Solución

① $c_1 = 40$

$n_1 = 799$

$\varphi(n_1) = 16 \cdot 46 = 736$

$e = 123$

		q	x	y
736	123	5	61	-365
123	121	1	-60	61
121	2	60	1	-60
2	1	2	0	1
	☺			

$\Rightarrow d_1 = -365 \equiv_{736} 371$

$m_1 = 40^{371} \bmod 799$

$\left\{ \begin{array}{l} \lambda(n_1) = mcm(16,46) = mcm(2^4, 2\cdot 23) = 16 \cdot 23 = 368 \\ \quad \Rightarrow \text{mal que menos ample } m^{368} \bmod n_1 = 1 \end{array} \right\}$

$m_1 = 40^{368+3} \bmod 799 = 40^3 \bmod 799 = \underline{\underline{80}}$

② $c_2 = 65$

$n_2 = 667$

$\varphi(n_2) = 22 \cdot 28 = 616$

$e = 123$

		q	x	y
616	123	5	1	-5
123	1	123	0	1
	☺			

$\Rightarrow d_2 = -5 \equiv_{616} 611$

$m_2 = 65^{-5} \bmod 667 = (65^{-1})^5 \bmod 667 = 65^{611} \bmod 667$

A) Calcular la inversa de 65 mod 667 y elevar a 5

B) Utilizar $\varphi(n_2) = 616$: $65^{616} \bmod 667 = 1 = \underline{65^{611}} \cdot 65^5 \bmod 667$

↳ es la inversa de $65^5 \bmod 667$

			q	x	y
A)	667	65	10	23	-236
	65	17	3	-6	23
	17	14	1	5	-6
	14	3	4	-1	5
	3	2	1	1	-1
	2	1	2	0	1
		☺			

$\Rightarrow (65^{-1})^5 \underset{667}{\equiv} (-236)^5 \underset{667}{\equiv} -5^8 1 \underset{667}{\equiv} 136$

B) $65^{-1} \equiv_{667} 103$

		q	x	y
667	103	6	-21	136
103	49	2	10	-21
49	7	9	-1	10
7	4	1	1	-1
4	1	4	0	1
	☺			

$\Rightarrow$ 136 //

③ $c_1 = m_3^e \bmod n_1 = 40$

$c_2 = m_3^e \bmod n_2 = 65$

$m_3^e \bmod n_1 n_2 = c_3 = c_1 n_2^{-1} n_2 + c_2 n_1^{-1} n_1 = 40 \cdot 115 \cdot 667 + 65 \cdot (-96) \cdot 799$

$= -1917560 \equiv_{n_1 n_2} 214172$ //

		q	x	y
799	667	1	-96	115
667	132	5	19	-96
132	7	18	-1	19
7	6	1	1	-1
6	1	6	0	1
	☺			

④ $m_1 = m_3 \bmod n_1$

$m_2 = m_3 \bmod n_2$

$m_3 \bmod n_1 n_2 = m_1 n_2^{-1} n_2 + m_2 n_1^{-1} n_1 = 80 \cdot 115 \cdot 667 + 136 \cdot (-76) \cdot 799$

$= -4295144 \equiv_{n_1 n_2} 501053$ //

(*)

⑤ e debe ser primo con $\varphi(n_1)$ y primo con $\varphi(n_2)$ para que tenga inversa mod $\varphi(n_1)$ y mod $\varphi(n_2)$. Obviamente será primo con $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$, puesto que es primo con cada una.

(*) Encontrar una clave c_3 de $m_3 \bmod n_1 n_2$ es laborioso ($214172 \bmod 532933$ — 122531)

⑥ 50105 → λ0λ 000 00λ 000 λ0λ 0λλ $= 2^{-1}+2^{-3}+2^{-9}+2^{-13}+2^{-15}+2^{-17}+2^{-18}$

$= 0.627117157$

1er paso : $0.627117157 \in [0.5782, 0.65)$ → índice 0.

2º paso : $\frac{0.627117157 - 0.5782}{(0.65 - 0.5782)} = 0.6812974573 \in [0.65, 0.7082)$

→ índice 11.

(convertir 0.627117157 a un intervalo $[0,1)$).

3er paso : $\frac{0.6812974573 - 0.65}{0.0582} = 0.5377568952 \in [0.52, 0.5782)$

→ índice 9.

4º paso y último (extensión de orden 4):

$\frac{0.5377568952 - 0.52}{0.0152} = 0.8051012921 \in [0.26, 0.3182)$

→ índice 5.

→ 10, 11, 9, 5

⑦ El intervalo para 10, 11, 9, 5 es:

$0.5782 + 0.65 * 0.0918 = 0.62487$

$0.62487 + 0.52 * 0.0582 * 0.0918 = 0.6270429552$

$0.6270429552 + 0.26 * (0.0582)^2 * 0.0918 = 0.6271061882$

→ $[0.6271061882,\ 0.6271061882 + \Delta)$ donde $\Delta = 0.0918 * (0.0582)^3$

$= 0.0000141574$

→ $[0.6271061882,\ 0.6271203422)$

50105 → $[0.627117157,\ 0.627117157 + 2^{-18}) =$

$[0.627117157,\ 0.627120957)$ no está incluido en el intervalo que codifica 10, 11, 9, 5

Si se envían varios mensajes seguidos puede haber confusión en recepción, puesto que no se garantiza la instantaneidad.

Como se envía un único mensaje, no hay problema, con enviar cualquier real del intervalo es suficiente.

50152 → $[0.6271133423,\ 0.6271171570)$ que es el intervalo de 10, 11, 9, 5

(8)

1. A
2. D
3. S
4. SG
5. Σ
6. SGO
7. SGOA
8. T
9. DE
10. SGOAT
11. SGOATS
12. SGOATSD
13. DET.

PASO 1: se lee 10 → (SGOAT) y es prefijo del siguiente

PASO 2: se lee 11 → como no está se debe tratar como caso "anormal" KWKWK.

LD KW = SGOAT
KWK = SGOATS ∉ al Diccionario → entrada 11.
→ (SGOATS) y es prefijo del siguiente

PASO 3: se lee 9 → (DE) y pasa la concatenación: SGOATSDE → SGOATSD ∉ al Diccionario → entrada 12
y DE es prefijo del siguiente

PASO 4: se lee 5 → (Σ) y pasa la concatenación: DEΣ, → DEΣ ∉ al Diccionario → entrada 13.

→ SGOATSGOATSDEΣ.

(9) φ^{-1}? $P = (8\ 11\ 5\ 7\ 10\ 2\ 3\ 4\ 1\ 13\ 14\ 6\ 12\ 9)$ Lee, por ejemplo, que en la posición 1 sale el símbolo nº 8. En φ^{-1} debería cumplirse que en la posición 8 salga el símbolo nº 1:

$$\varphi^{-1} = \begin{pmatrix} 9 & 6 & 7 & 8 & 3 & 12 & 4 & 1 & 14 & 5 & 2 & 13 & 10 & 11 \\ \text{posición} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \end{pmatrix}$$

(1 en posición 8 — ejemplo)

MENSAJE ORIGINAL = "AS GOOD AS IT GETS".

PUNTO DE RECUPERACIÓN

(6) 43504 → 0.5567626953

⇒ 9, 10, 12, 8

(7) Intervalo para 9, 10, 12, 8 → $[0.5567451135, 0.5567666656)$

Intervalo para 43504 → $[0.5567626953, 0.5567932129)$

$= 0.5567626953 + 2^{-15}$

Un posible número que ∈ al intervalo 9, 10, 12, 8 podría ser

$[0.5567626953, 0.5567626953 + 2^{-18})$ =

$= [0.5567626953, 0.5567669100)$ → 435040 .

(8)

1. A
2. D
3. S
4. U
5. I
6. QDG
7. QDGE
8. T
9. ID
10. QDGEA
11. IDO
12. QDGEAO
13. QDGEAOT

→ IDODGEAODGEAOT

(9) $\sigma^{-1} = (2\ 8\ 10\ 11\ 14\ 12\ 5\ 3\ 13\ 4\ 1\ 9\ 6\ 7)$

MENSAJE ORIGINAL = "DO GET A GOOD IDEA"