{n_1} -5178$

$\equiv_{n_1} 545$

(10)

1	2	3	4	5	6	7	8		
3	6	9	0	5	2	1	4	545	
6	9	0	3	2	1	4	3		
9	0	3	2	1	4	3	2		
0	3	2	1	4	3	2	1		
3	2	1	4	3	2	1	4		
2	1	4	3	2	1	4	5	240	→ 32145 14320003
1	4	3	2	1	4	5	1		
4	3	2	1	4	5	1	4		
3	2	1	4	5	1	4	3		
2	1	4	5	1	4	3	2		
1	4	5	1	4	3	2	0	823	
4	5	1	4	3	2	0	0		
5	1	4	3	2	0	0	0		
1	4	3	2	0	0	0	3		

(11) $p(A)$, $p(B)$ superiores a $p(C)$, $p(D)$, $p(E)$ → 3 opciones de asignación

A,B 1 dígito	0,1	0,2	1,2
C,D,E 2 dígitos	20,21,22	10,11,12	00,01,02
	opción 1	opción 2	opción 3

32145 14320003 → 10020111120111100200000010.

Opción 1 : 1,0,0,20,1,1,1,1,20,1,1,1,1,0,0,20,0,0,0,0,0,1,0, → 23 resultados.

Opción 2 : 10,0,2,0,11,11,2,0,11,11,0,0,2,0,0,0,0,0,0,10 → 20 resultados.

Opción 3 : 1,00,2,01,1,1,1,1,20,1,1,1,1,00,2,00,00,00,1,0! falta 1 dígito

la secuencia tiene 20 resultados → opción 2.

Por inspección : 10 → D, 0 → B, 2 → A, 11 → C, 12 → E.

$\bar{L} = 1 \cdot 0{,}6 + 2 \cdot 0{,}4 = 1.4$ dígitos ternarios/símbolo

$H = -(0.31 \log_3 0.31 + 0.29 \log_3 0.29 + 0.19 \log_3 0.19 + 0.19 \log_3 0.19 + 0.02 \log_3 0.02)$

$= 1.302887$ dígitos ternarios/símbolo

→ $E = H/\bar{L} = 0.9306$.

Consideraciones a otras soluciones:

① Multiplicar los elementos de $\mathbb{Z}_{n_1}$ por uno del CRR_{n_1} da como resultado una permutación de $\mathbb{Z}_{n_1}$.

④ $$q t^{\ell} \underset{\uparrow \text{TCR}}{\equiv_{n_2}} (\underbrace{q t^{\ell} \bmod t^{\ell}}_{0}) s (\underbrace{s^{-1} \bmod t^{\ell}}_{\text{existe}}) + (q t^{\ell} \bmod s) t^{\ell} (\underbrace{t^{-\ell} \bmod s}_{\text{existe}})$$

y $$q t^{\ell} \bmod s = t^{\ell} \cdot t^{\phi(n_2)} \bmod s = t^{\ell} ((\underbrace{t^{\phi(s)} \bmod s}_{1 \text{ por EULER}})^{\phi(t^{\ell})} \bmod s) \bmod s$$

$$\rightarrow q t^{\ell} \equiv_{n_2} (t^{\ell} \bmod s) t^{\ell} (t^{-\ell} \bmod s) \equiv_{n_2} (1 + q_2 s) t^{\ell} \quad (\text{algún } q_2)$$
$$\equiv_{n_2} t^{\ell} + q s t^{\ell} \equiv_{n_2} t^{\ell} + q n_2 \equiv_{n_2} t^{\ell} \quad ■$$

⑥ $$c_1^{e} = q t^{\ell}, \quad c_1 \underset{\uparrow \text{TCR}}{\equiv_{n_2}} (\underbrace{q t^{\ell} \bmod t^{\ell}}_{0}) s (s^{-1} \bmod t^{\ell}) + (q t^{\ell} \bmod s) t^{\ell} (t^{-\ell} \bmod s)$$
$$\equiv_{n_2} [(q t^{\ell} t^{-\ell} \bmod s) + q_2 s] t^{\ell} \quad (\text{algún } q_2)$$
$$\equiv_{n_2} (\underbrace{q \bmod s}_{\text{inferior a } n_2}) t^{\ell} \rightarrow c_1 \text{ es múltiplo de } t^{\ell} \quad ■$$

⑧ $$(t^{\ell})^{ed} \equiv_{n_2} t^{\ell + \ell K \phi(n_2)} \equiv_{n_2} t^{\ell + \phi(n_2)} t^{(\ell K - 1)\phi(n_2)} \equiv_{n_2} t^{\ell} t^{(\ell K - 1)\phi(n_2)}$$
$$\underset{\uparrow \text{repetir}}{\equiv_{n_2}} t^{\ell + \phi(n_2)} t^{(\ell K - 2)\phi(n_2)} \equiv_{n_2} t^{\ell} t^{(\ell K - 2)\phi(n_2)} \underbrace{\equiv_{n_2} \cdots \equiv_{n_2}}_{\text{repetir}} t^{\ell} \quad ■$$

⑪ Considerando $p(A) = 3/20$, $p(B) = 11/20$, $p(C) = 4/20$, $p(D) = 2/20$, $p(E) = 0$.

$\bar{L} = 1.3$ dígitos ternarios/símbolo

$H = 1.0609$ dígitos ternarios/símbolo

$E = H/\bar{L} = 0.816$.