PROBLEMA 1

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} H(Y) - H(Y|X) = \max_{p(x)} H(X) - H(X|Y).$$

$H(X) = H(p)$ con $p(x_1) = p$.

$H(X|Y=y_1) = H(X|Y=y_5) = H(X|Y=y_6) = H(X|Y=y_7) = 0$.

y_i, $i=2,3$: $2\,p(y_i|x_1) = p(y_i|x_2)$, $2\,p(x_1|y_i)(1-p) = p(x_2|y_i)\,p$

$p(x_1|y_i) + p(x_2|y_i) = 1 \rightarrow p(x_1|y_i) = \dfrac{1}{1 + \frac{2(1-p)}{p}} = p/(2-p)$.

$p(y_i) = p(y_i|x_1)\,p + p(y_i|x_2)(1-p) = 1/6\,(2-p)$.

y_4: $p(y_4|x_1) = p(y_4|x_2)$, $p(x_1|y_4)(1-p) = p(x_2|y_4)\,p$

$\rightarrow p(x_1|y_4) = \dfrac{1}{1 + \frac{1-p}{p}} = p$., $p(y_4) = 1/6$ (no depende de p).

$$I(X;Y) = H(p) - 2 \cdot 1/6\,(2-p)\,H\left(\frac{p}{(2-p)}\right) - 1/6\,H(p).$$

p	0.5	0.6	0.4	0.3	0.45	0.46	0.44	0.43
$I(X;Y)$	0.32418	0.31935	0.3264	0.3234	0.3252	0.3279	0.32837	0.32825 ...

$p \in (0.43, 0.45)$, $p \sim 0.44 \rightarrow C \sim 0.3283$

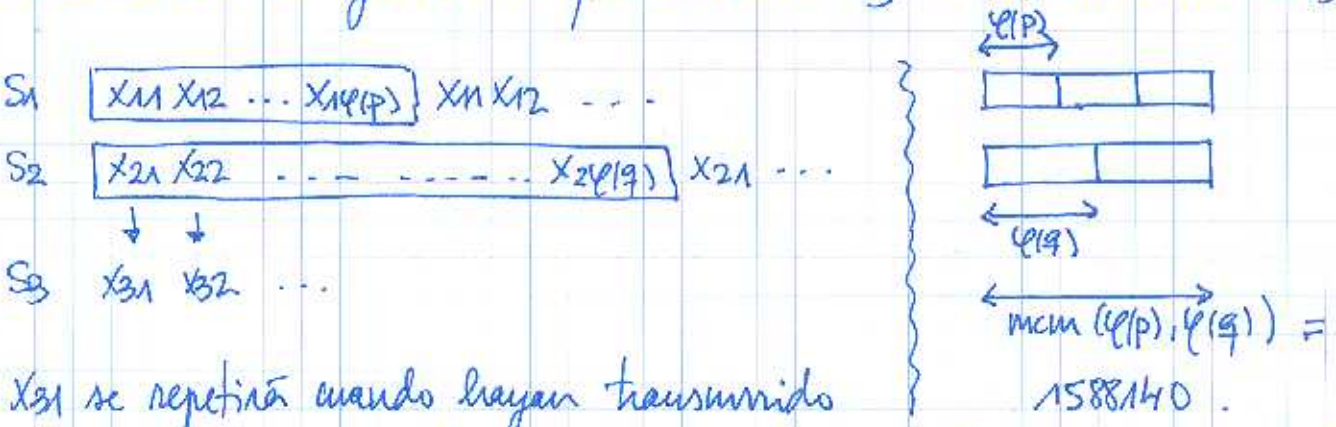
NOTA: Derivar es costoso $\longrightarrow p = 0.439988$ y $C = 0.32837$.

PROBLEMA 2

① x_{10} puede ser $<p$ diferente de $\emptyset$ y $\in CRR_p$, p primo. Como a_1 es una raíz primitiva $a_1, a_1^2, a_1^3, \dots, a_1^{\varphi(p)}$ genera todo el CRR_p. Para ello $a_1^j \equiv_p x_{11}$ para algún j ($x_{11} \in CRR_p$). Entonces $a_1^{j+1} \equiv_p x_{12}$, ... El periodo de S_1 es el orden de a_1, $\varphi(p) = 4590$. El de S_2, $\varphi(q) = 6228$

② Las inicializaciones deben generar S_3 diferentes, y se tendrán tantas como x_{30} diferentes. Es decir, tantas como pares (x_{10}, x_{20}) diferentes.
Como $x_{10} \in CRR_p$ y $x_{20} \in CRR_q \rightarrow x_{30} \in CRR_{pq} \rightarrow \varphi(pq) = 28586520$ //

③ Sabemos que $x_{3n} \in CRR_{pq}$, el periodo máximo será $\varphi(pq)$.
Para generar $\varphi(pq)$ valores se necesitan todos los pares (x_{1n}, x_{2n}).
En este caso la generación particular de S_3 no los considera todos:



x_{31} se repetirá cuando hayan transmitido 1588140 pares. Por esta razón (no están todos los $x_{3n} \in CRR_{pq}$), el número 1 estará o no en S_3, dependerá de la inicialización.

④ $x_{30}^{e} \bmod u = 3897$, d?

$\varphi(u)=$	28586520	$e=$	9301963	3	$x=$	-516778	$y=$	1588147
	9301963		680631	13		37813		-516778
	680631		453760	1		-25209		37813
	453760		226871	2		12604		-25209
	226871		18	12603		-1		12604
	18		17	1		-1		-1
	17		1	17		0		1
			0					

$x_{30} = 3897^{1588147} \bmod 28597339$

3897 es menor a p y a q $\rightarrow$ $3897 \in CRR_{pq} \rightarrow 3897^{\lambda(n)} \equiv_n 1 \rightarrow$

$x_{30} = 3897^{7} \bmod 28597339$. (módulo grande para la calculadora)

$\rightarrow$ $x_{10} = x_{30} \bmod p = (3897^{7} \bmod pq) \bmod p = 3897^{7} \bmod p = 516$

(resoluble con cálculos más pequeños). $x_{20} = 3897^{7} \bmod q = 4417$

$\Rightarrow$ $x_{30} \equiv_n 516 \cdot q \cdot q^{-1} + 4417 \cdot p \cdot p^{-1}$ (Sigue)

q = 6229	p = 4591	1	x = 199	y = -270
4591	1638	2	-71	199
1638	1315	1	59	-71
1315	323	4	-14	59
323	23	14	1	-14
23	1	23	0	1
	0			

$\rightarrow x_{30} \equiv_n 516 \cdot 1239571 + 4417 \cdot (-1239570) = 25985576$ //

⑤ La extensión más corta cumple con los símbolos de probabilidad mínima 1/182 :

n	1	2	3
Δ	$1/182 = 0.005\ldots$	$(1/182)^2 = 0.000003$	$(1/182)^3 <$ 0.0000024

$\rightarrow n_{min} = 2$ //

la más larga con símbolos de probabilidad máxima 1/13 :

n	1	...	5	6
Δ	$1/13 = 0.07$	...	$(1/13)^5 = 0.0000026$	$(1/13)^6 <$ 0.0000024

$\rightarrow n_{max} = 5$ //.

⑥ $S_3 = \{x_{31}, x_{32}, \ldots\}$

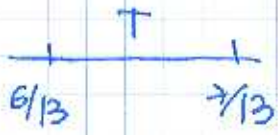
$x_{31} \equiv_n \underbrace{(a_1 516 \bmod p)}_{3952} q \cdot q^{-1} + \underbrace{(a_2 4417 \bmod q)}_{2314} p p^{-1} = 8543$

$x_{32} \equiv_n (a_1 \cdot 3952 \bmod p)\, q q^{-1} + (a_2 \cdot 2314 \bmod q)\, p p^{-1} = 16262834$

Es suficiente puesto que el criptograma tiene 11 dígitos :

$$\begin{array}{r} 21352824628 \\ -\ 85431626283 \\ \hline 46921208445 \end{array} \quad \text{(resta mod 10)}$$

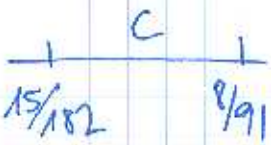
⑦ Para descomprimir podemos considerar 0.46921208445 . Una vez encontrado el intervalo nos quedaremos con los dígitos necesarios pero que garantizan que el número pertenece al intervalo. (duda)



$\Delta_1 = 1/13$ $\quad \frac{0.4692120845 - 6/13}{1/13} = 0.0997570785$

al menos 8 dígitos.

$\Delta_2 = \Delta_1 \cdot 14/182 = \Delta_1 \cdot 1/13$ $\quad \frac{0.0997709 - 17/182}{14/182} = 0.0825564557$



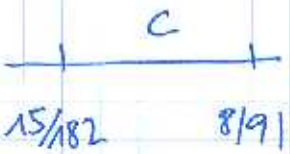
$\Delta_3 = \Delta_2 \cdot 1/182 = 0.000032$ $\quad \frac{0.08255645 - 15/182}{1/182} = 0.0252739$

$\Delta_4 = \Delta_3 \cdot 1/13 = 0.0000025$ → El siguiente Δ_5 será < 0.0000024.

Precisión necesaria: $[\underbrace{6/13 + 17/182\,\Delta_1 + 15/182 \cdot \Delta_2}, \underbrace{0.469211262 + \Delta_4})$

$[\quad 0.469211262\ldots, \quad 0.469211376\ldots)$

→ Del número 0.4692120845, solo son necesarios los 6 primeros: 0.469212. El resto es otra codificación



$\Delta_1 = 1/182$ $\quad \frac{0.0845 - 15/182}{1/182} = 0.3699$

$\Delta_2 = 1/182 \cdot \Delta_1$. Son 2 símbolos de prob. mínima, $n=2$

→ TECACP

El siguiente $\Delta_3 < 0.0000024$.

(8) $p^{-1} = (4\ 3\ 5\ 2\ 6\ 1\ 10\ \ldots)$

TECACP → ACCEPT.

NOTA! Si se recibe con $\underbrace{469450}_{\text{TEER}}\ \underbrace{26419}_{\text{FC}}$ → REJECT.