3.20 A *Substitution Cipher* over a plaintext space of size n has $|\mathcal{K}| = n!$ ***Stirling's formula*** gives the following estimate for $n!$:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

(a) Using Stirling's formula, derive an estimate of the unicity distance of the *Substitution Cipher*.

(b) Let $m \geq 1$ be an integer. The *m-gram Substitution Cipher* is the *Substitution Cipher* where the plaintext (and ciphertext) spaces consist of all 26^m m-grams. Estimate the unicity distance of the *m-gram Substitution Cipher* if $R_L = 0.75$.

Solution:

Let's assume:

L > Unicity distance of the substation cipher

C > Corresponding ciphertext

When n! possible key the probability of guessing key is 1/n!

There are 2 cases for this. One when the length of Ciphertext (c) <L [result: more possible plaintexts]

Other, length of the ciphertext (c) > L

<u>For estimating unicity of substitution cipher,</u>

When the length of the given ciphertext k , the possible plaintext are:

n(n-1)(n-2)(n-3)…..(n-k+1)

when n is larger than k then value becomes $n^{K.}$

Now,

Suppose ciphertext= L

Possible plaintext n^L but if N is larger than L

n! = $\approx \sqrt{(2\pi n)} * (n/e)^n$

adding log on both sides,

$\log(n!) \approx \log(\sqrt{(2\pi n)} * (n/e)^n)$

$\log(n!) \approx 1/2\log(2\pi n) + n \log (n/e)$

we know $\log(x^y) = y * \log(x)$ so,

$\log(n!) \approx 1/2\log(2\pi n) + n\log(n) - n$

Solving for L,

$L \approx (1/2\log(2\pi n) + n\log(n) - n) / \log(n)$

So,

$L \approx (1/2\log(2\pi n) + n\log(n) - n) / \log(n)$

3.8 Suppose that y and y' are two ciphertext elements (i.e., binary n-tuples) in the *One-time Pad* that were obtained by encrypting plaintext elements x and x', respectively, using the same key, K. Prove that $x + x' \equiv y + y' \pmod 2$.

Here as we know,

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. For $K \in (\mathbb{Z}_2)^n$, define $e_K(x)$ to be the vector sum modulo 2 of K and x (or, equivalently, the exclusive-or of the two associated bitstrings). So, if $x = (x_1, \ldots, x_n)$ and $K = (K_1, \ldots, K_n)$, then

$$e_K(x) = (x_1 + K_1, \ldots, x_n + K_n) \bmod 2.$$

Decryption is identical to encryption. If $y = (y_1, \ldots, y_n)$, then

$$d_K(y) = (y_1 + K_1, \ldots, y_n + K_n) \bmod 2.$$

Given.

Plaintext: x and x'

cipher text after encrypting,

$y = x + K$ ----1

$y' = x' + K$ ----2, where + denotes X-OR operation

From 1 and 2 equation we get,

$y + y' = (x + K) + (x' + K)$

$y + y' = x + x' + 2K$

K denotes tuple, also

2K ≡ 0 (mod2) as binary tuple addition with itself =0

We get,

y + y’ ≡ x + x’ (mod2)

i,e,

X-OR of (y and y’ equivalent to x and x’)mod 2

Also, if we (add plaintext of x and x’ equivalent to adding the ciphertext of y and y’ bitwise) modulo 2

Hence, proved.

3.4 Let $\mathcal{P} = \{a, b\}$ and let $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$. Let $\mathcal{C} = \{1, 2, 3, 4, 5\}$, and suppose the encryption functions are represented by the following encryption matrix:

	a	b
K_1	1	2
K_2	2	3
K_3	3	1
K_4	4	5
K_5	5	4

Now choose two positive real numbers α and β such that $\alpha + \beta = 1$, and define $\mathbf{Pr}[K_1] = \mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = \alpha/3$ and $\mathbf{Pr}[K_4] = \mathbf{Pr}[K_5] = \beta/2$.

Prove that this cryptosystem achieves perfect secrecy.

Here,

Suppose,

α = 0.6

β= 0.4

α + β = 1

0.6+ 0.4 =1

Hence,

Pr [K1] = Pr [K2] = Pr [K3] = α/3 = 0.6/3 = 1/5

And, Pr [K4] = Pr [K5] = β/2 = 0.4/2 = 1/5

Pr[a] + Pr[b] = 1

Pr[a] = 1/5

and Pr[b] = 4/5

Pr[y] = ∑Pr(k) * Pr(dk (y))

Now,

Pr[1] = (Pr[a] * Pr[K1]) + (Pr[b] + Pr[K3])

= (1/5 * 1/5) + (4/5 * 1/5) = 1/25 + 4/25 = 5/25 = 1/5

Pr[2] = (Pr[a] * Pr[k2]) + (Pr[b] * pr[K1])

= (1/5 * 1/5) + (4/5 * 1/5) = 1/25 + 4/25 = 5/25 = 1/5

Pr[3] = (Pr[a] * Pr[k3]) + (Pr[b] * pr[K2])

= (1/5 * 1/5) + (4/5 * 1/5) = 1/5

Pr[4] = (Pr[a] * Pr[k4]) + (Pr[b] * pr[K5])

= (1/5 * 1/5) + (4/5 * 1/5) = 1/5

Pr[5] = (Pr[a] * Pr[k5]) + (Pr[b] * pr[K4])

= (1/5 * 1/5) + (4/5 * 1/5) = 1/5

Now, P[1] + P[2] + P[3] + p[4] +[5] =1

As 1/5 + 1/5 + 1/5 + 1/5 + 1/5 = 1

Perfect secrecy achieved when

A posteriori probabilities = a priori probabilities

Pr[x | y] = Pr[x] for x € P and y € C

Pr[x | y] = (Pr[x] * pr[y | x]) / Pr[y]

Where **Pr[y | x] =** *{k:dky=x}*Pr*[K]* $\sum_{\{k:dk(y)=x\}} \Pr\ [K]$

= 1/5+ 1/5 +1/5 + 1/5 + 1/5 = 1

Pr[x] = (1/5 * 1)/(1/5) = 1

3.15 Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

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

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

Here,

H(P|C) = H(P, C) − H(C)

Since,

Pr[a] = 1/2,

Pr[b] = 1/3,

Pr[c] = 1/6.

Also,

H(P) = $1/2 \log_2 2 + 1/3 \log_2 3 + 1/6 \log_2 6 = 2/3 + 1/2 \log_2 3 \approx$ **1.459**

Now,

Calculation of probability Distribution of C

Pr[y = 1] = 2/9,

Pr[y = 2] = 5/18,

Pr[y = 3] = 1/3,

Pr[y = 4] = 1/6

Hence, entropy of the ciphertext:

H(C) = $-2/9 \log_2 2/9 - 5/18 \log_2 5/18 - 1/3 \log_2 1/3 - 1/6 \log_2 1/6 \approx$ **1.955.**

Since,

$Pr[x = a, y] = 1/6$, for $y = 1, 2, 3$
$Pr[x = b, y] = 1/9$, for $y = 2, 3, 4$
$Pr[x = c, y] = 1/18$, for $y = 1, 3, 4$

Remaining 3 probabilities are 0 so,

H(P, C) = $3 \times [1/6 \log_2 6 + 1/9 \log_2 9 + 1/18 \log_2 18]$ **≈ 3.044,**

Hence,

H(P|C) = $H(P, C) - H(C) = 3.044 - 1.955$ **≈ 1.089.**