

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.

$$\Pr(K) = \frac{1}{n} \quad \text{Perfect secrecy} \quad x \in P, y \in C$$

$$\Pr(C) = \sum_p \Pr(K) \Pr(p)$$

$$= \sum_p \frac{1}{n} \times \Pr(p)$$

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

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

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

Exercise 2

Consider a cryptosystem in which the sets representing the plaintext, ciphertext and keys are: $P = \{a, b, c\}$, $K = \{K_1, K_2, K_3\}$ 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 $H(P|C)$.

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

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

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

$$H(P) = - (\Pr(a) \log_2 \Pr(a) + \Pr(b) \log_2 \Pr(b) + \Pr(c) \log_2 \Pr(c))$$

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

$$= - \left(\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{6} \log_2 \frac{1}{6} \right)$$

$$= - (-0.50 - 0.93 - 0.43)$$

$$= 1.46$$

$$H(K) = - \left(3 \left(\frac{1}{3} \log_2 \frac{1}{3} \right) \right)$$

$$= 1.58$$

To calculate $H(C)$, we need $\Pr(c) \forall c \in C$

$$\Pr(1) = \Pr(K_1) \Pr(a) + \Pr(K_3) \Pr(c)$$

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

$$\Pr(2) = \Pr(K_1) \Pr(b) + \Pr(K_2) \Pr(a)$$

$$= \frac{1}{3} \left(\frac{1}{3} + \frac{1}{2} \right) = \frac{5}{18} \quad * \Pr(K) = \frac{1}{3}$$

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

$$= \frac{1}{3} \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \right) = \frac{1}{3} \left(\frac{3+2+1}{6} \right) = \frac{6}{18} = \frac{1}{3}$$

$$\Pr(4) = \frac{1}{3} (\Pr(b) + \Pr(c)) = \frac{1}{3} \left(\frac{1}{3} + \frac{1}{6} \right)$$

$$= \frac{1}{3} \left(\frac{3}{6} \right) = \frac{1}{6}$$

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

$$H(C) = - (\Pr(1) \log_2 \Pr(1) + \Pr(2) \log_2 \Pr(2) + \Pr(3) \log_2 \Pr(3) + \Pr(4) \log_2 \Pr(4))$$

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

$$= 1.96$$

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

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

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

- Calculate $\Pr(P|C)$ for each $p \in P$ and $c \in C$ as follows. (For the rest, use a calculator directly)

$$\Pr(a|1) = \frac{\Pr(a) \Pr(1|a)}{\Pr(1)} = \frac{\frac{1}{2} \cdot \Pr(k)}{\frac{2}{9}} = \frac{\frac{1}{2} \cdot \frac{1}{3}}{\frac{2}{9}} = \frac{3}{4}$$

		P		
		a	b	c
C	1	$\frac{3}{4}$	0	$\frac{1}{4}$
	2	$\frac{3}{5}$	$\frac{2}{5}$	0
	3	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$
	4	0	$\frac{2}{3}$	$\frac{1}{3}$

* 3.6 $H(X|y) = - \sum_x \Pr(x|y) \log_2 \Pr(x|y)$

From the Stinson book

Entropy calculation

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

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

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

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

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

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

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

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

$$= \frac{2}{9} \cdot 0.81 + \frac{5}{18} \cdot 0.96 + \frac{1}{3} \cdot 1.46 + \frac{1}{6} \cdot 0.92$$

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

$$= 1.08$$

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

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.

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

In the english alphabet there are 26 letters and the affine cipher's key is a combination of two factors α and β . α must be coprime with the size of the alphabet. And in practicality (as we saw in class) $\alpha > 26$ are equivalent to $\alpha < 26$. Therefore α can take 12 possible values

(1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25). And β can be any integer such that $0 \leq \beta < 26$. Thus $|K| = 12 \cdot 26 = 312$

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

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

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

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

$$\star 3.10 \quad H(K, P, C) = H(K) + H(P)$$

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

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

$$\leq H(K) + H(P) - H(P) - H(C) \quad \star 3.9$$

$$= H(K) - H(C)$$

$$= 8.29 - 4.7$$

$$= 3.59$$

$$H(X,Y) \leq H(X) + H(Y)$$

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

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