

Exercise 1

Let  $n$  be a positive integer. A Latin square of order  $n$  is an  $n \times n$  array  $L$  of the integers  $1, \dots, n$  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  $P = C = K = 1, \dots, n$ , 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.

$$\Pr(K) = \frac{1}{n}$$

Perfect secrecy

$$x \in \mathcal{P}, \quad y \in \mathcal{C}$$

$$\begin{aligned} \Pr(C) &= \sum_p \Pr(K) \Pr(p) \\ &= \sum_p \frac{1}{n} \times \Pr(p) \\ &= \frac{1}{n} \end{aligned}$$

$$\Rightarrow \Pr(P|C) = \frac{\Pr(P) \Pr(C|P)}{\Pr(C)}$$

$$= \frac{\Pr(P) \frac{1}{n}}{\frac{1}{n}} = \Pr(P)$$

## 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  $H(P|C)$ .

$$Pr(a) = 1/2$$

$$Pr(b) = 1/3$$

$$Pr(c) = 1/6$$

$$H(X) = - \sum_i Pr(x_i) \log_2 Pr(x_i)$$

$$\begin{aligned} \bullet H(P) &= - ( Pr(a) \log_2 Pr(a) + Pr(b) \log_2 Pr(b) + Pr(c) \log_2 Pr(c) ) \\ &= - ( \frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{6} \log_2 \frac{1}{6} ) \\ &= - ( -0.50 - 0.53 - 0.43 ) \\ &= 1.46 \end{aligned}$$

$$\begin{aligned} \bullet H(K) &= - \left( 3 \left( \frac{1}{3} \log_2 \frac{1}{3} \right) \right) \\ &= 1.58 \end{aligned}$$

$$\bullet \text{ Para calcular } H(C) \text{ hay que calcular las } Pr(C)$$

$$\begin{aligned} Pr(1) &= Pr(K_1) Pr(a) + Pr(K_3) Pr(c) \\ &= \frac{1}{3} \cdot \frac{1}{2} + \frac{1}{3} \cdot \frac{1}{6} = \frac{1}{6} + \frac{1}{18} = \frac{3+1}{18} = \frac{4}{18} = \frac{2}{9} \end{aligned}$$

$$\begin{aligned} Pr(2) &= Pr(K_1) Pr(b) + Pr(K_2) Pr(a) \\ &= \frac{1}{3} \left( \frac{1}{3} + \frac{1}{2} \right) = \frac{5}{18} \quad \star Pr(K) = \frac{1}{3} \end{aligned}$$

$$\begin{aligned} Pr(3) &= \frac{1}{3} ( Pr(a) + Pr(b) + Pr(c) ) \\ &= \frac{1}{3} \left( \frac{1}{2} + \frac{1}{3} + \frac{1}{6} \right) = \frac{1}{3} \left( \frac{3+2+1}{6} \right) = \frac{6}{18} = \frac{1}{3} \end{aligned}$$

$$\begin{aligned} Pr(4) &= \frac{1}{3} ( Pr(b) + Pr(c) ) = \frac{1}{3} \left( \frac{1}{3} + \frac{1}{6} \right) \\ &= \frac{1}{3} \left( \frac{2}{6} \right) = \frac{1}{6} \end{aligned}$$

$$Pr(1) = 2/9$$

$$Pr(2) = 5/18$$

$$Pr(3) = 1/3$$

$$Pr(4) = 1/6$$

$$\begin{aligned} H(C) &= - ( Pr(1) \log_2 Pr(1) + Pr(2) \log_2 Pr(2) + Pr(3) \log_2 Pr(3) \\ &\quad + Pr(4) \log_2 Pr(4) ) \\ &= 1.96 \end{aligned}$$

$$H(K|C) = H(K) + H(P) - H(C) \quad \star \text{ Del libro de Dauglas}$$

$$\bullet H(K|C) = 1.58 + 1.46 - 1.96 = 1.08$$

• Para el término  $P_r(P|C)$

C \ P	a	b	c
1	$3/4$	0	$1/4$
2	$3/5$	$2/5$	0
3	$1/2$	$1/3$	$1/6$
4	0	$2/3$	$1/3$

Del libro de Dawles \* 3.6  $H(X|Y) = - \sum_x P_r(x|y) \log_2 P_r(x|y)$

Entropía condicional

$$H(X|Y) = - \sum_y P_r(y) \sum_x P_r(x|y) \log_2 P_r(x|y)$$

$$\begin{aligned} H(P|1) &= -(P_r(a|1) \log_2 P_r(a|1) + P_r(b|1) \log_2 P_r(b|1) \\ &\quad + P_r(c|1) \log_2 P_r(c|1)) \\ &= - \left( \frac{3}{4} \log_2 \frac{3}{4} + 0 + \frac{1}{4} \log_2 \frac{1}{4} \right) = 0.81 \end{aligned}$$

$$H(P|2) = 0.96$$

$$H(P|3) = 1.46$$

$$H(P|4) = 0.92$$

$$P_r(1) = 2/9$$

$$P_r(2) = 5/16$$

$$P_r(3) = 1/3$$

$$P_r(4) = 1/6$$

$$H(P|C) = \sum_c P_r(c) H(P|c)$$

$$= \frac{2}{9} \cdot 0.81 + \frac{5}{16} \cdot 0.96 + \frac{1}{3} \cdot 1.46 + \frac{1}{6} \cdot 0.92$$

$$= 1.08$$

### 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.

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

• Recordemos que hay 26 posibles letras en el alfabeto. y en el affine cipher la llave es una combinación de 2 factores ( $\alpha$  y  $\beta$ ).  $\alpha$  debe ser coprimo al  $n$  (tamaño del alfabeto) y recordemos que en clase vimos por qué  $\alpha > 26$  son equivalentes a los  $\alpha < 26$ . Entonces para  $\alpha$  hay 12 opciones (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25) y  $\beta$  puede ser cualquier entero entre 0 y 25 (26 opciones). Por lo tanto el número de elementos de  $K$  es  $12 \cdot 26 = 312$

$$\Rightarrow H(K) = - \cancel{312} \left( \frac{1}{\cancel{312}} \log_2 \frac{1}{\cancel{312}} \right) = 8.29$$

$$H(P) = - 26 \left( \frac{1}{26} \log_2 \frac{1}{26} \right) = 4.7$$

$$H(C) = - 26 \left( \frac{1}{26} \log_2 \frac{1}{26} \right) = 4.7$$

$$H(K|C) = 8.29$$

## 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 in a plaintext of this length is  $\frac{m^2}{R_L}$ .)

$$N_0 \approx \frac{\log_2 |K|}{R_L \log_2 |P|}$$

- Assuming English alphabet, it is clear that  $|P| = 26^m$  where  $m$  is the length of the message. Similarly  $|K| = 26^m$  since there are 26 possibilities for each row. This implies there are  $26^{m^2}$   $m \times m$  matrices (due to the  $m$  rows). However, not all of them might be reversible so  $|K| < 26^{m^2}$

Therefore

$$\begin{aligned} \frac{\log_2 |K|}{R_L \log_2 26^m} &< \frac{\log_2 26^{m^2}}{R_L \log_2 26^m} \\ &< \frac{m^2 \log_2 26}{m R_L \log_2 26} \\ &< \frac{m}{R_L} \end{aligned}$$