1.- Given that $P_r[C = K = 1, \ldots, n$ and $P_r[K] = 1/n$

We need to determine that $P_r[P|C] = \frac{P_r[P] \cdot P_r[C|P]}{P_r[C]}$

what means the $P_r[C|P]$ is the probability of the key

so that $P_r[C|P] = P_r[K] = 1/n$

And to Determine $P_r[C]$ we have to analyze the possibles cases of the ciphertext

in a 3x3 matrix $(n=3)$ we have that

$P_r[C=3] = 3/9 = 1/3 \quad P_r[c=2] = 3/9 = 1/3 \quad P_r[c=1] = 3/9 = 1/3$

So $P_r[C] = P_r[e_i(j)] = \sum_i^n \sum_j^n P_r[L(i,j)]$ and this is equal to $n/n^2 = 1/n$. Because each ciphertext ocurs n times in the $n \times n = n^2$ matrix.

With this information we have that

$$P_r[P|C] = \frac{P_r[P] \cdot P_r[C|P]}{P_r[C]} = \frac{P_r[P] \cdot 1/n}{1/n}$$

$\rightarrow P_r[P|C] = P_r[P]$

and the Latin Square Cryptosystem achieves perfect secrecy.

2. With $P_r[a] = 1/2$, $P_r[b] = 1/3$, $P_r[c] = 1/6$

$P_r[K] = 1/3$

1. $H(P) = -\sum_{x \in X} P_r[x] \log_2 P_r[x]$ with $x = a, b, c$ so.

$= -(P_r[a] \log_2 P_r[a] + P_r[b] \log_2 P_r[b] + P_r[c] \log_2 P_r[c])$

$= -(1/2 \log_2 1/2 + 1/3 \log_2 1/3 + 1/6 \log_2 1/6)$

$= -(-1{,}459) = 1{,}459$

$H(C) = -\sum_{x \in X} P_r[x] \log_2 P_r[x]$ with $x = 1, 2, 3, 4$.

But the Prob of each ciphertext is dependant of the Prob of each Key and each Plain text. $P[C]$ is ...

So if $y = 1$ and the $P_r[K]$ and $P_r[P]$ are independanto $\to$ $y = 1 \Rightarrow K = 1,\ P = a;\ K = 3,\ P = c$

$\Rightarrow P_r[y = 1] = P_r[K = 1] \cdot P_r[P = a] + P_r[K = 3]\, P_r[P = c]$

$= 1/3 \cdot 1/2 + 1/3 \cdot 1/6$

$= 1/6 + 1/18 = \frac{3+1}{18} = \frac{4}{18} = \frac{2}{9}$

for $y = 2$ we have: $K = 1,\ P = b$. and $K = 2,\ P = a$

$\Rightarrow P_r[y = 2] = P_r[K = 1] \cdot P_r[P = b] + P_r[K = 2]\, P_r[P = a]$

$= 1/3 \cdot 1/3 + 1/3 \cdot 1/2 = 1/9 + 1/6$

$= \frac{2+3}{18} = \frac{5}{18}$

For $y=3 \Rightarrow K=1, P=c$ and $K=2, P=b$ and $K=3, P=a$,

$$\Rightarrow Pr[y=3] = Pr[K=1]\,Pr[P=c] + Pr[K=2]\,Pr[P=b] + Pr[K=3]\,Pr[P=a]$$

$$= \tfrac{1}{3}\cdot\tfrac{1}{6} + \tfrac{1}{3}\cdot\tfrac{1}{3} + \tfrac{1}{3}\cdot\tfrac{1}{2}$$

$$= \tfrac{1}{18} + \tfrac{1}{9} + \tfrac{1}{6}$$

$$= \frac{1+2+3}{18} = \frac{6}{18} = \frac{1}{3}$$

For $y=4 \Rightarrow K=2, P=c$ and $K=3, P=b$

$$\Rightarrow Pr[y=4] = Pr[K=2]\,Pr[P=c] + Pr[K=3]\,Pr[P=b]$$

$$= \tfrac{1}{3}\cdot\tfrac{1}{6} + \tfrac{1}{3}\cdot\tfrac{1}{3}$$

$$= \tfrac{1}{18} + \tfrac{1}{9}$$

$$= \frac{1+2}{18} = \frac{3}{18} = \frac{1}{6}$$

So $H(C) = -\sum_{c\in C} Pr[c]\cdot\log_2 Pr[c]$

$$= -\left(\tfrac{2}{9}\log_2\left(\tfrac{2}{9}\right) + \tfrac{5}{18}\log_2\left(\tfrac{5}{18}\right) + \tfrac{1}{3}\log_2\left(\tfrac{1}{3}\right) + \tfrac{1}{6}\log_2\left(\tfrac{1}{6}\right)\right)$$

$$= -(-1.9546) = 1.955.$$

$$H(K) = -\left(\tfrac{1}{3}\log_2\left(\tfrac{1}{3}\right) + \tfrac{1}{3}\log_2\left(\tfrac{1}{3}\right) + \tfrac{1}{3}\log\left(\tfrac{1}{3}\right)\right)$$

$$= -(-1{,}5849) = 1{,}585$$

By the key equivocation we have that

$$H(K|C) = H(K) + H(P) - H(C)$$

$$= 1{,}585 + 1{,}459 - 1{,}955 = 1{,}089.$$

With $H(P|C) = -\sum_{y} \sum_{x} Pr[y] \cdot P[x|y] \log_2 [Pr[x|y]]$

We first do $H(P|c) = -\sum_{x} Pr[x|y] \log_2 [Pr[x|y]]$ for each $H(P|c=1)$, $H(P|c=2)$, $H(P|c=3)$ $H(P|c=4)$

So for $H(P|c=1)$ we have that:

$$H(P|c=1) = -((Pr[a|1] \log_2 [Pr[a|1]]) + P[b|1] \log_2 Pr[b|1]$$
$$+ Pr[c|1] \log_2 Pr(c|1)$$

We dont know the values of $Pr[a|1]$, ... $Pr[c|1]$ so.

$$Pr[a|1] = \frac{Pr[a] \cdot Pr[1|a]}{Pr[1]} = \frac{1/2 \cdot Pr[K]}{2/9} = \frac{1/2 \cdot 1/3}{2/9}$$

$$= \frac{1/6}{2/9} = 9/12 = 3/4$$

$$Pr[b|1] = \frac{P[b] \cdot Pr[1|b]}{Pr[1]} = \frac{1/3 \cdot 0}{2/9} = 0$$

$$Pr[c|1] = \frac{P[c] \cdot Pr[1|c]}{Pr[1]} = \frac{1/6 \cdot Pr[K]}{2/9} = \frac{1/6 \cdot 1/3}{2/9}$$

$$= \frac{1/18}{2/9} = 9/36 = \frac{1}{4}$$

So $H(P|c=1) = -(3/4 \log_2 3/4 + 0 \log_2 0 + 1/4 \log_2 1/4)$

$$= -(-0.81) = +0,81$$

For $H(P|c=2)$ we will simplify the process

$$H(P|c=2) = -(Pr[a|2] \log_2 Pr[a|2] + Pr[b|2] \log_2 [Pr[b|2]])$$

$$P[a|2] = \frac{Pr[a] \cdot P[2|a]}{Pr[2]} = \frac{1/2 \cdot 1/3}{5/18} = \frac{1/6}{5/18} = \frac{18}{30} = 3/5$$

$$P[b|2] = \frac{P[b]\ P[2|b]}{P[2]} = \frac{1/3 \cdot 1/3}{5/18} = 2/5$$

So $H(P|c=2) = -\left(3/5 \log_2 3/5 + 2/5 \log 2/5\right)$

$= -(-0,97095) = +0,971$

$H(P|C=3) = -(Pr[a|3] \log_2 Pr[a|c] + Pr(b|3] \log_2 Pr[b|3]$

$+ Pr[c|3] \log_2 Pr(c|3]$

$$Pr[a|3] = \frac{Pr[a]\ Pr[3|a]}{Pr[3]} = \frac{1/2 \cdot 1/3}{1/3} = 1/2$$

$$Pr[b/3] = \frac{Pr(b]\ Pr[3/b]}{Pr[3]} = \frac{1/3 \cdot 1/3}{1/3} = 1/3$$

$$Pr[c/3] = \frac{Pr[c]\ Pr\{3/c]}{Pr[3]} = \frac{1/6 \cdot 1/3}{1/3} = 1/3$$

$\Rightarrow H(P|C=3) = -(1/2 \log_2 1/2 + 1/3 \log_2 1/2 + 1/3 \log_2 1/3)$

$= -(-1,459) = 1,459.$

So $H(P|c=4) = -(Pr(b|4) \log_2 Pr[b|4] + Pr[c|4] \log_2 Pr[c|4]$

$$Pr(b/4] = \frac{Pr[b]\ Pr[4|b]}{Pr[4]} = \frac{1/2 \cdot 1/3}{1/6} = 2/3$$

$$Pr(c/4] = \frac{Pr[c]\ Pr[4/c]}{Pr[4]} = \frac{1/6 \cdot 1/3}{1/6} = 1/3$$

So $H(P|C=4) = -(2/3 \log_2 2/3 + 1/3 \log_2 1/3)$

$= -(-0,918) = 0,918$

Now whats left is to

$$H(P|C) = \sum_{y \in C} P_r[y] \cdot H(P|C=y)$$

$$= \frac{2}{9} \cdot 0{,}81 + \frac{5}{18} \cdot 0{,}97 + \frac{1}{3} \cdot 1{,}454 + \frac{1}{6} \cdot 0{,}918$$

$$= 1{,}08905 \ldots = 1{,}09$$

3.— We need $H(K|C)$ and $H(K|P,C)$

First lets determine the number of possible keys and plain texts.

as we have 26 letters in the alphabet we can have that $P_r[P] = P_r[C] = \frac{1}{26}$

$|P| = 26$

But for the keys we have to consider. a and b:

we know that b should be betwen 0 and 25 because $b < m$, m = length of the alphabet and a should be all the coprimes lesser than m.

so $a = (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25)$

so we eventually have $12 \cdot 26$ possible keys

so $|K| = 312$.

Now $H(P) = -\sum P_r(P) \cdot \log(P_r(P))$ and with 26 possibilities $\Rightarrow$

$$H(P) = 26 \cdot -(1/26 \log_2 P_r(1/26)) = H(C)$$
$$= 26 \cdot 0{,}18 = 4{,}68$$

For $H(K) = -\sum P_r(K) \cdot \log(P_r(K))$ and with 312 possibilities $\Rightarrow$

$$H(K) = 312 \cdot -(1/312 \log_2 P_r(1/312)) =$$
$$= 312 \cdot 0{,}0265 = 8{,}268$$

So $H(K|C) = H(K) + H(P) - H(C)$
$$= H(K) = 8{,}268$$

Escaneado con CamScanner

4.- The unicity distance has the estimate for

$$n_0 \approx \frac{\log_2 |K|}{R_L \log_2 |P|}$$

So we have to find $|K|$ and $|P|$

For $|P|$ we have to consider that for an english alphabet we could have 26 posibilities for each position in the m length plain text so

$|P| = 26 \cdot 26 \cdot 26 \cdot \ldots$ this happens m times so

$|P| = 26^m$

Now with $|K|$. For an english alphabet we can have 26 posibilities for each position in a row of the matrix. so if a row is of length m => (m colums)

$r = 26 \cdot 26 \cdot 26 \cdot 26 \ldots$ with m colums

we have that each row has 26^m possibilities

then we know that we have m rows given a $m \times m$ matrix

so matrix $= r \cdot r \cdot r \cdot r \ldots$ this happens m times

$= 26^m \cdot 26^m \cdot 26^m \cdot \ldots$

$= 26^{3 \cdot m} \cdot 26^m \ldots$ so at the end

we have $26^{m \cdot m} = 26^{m^2}$ possible $m \times m$ matrices, but not every matrix has inverse so the $|K|$ is leser than 26^{m^2} $\Rightarrow |K| < 26^{m^2}$

Escaneado con CamScanner

So returning to the unicity distance

$n_0 \approx \frac{\log_2|K|}{R_L \log_2|P|}$ with the fact that $|P| = 26^m$ and $|K| = 26^{m^2}$

$$\frac{\log_2|K|}{R_L \log_2|P|} = \frac{\log_2|K|}{R_L \log(26^m)}$$ and we can create an inequality

$$\Rightarrow \frac{\log_2|K|}{R_L \log_2(26^m)} \leq \frac{\log_2(26^{m^2})}{\log_2(26^m) \, R_L}$$ and with log properties

$$\Rightarrow \log(26^{m^2}) = m^2 \cdot \log(26) \quad \text{and} \quad \log(26^m) = m\log(26)$$

$$\Rightarrow \frac{\log_2(26^{m^2})}{\log_2(26^m) \cdot R_L} = \frac{m^2 \log_2(26)}{m \log_2(26) \cdot R_L} = \frac{m}{R_L}$$