① $g^K \bmod n = g^{qt+K \bmod t} \bmod n = (g^t)^q \bmod n \; g^{K \bmod t} \bmod n$

→ $(g^t)^q \bmod n$ debería ser 1: { a) $q = 0$, para ello $K < t$
b) $t = \varphi(n) = 2^{3-1}(2-1)7^{2-1}(7-1) = 80$, y $g$ primo con $n$.

② ALG. EXTENDIDO DE EUCLIDES:

| | | | K | g | |
|---|---|---|---|---|---|
| 8451823 | 1342813 | 6 | 7 | -44 | $K = 7$, $g = -44$ |
| 1342813 | 394945 | 3 | -2 | 7 | $(7 \cdot 8451823 - 44 \cdot 1342813 =$ |
| 394945 | 157978 | 2 | 1 | -2 | $78989)$ |
| 157978 | 78989 | 2 | 0 | 1 | |
| 0 | | | | | |

(*) VER NOTA 1 AL FINAL

③ $a = g^{K \bmod t} \bmod n = -44^7 \bmod 200 = (-44)^{3 \cdot 2} \cdot (-44) \bmod 200$

Notar que $K < t$

$= (-184)^2 \cdot -44 \bmod 200 = -64 \bmod 200 = 136$ //

$b = g \cdot a^q \bmod n = 307 \cdot 136^{241} \bmod 200 = 107 \cdot (8 \cdot 17)^{241} \bmod 200$,

$= 107 \cdot 17 \cdot 8^{241} \bmod 200 = 19 \cdot 8^{241} \bmod 200$

$17^{\varphi(n)} \equiv_n 1$, 17 es primo con 200.

Se puede utilizar el método del campesino ruso para calcular $8^{241} \bmod 200$ pero notar que $2^{10} \bmod 200$ es inmediato e igual a 24 (es menor que $2^8 \equiv_{200} 112$). Por tanto:

$$2^{3(10 \cdot 24 + 1)} \underset{200}{\equiv} 24^{3 \cdot 24} \cdot 2^3 \underset{200}{\equiv} 24^{24} \cdot 2^3 \underset{200}{\equiv} 24^{3 \cdot 8} \cdot 2^3 \underset{200}{\equiv} 24^{3 \cdot 2} \cdot 24^2 \cdot 2^3$$

↑ 1ª operación

$$\underset{200}{\equiv} 24^2 \cdot 2^3 \underset{200}{\equiv} 176 \cdot 8 \underset{200}{\equiv} 8 \Rightarrow b = 19 \cdot 8 \bmod 200 = 152 \; ///.$$

↑ 2ª operación

(*) VER NOTA 2 AL FINAL

④ Consideramos $b_1, b_2 \neq 0$ (solución trivial)

$$\left.\begin{aligned} b_1 &= q_1 \cdot a^p \bmod n \neq 0 \\ b_2 &= q_2 \cdot a^p \bmod n \neq 0 \end{aligned}\right\} q_1, q_2 \text{ y } a^p \text{ no nulos ni múltiplos de } n.$$

$$\left.\begin{aligned} q_1 a^p &= c_1 n + b_1 \\ q_2 a^p &= c_2 n + b_2 \end{aligned}\right\} \text{si } b_1 = b_2 \rightarrow (q_1 - q_2) a^p = (c_1 - c_2) n$$

$$\Rightarrow (q_1 \bmod n - q_2 \bmod n)(a^p \bmod n) \bmod n = 0.$$

$$\qquad\quad \# \qquad\quad \# \qquad\quad \#$$

$$\qquad\quad 0 \qquad\quad 0 \qquad\quad 0$$

Como $a^p$ no es nulo ni múltiplo de $n$, sólo será cierto si $q_1 \equiv_n q_2$ //

En nuestro caso los primos de $P$ reducidos mod $n$ son $\{39, 41, 63, 107\}$, todos diferentes.

(*) VER NOTA 3 AL FINAL

⑤ $p = 241$, $q = 307$ } $n_{RSA} = 73987$, $\varphi(n_{RSA}) = 73440$

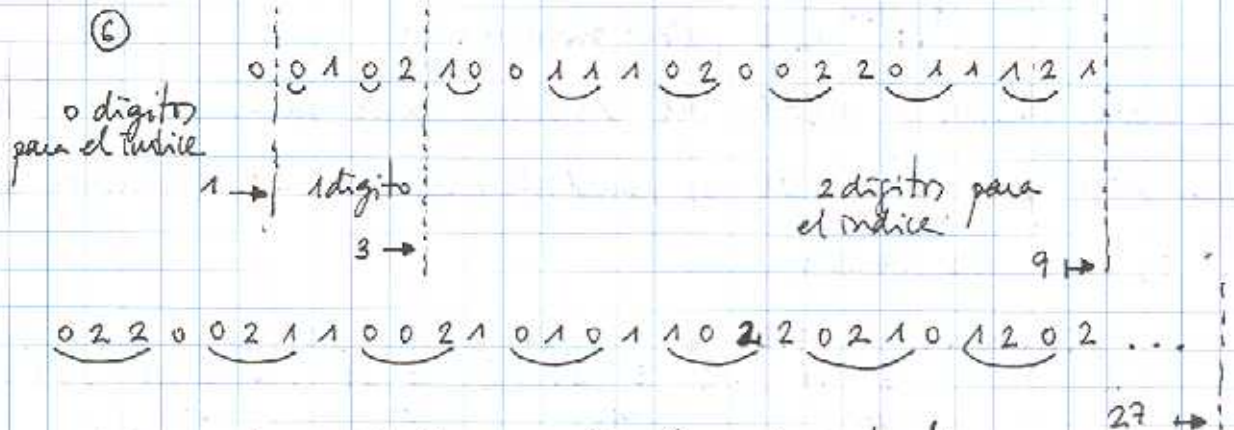
$e = 41$

$\rightarrow -9\varphi(n) + 16121 \cdot e = 1$

$\rightarrow d = 16121$ //.

| 73440 | 41 | 1791 | -9 | 16121 |
|---|---|---|---|---|
| 41 | 9 | 4 | 2 | -9 |
| 9 | 5 | 1 | -1 | 2 |
| 5 | 4 | 1 | 1 | -1 |
| 4 | 1 | 4 | 0 | 1 |
| | 0 | | | |

⑥




| | | |
|---|---|---|
| 0-NULL | 6-10 | 12-11 |
| 1-0 | 7-12 | 13-21 |
| 2-1 | 8-01 | 14-1212 |
| 3-2 | 9-2011 | 15-120 |
| 4-20 | 10-010 | 16-1202 |
| 5-201 | 11-121 | |

→ Es el parsing de la información: 012 202 011 012 012 011 010 121 112 112

121 201 202 ≡ 5, 20, 4, 5, 5, 4, 3, 16, 14, 14, 16, 19, 20

⇒ "ES DE ED CONNORS" //

⑦ NO ES NECESARIO ORDENAR

$P(112) = P_1^2 P_2 = 0.060016$ ; $\bar{F}(x) = F(x) - P(x)/2 = 0.030008$

$l(x) = \lceil \log_2 1/P(x) \rceil + 1 = 6$

$2^{-4} = 0.0625 > \bar{F}(x)$

$2^{-5} = 0.03125 > \bar{F}(x)$

$2^{-6} = 0.015625$ $\Rightarrow$ $000001 \in [0.015625, 0.03125)$ //

⑧ $\bar{F}(x) = 0.030008$, valor central del intervalo

Como se tienen símbolos ternarios se codificará $[\lfloor \bar{F}(x) \rfloor, \lfloor \bar{F}(x) \rfloor + D^{-l(x)})$

con $D = 3$.

$3^{-3} = 0.037037 > \bar{F}(x)$

$3^{-4} = 0.0123456 < \bar{F}(x)$

$2 \cdot 3^{-4} = 0.0246912 < \bar{F}(x)$ ; STE codifica $\lfloor \bar{F}(x) \rfloor$ como el más cercano a $\bar{F}(x)$

$\Rightarrow$ $0002 \in [0.0246912, 0.037037)$ //

Comprobación que $l(x) = 4$:

$\bar{F}(x) - \lfloor \bar{F}(x) \rfloor \leq P(x)/2$ , c. instantánea

$\bar{F}(x) - \lfloor \bar{F}(x) \rfloor \leq D^{-l(x)}$ , $\bar{F}(x)$ $\in$ al intervalo

$\rightarrow$ $D^{-l(x)} \leq P(x)/2$ $\rightarrow$ $l(x) \geq \log_D 1/P(x) + \log_D 2$ ; $l(x) = \left\lceil \log_D \frac{2}{P(x)} \right\rceil$

⑨ Para una codificación binaria: $H(S^n) \leq L_n \leq H(S^n) + 2$ = 4 //.

Recordar que el 2 se debe a $l(x) = \lceil \log_2 1/p(x) \rceil + 1$ (el techo y el 1)

Ahora nos quedará: $H_D(S^n) \leq L_n \leq H_D(S^n) + 1 + \log_D 2$

$\rightarrow$ $H_D(S) \leq \frac{L_n}{n} \leq H_D(S) + 1 + \log_D 2$ //.

(*) NOTAS (no necesarias para la resolución del problema)

NOTA 1. Tanto Aldous como Simon utilizan el algoritmo extendido de Euclides para calcular $g$ y $K$. Sin embargo, se podrían tener otros como $K=-10$ y $g=63$ puesto que $-10.8451823+63.1342813=78989$ //

Notar también que los $K$ y $g$ calculados son co-primos:

$$K(78989.107)+g(78989.17)=78989$$

$$107K+17g=1 \text{ //}$$

NOTA 2. El cálculo $8^{241} \bmod 200$ puede generalizarse:

Se desea calcular $a^s \bmod n$ con $\begin{cases} s = r\cdot\varphi(n)+1 \\ n = a\cdot b \\ mcd(a,b)=1 \quad \text{(factores de } n\text{)} \end{cases}$

$a^s \bmod n = v$ ?

① $a^s = q_1 \cdot n + v$

$a^s \bmod a = q_1 n \bmod a + v \bmod a \rightarrow v \bmod a = 0$.

② $a^s \bmod b = v \bmod b$

Notar que $a \in CRR$ de $b$ por ser co-primos ($a^\ell \in CRR$, $\ell$ entero)

Como $s = r\varphi(n)+1 = r\varphi(a)\varphi(b)+1$ se tiene:

$$[a^{r\varphi(a)}]^{\varphi(b)} \cdot a \bmod b = [a^\ell]^{\varphi(b)} \bmod b \cdot a \bmod b$$

$$= a \bmod b.$$

$\rightarrow v = q_2 b + a$.

Aplicando ①: $v \bmod a = 0 = q_2 b \bmod a \rightarrow q_2 = q_3 \cdot a$ (múltiplo puesto $a,b$ coprimos).

$\rightarrow v = q_3(ab) + a$, pero $v < ab \rightarrow q_3 = 0$, $\boxed{v = a}$

NOTA 3. Para calcular $q$ Simon realiza $ja^i \bmod n$ con $i,j \in \mathbb{P}$. Es necesario garantizar que todas las $b$ sean diferentes (puede comprobarse)

Pueden ser iguales si $q_1 a^{p_1} \equiv_n q_2 a^{p_2}$ (no se considera la solución nula)

Si $p_2 > p_1$, $q_1 a^{p_1} \equiv_n q_2 a^{p_1} a^{p_2-p_1} \rightarrow q_1/q_2 \equiv_n a^{(p_2-p_1)}$ ($q_2$ tiene inversa por ser coprimo con $n$).

Esta condición no se cumple para los datos del problema.