① Por inspección puede verse que, por ejemplo, la emisión del símbolo A depende del estado ($P(A/G)=0$) //

② Hay que resolver la cadena:

$$p_A = 0.5 p_U \rightarrow 2p_A = p_U$$

$$p_G = 0.2 p_C \rightarrow 5p_G = p_C$$

$$0.3 p_U = 0.7 p_A + 0.6 p_G \rightarrow 10 p_A = 7p_A + 6p_G \rightarrow p_A = 2p_G$$

$$p_G = \frac{1}{(1+5+2+4)} = 1/12 \quad ; \quad p_U = 4p_G = 1/3 \quad ; \quad p_A = 1/6 \quad ; \quad p_C = 5/12$$

$$H(X_2|X_1) = H(X_2|X_1=A)\, p_A + \ldots = 0.8619308 \text{ bits/símbolo} \; //$$

(memoria de orden 1)

$$H(X_2|X_1=A) = H(0.7) = 0.88129$$

$$H(X_2|X_1=U) = H(0.5) = 1$$

$$H(X_2|X_1=C) = H(0.2) = 0.721928$$

$$H(X_2|X_1=G) = H(0.6) = 0.97095$$

③

K \ m	A	C	G	U
A	A	C	G	U
C	C	G	U	A
G	G	U	A	C
U	U	A	C	G

m: G G A G G C G G G G G U
K: G U A C G U A C G U A C

C: A C A U A A G U A C G A //

④ K_s es única en $\mathbb{Z}_{n_1 n_2 n_3 n_4}$ y es:

$$K_s \underset{n_1 n_2 n_3 n_4}{\equiv} 33 \cdot \underbrace{(3 \cdot 29 \cdot 5 \cdot 17 \cdot 7 \cdot 13)}_{672945} \underbrace{672945^{-1}}_{\text{inversa mod}(2\cdot 31)} + 22 \cdot 479570 \cdot \underbrace{(479570)^{-1}}_{\text{inversa mod } 87} +$$

$$+ 13 \cdot 490854 \cdot \underbrace{(490854)^{-1}}_{\text{inversa mod } 85} + 75 \cdot 458490 \cdot \underbrace{(458490)^{-1}}_{\text{inversa mod } 91}$$

458490	91	5038	$\boxed{37}$	-186419
91	32	2	-13	37
32	27	1	11	-13
27	5	5	-2	11
5	2	2	1	-2
2	$\boxed{1}$	2	0	1
	0			

$\rightarrow K_S \equiv_{n_1 n_2 n_3 n_4} 725977873 \equiv 1669384$

(VER NOTA1 al final)

⑤ $16693843^{1693} \bmod n_1 n_2 = 4807^{1693} \bmod n_1 n_2$

Si 4807 es primo con $n_1 n_2 = 5394$ podemos utilizar el Tª de Euler:

	1	8	5	3	2	7	2	
5394	4807	587	111	32	15	2	$\boxed{1}$	0

y $\phi(5394) = 1 \cdot 30 \cdot 2 \cdot 28 = 1680$

$4807^{1693} \bmod 5394 = 4807^{13} \bmod 5394$

$= ((4747)^2 4747)^2 4807 \bmod 5394 = 4441$

$4807^2 \bmod 5394 = 4747$.

Y d será:

1693	1680	1	517	-521
1680	13	129	-4	517
13	3	4	1	-4
3	$\boxed{1}$	3	0	1
	0			

$\rightarrow d = 517$

⑥ n_2 y n_4 compartirían un factor $\rightarrow$ calcular el $mcd(n_2, n_4)$ y luego extraer los 2 factores que faltan:

$mcd(n_2, n_4) = 13 \rightarrow n_2/13 = 11$ y $n_4/13 = 7$

⑦ $K_t = K_S \bmod \underbrace{n_1 n_2}_{n} = 4807$, hay n posibles K_S, y por cada una de ellas hay $\phi(n)$ posibles d, que configuran de forma correcta las claves del resto de pasos del algoritmo:

$n\phi(n) = 9061920$ claves diferentes

(VER NOTA2 al final)

(8) Multiplicar el CRR$_n$ por uno de sus elementos genera una permutación del CRR$_n$. Como $d \in CRR_n$ entonces $d^2 \in CRR_n$, por lo que $d^3 \in CRR_n, \dots, d^t \in CRR_n$.

Para que sean diferentes debe cumplirse que $ord_n(d) \geq t$.

El número máximo de valores diferentes es precisamente el número de elementos del CRR$_n$, es decir, $\phi(n)$ (en este caso d sería una raíz primitiva).

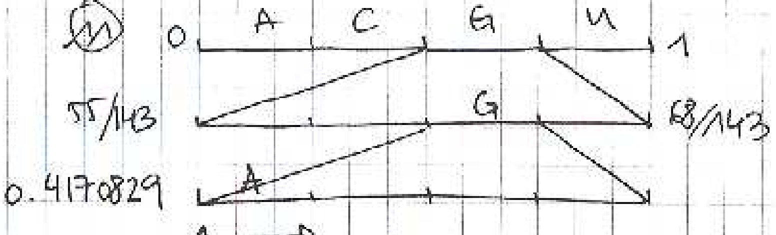
(9) Multiplicar $\mathbb{Z}_n$ por un elemento del CRR$_n$ genera una permutación de $\mathbb{Z}_n$. Si $K_S \in \mathbb{Z}_n$ podría ser que $K_S d \equiv_n 0$. Para evitarlo podríamos elegir K_S tal que $\in CRR_n$.

(VER NOTA 3 al final).

(10)

	A	C	G	U
4807	32/143	23/143	13/143	75/143
$4807 \cdot 577 \equiv_n 3979$	11/210	64/210	69/210	66/210
$3979 \cdot 577 \equiv_n 2029$	45/174	28/174	74/174	27/174

(11)



$\Delta = 13/143 \cdot 69/210 \cdot 45/174 = 0.007725033 \Rightarrow \bar{F}(x) = 0.4170829 + \frac{\Delta}{2}$

$= 0.4209454$

y $l = \left\lceil \log_D 2/p(x) \right\rceil = \left\lceil \log_4 \frac{2}{0.007725033} \right\rceil = 5$

(1) $4^{-1} = 0.25$ $\quad 1 \cdot 4^{-1} + 1 \cdot 4^{-2} = 0.31$ $\quad \dots \Rightarrow \boxed{12233}033\dots \Rightarrow$ CGGUU

$2 \cdot 4^{-1} = 0.5$, no está $\quad 1 \cdot 4^{-1} + (2)\, 4^{-2} = 0.375$

$l = 5$

NOTA 1: K_S podría haberse encontrado en $\mathbb{Z}_{n_1 n_2}$ puesto que es la utilizada en el resto del problema:

n_2	n_1			
87	62	1	5	-7
62	25	2	-2	5
25	12	2	1	-2
12	$\boxed{1}$	12	0	1
	0			

$\Rightarrow K_S \equiv_{n_1 n_2} 33 \cdot 87 \cdot 5 + 22 \cdot 62 \cdot (-7)$

$\equiv 14355 - 9548 \equiv 4807$

NOTA 2: Para reducir la complejidad se ha evitado utilizar un RSA con $n = n_1 n_2 n_3 n_4$. En este caso el número de claves hubiera sido $n\phi(n) \doteq 3{,}2 \cdot 10^{14}$.

NOTA 3: Si se necesitan valores diferentes y no nulos, entonces el número de claves se reduce y el procedimiento para generar K_S se modifica:

3.1) $\phi(n)$ posibles claves para K_S y de las $\phi(n)$ posibles d sólo aquellas en que d y d^2 sean distintos (en este problema), es decir, $d \neq 1 \Rightarrow \phi(n)(\phi(n)-1) \simeq \phi^2(n) \simeq 6 \cdot 10^{13}$

3.2) Para encontrar K_S tal que $\in CRR_n$ es necesario que K_S sea primo con n_1, y con n_2, y con n_3, y con n_4. Se puede generar eligiendo 1 valor del CRR_{n_1}, 1 valor del CRR_{n_2}, 1 valor del CRR_{n_3} y 1 valor del CRR_{n_4} y no 4 valores aleatorios como propone el problema.