Name: Kevin Huertas

Information Security CMP-5006

Homework 1

Exercise 1

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L. An example of a Latin square of order 3 is as follows:

	C1	C2	C3
R1	1	2	3
R2	3	1	2
R3	2	3	1

Given any Latin square L of order n, we can define a related Latin Square Cryptosystem. Let the sets $P = C = K = 1, \ldots, n$, be the sets representing the space for the plaintext, ciphertext and keys. For $1 \leq i \leq n$, the encryption rule e_i is defined to be $e_i(j) = L(i, j)$. Here, i would be the key, j the plaintext, and $e_i(j)$ the ciphertext.

Give a complete proof that this Latin Square Cryptosystem achieves perfect secrecy provided that every key is used with equal probability.

① Exercise ①

Latin square

$P = C = K = 1, \ldots, n$

$1 \leq i \leq n$

$e_i \rightarrow e_i(j) = L(i,j)$

$i \rightarrow$ key

$j \rightarrow$ plaintext

$e_i(j)$ ciphertext

$x, y \in \{1, \ldots, n\}$

$K_{x,y} \rightarrow e_{K_{x,y}}(x) = y$

$C(k) = \{1, \ldots, n\}$

Uniformidad de cifrado $\rightarrow$ igual probabilidad $P_r(K=k) = \frac{1}{n}$ en $k \in K$

Para $y \in \{1, \ldots, n\}$ $\rightarrow$

$$Pr(y=y) = \sum_{x \in (1, \ldots, n)} Pr[K = K_{x,y}] Pr(x=x)$$

$$= \sum_{x \in \{1, \ldots, n\}} \left(\frac{1}{n}\right) \times Pr(x=x)$$

$$= \frac{1}{n}$$

Para $x \in \{1, \ldots, n\}$ $\rightarrow$

$$Pr[y=y \mid x=x]$$

$$= Pr[K = K_{x,y}]$$

$$= \frac{1}{n}$$

$Pr[x = x \mid y=y) = Pr[x=x]$ Para x, y

Exercise 2

Consider a cryptosystem in which the sets representing the plaintext, ciphertext and keys are: $P = a, b, c$, $K = K1, K2, K3$ and $C = 1, 2, 3, 4$. Suppose the encryption matrix is as follows:

	a	b	c
K1	1	2	3
K2	2	3	4
K3	3	4	1

Given that keys are chosen equiprobably, and the plaintext probability distribution is $Pr[a] = 1/2$, $Pr[b] = 1/3$, $Pr[c] = 1/6$, compute $H(P)$, $H(C)$, $H(K)$, $H(K|C)$, and $H(P|C)$.

(2)

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

$P = a, b, c$

$K = K_1, K_2, K_3$

$C = 1, 2, 3, 4$

$Pr(a) = \frac{1}{2}$

$Pr(b) = \frac{1}{3}$

$Pr(c) = 1/6$

probabilidades

$H(K) = \frac{1}{3}\log_2 3 + \frac{1}{3}\log_2 3 + \frac{1}{3}\log_2 3 \approx 1.585$ //

$H(P) = \frac{1}{2}\log_2 2 + \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6 = \frac{2}{3} + \frac{1}{2}\log_2 3$

≈ 1.459 //

$H(C) = \begin{cases} Pr(y=1) = 4/18 = \frac{2}{9} \\ Pr(y=2) = 5/18 = \frac{5}{18} \\ Pr(y=3) = 6/18 = \frac{1}{3} \\ Pr(y=4) = 3/18 = \frac{1}{6} \end{cases} \rightarrow H(C) = 1.955$

Theorema Shannon:

- $H(K|C) = H(K) + H(P) - H(C) = 1$

$= 1.039$

- $H(P|C) \rightarrow Pr(x|y)$ p/ $\forall$ $\rightarrow$

	a	b	c
1	3/4	0	1/4
2	3/5	2/5	0
3	1/2	1/3	1/6
4	0	2/3	1/3

$H(P,C) = 3 \times \left[\frac{1}{6}\log_2 6 + \frac{1}{9}\log_2 9 + \frac{1}{18}\log_2 18\right]$

≈ 3.044

$H(P|C) = H(P,C) - H(C)$

≈ 1.089 //

Exercise 3

Compute $H(K|C)$ and $H(K|P,C)$ for the Affine Cipher, assuming that keys are used equiprobably and the plaintexts are equiprobable.

3 $H(K,C)$

$H(K|P,C)$

keys = equipabably

plaintext = equiprobable

- 26 alphabet

Affine Cipher 2 keys (a,b)

posible keys = 312

$P = C = \mathbb{Z}_{26}$

$H(K|C) = \log_2 312$

$H(K|P,C) = \log_2 12$

Exercise 4

Show that the unicity distance of the Hill Cipher (with an $m \times m$ encryption matrix) is less than $\frac{m}{R_L}$. (Note that the number of alphabetic characters ina plaintext of this length is $\frac{m^2}{R_L}$.)

(4) Hil Cipher

$m \times m$ encryption matrix $< n/R_L$

. matrix

$m \times m$ con entradas $\mathbb{Z}_{26}$ son 26^{m^2} | No todas invertibles

- $|K| < 26^{m^2}$ | $|P| = 26^m$

$$\frac{\log_2 |K|}{R_L \log_2 |P|} < \frac{m^2 (\log_2 26)}{m (\log_2 26) R_L} = \frac{m}{R_L}$$

//