# Substitution Cipher

Math 4175

# §2.2.1. Permutation

A permutation of an ordered set S is a rearrangement of the elements of S into one-to-one correspondence with S itself. In other words, a permutation on S is a 1-1 and onto function $\pi : S \to S$

# §2.2.1. Permutation

A permutation of an ordered set S is a rearrangement of the elements of S into one-to-one correspondence with S itself. In other words, a permutation on S is a 1-1 and onto function $\pi : S \to S$

Example: Let $S = \{a, b, c\}$. The following is a permutation:

| | | |
|---|---|---|
| a | b | c |
| A | C | B |

We used small letters in the first row and capital letters in the second row for easy reading.

# §2.2.1. Permutation

A permutation of an ordered set S is a rearrangement of the elements of S into one-to-one correspondence with S itself. In other words, a permutation on S is a 1-1 and onto function $\pi : S \to S$

Example: Let $S = \{a, b, c\}$. The following is a permutation:

```
a b c
A C B
```

We used small letters in the first row and capital letters in the second row for easy reading.

Verify that there are $3! = 6$ possible permutations for the above set S.

# §2.2.1. Permutation

Let S be the set of all 26 alphabets. Following is a permutation on S:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

- There are $26! > 4 \times 10^{26}$ permutations and so writing all of them is infeasible.

# §2.2.1. Permutation

Let S be the set of all 26 alphabets. Following is a permutation on S:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

- There are $26! > 4 \times 10^{26}$ permutations and so writing all of them is infeasible.
- Again by replacing $A = 0, B = 1, \cdots, Z = 25$, we will identify S with $\{0, 1, \cdots, 25\}$.

## §2.2.1. Permutation

Let S be the set of all 26 alphabets. Following is a permutation on S:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

- There are $26! > 4 \times 10^{26}$ permutations and so writing all of them is infeasible.
- Again by replacing $A = 0, B = 1, \cdots, Z = 25$, we will identify S with $\{0, 1, \cdots, 25\}$.
- Each shift by n mod 26 for $1 \leq n \leq 25$, that is each key in the Shift Cipher, yields a permutation.

# §2.2.1. Permutation

For each permutation $\pi$ on S, there is a unique inverse permutation $\pi^{-1}$ defined by $\pi^{-1}(y) = x$ where $\pi(x) = y$.

# §2.2.1. Permutation

For each permutation $\pi$ on S, there is a unique inverse permutation $\pi^{-1}$ defined by $\pi^{-1}(y) = x$ where $\pi(x) = y$.

For example, if $\pi$ is the permutation:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

# §2.2.1. Permutation

For each permutation $\pi$ on S, there is a unique inverse permutation $\pi^{-1}$ defined by $\pi^{-1}(y) = x$ where $\pi(x) = y$.

For example, if $\pi$ is the permutation:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

then $\pi^{-1}$ is given by

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| d | l | r | y | v | o | h | e | z | x | w | p | t | b | g | f | j | q | n | m | u | s | k | a | c | i |

## §2.2.1. Permutation

For each permutation $\pi$ on S, there is a unique inverse permutation $\pi^{-1}$ defined by $\pi^{-1}(y) = x$ where $\pi(x) = y$.

For example, if $\pi$ is the permutation:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

then $\pi^{-1}$ is given by

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| d | l | r | y | v | o | h | e | z | x | w | p | t | b | g | f | j | q | n | m | u | s | k | a | c | i |

Notice that $\pi^{-1}(\pi(\alpha)) = \alpha$.

# §2.2.1. Permutation

A Substitution Cipher is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K}$ consists of all possible permutations of the symbols $0, 1, \cdots, 25$ ( or of 26 alphabets). For each $\pi \in \mathcal{K}$, we define

$$e_\pi(x) = \pi(x)$$

$$d_\pi(x) = \pi^{-1}(x)$$

# §2.2.1. Permutation

A Substitution Cipher is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K}$ consists of all possible permutations of the symbols $0, 1, \cdots, 25$ ( or of 26 alphabets). For each $\pi \in \mathcal{K}$, we define

$$e_\pi(x) = \pi(x)$$

$$d_\pi(x) = \pi^{-1}(x)$$

- Notice that every Shift Cipher is a Substitution Cipher where the permutation is obtained by a shift.

# §2.2.1. Permutation

A Substitution Cipher is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K}$ consists of all possible permutations of the symbols $0, 1, \cdots, 25$ ( or of 26 alphabets). For each $\pi \in \mathcal{K}$, we define

$$e_\pi(x) = \pi(x)$$

$$d_\pi(x) = \pi^{-1}(x)$$

- Notice that every Shift Cipher is a Substitution Cipher where the permutation is obtained by a shift.
- Substitution Cipher has also been used for hundreds of years, for example, many puzzles in newspapers.

## §2.2.1. Permutation

Suppose that Alice uses the following key in a Substitution Cipher:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

# §2.2.1. Permutation

Suppose that Alice uses the following key in a Substitution Cipher:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

Then encipher:

I came I saw I conquered

# §2.2.1. Permutation

Suppose that Alice uses the following key in a Substitution Cipher:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

Then encipher:

I came I saw I conquered
Z YXTH Z VXK Z YFSRUHCHA (ciphered)

# §2.2.1. Permutation

Suppose that Alice uses the following key in a Substitution Cipher:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

Then encipher:

I came I saw I conquered
Z YXTH Z VXK Z YFSRUHCHA (ciphered)

Decipher the following by using above key:

KHBYFTH NXYW GFWZHV
MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA

# §2.2.2 Cryptanalysis

There are many different attack model to decrypt a cryptosystem. The most common types are as follows:

- **Ciphertext Only Attack:** Oscar possesses a string of a ciphertext, $\mathbf{y}$.

# §2.2.2 Cryptanalysis

There are many different attack model to decrypt a cryptosystem. The most common types are as follows:

- **Ciphertext Only Attack:** Oscar possesses a string of a ciphertext, $\mathbf{y}$.
- **Known Plaintext Attack:** Oscar possesses a string of a plaintext, $\mathbf{x}$, and the corresponding ciphertext, $\mathbf{y}$.

# §2.2.2 Cryptanalysis

There are many different attack model to decrypt a cryptosystem. The most common types are as follows:

- **Ciphertext Only Attack:** Oscar possesses a string of a ciphertext, **y**.
- **Known Plaintext Attack:** Oscar possesses a string of a plaintext, **x**, and the corresponding ciphertext, **y**.
- **Chosen Plaintext Attack:** Oscar has obtained temporary access to the encryption machine. Hence he is able to choose plaintext(s) and construct the corresponding ciphertext(s).

# §2.2.2 Cryptanalysis

There are many different attack model to decrypt a cryptosystem. The most common types are as follows:

- **Ciphertext Only Attack:** Oscar possesses a string of a ciphertext, $\mathbf{y}$.
- **Known Plaintext Attack:** Oscar possesses a string of a plaintext, $\mathbf{x}$, and the corresponding ciphertext, $\mathbf{y}$.
- **Chosen Plaintext Attack:** Oscar has obtained temporary access to the encryption machine. Hence he is able to choose plaintext(s) and construct the corresponding ciphertext(s).
- **Chosen Ciphertext Attack:** Oscar has obtained temporary access to the decryption machine. Hence he is able to choose ciphertext(s) and construct the corresponding plaintext(s).

# §2.2.2 Cryptanalysis

There are many different attack model to decrypt a cryptosystem. The most common types are as follows:

- **Ciphertext Only Attack:** Oscar possesses a string of a ciphertext, **y**.
- **Known Plaintext Attack:** Oscar possesses a string of a plaintext, **x**, and the corresponding ciphertext, **y**.
- **Chosen Plaintext Attack:** Oscar has obtained temporary access to the encryption machine. Hence he is able to choose plaintext(s) and construct the corresponding ciphertext(s).
- **Chosen Ciphertext Attack:** Oscar has obtained temporary access to the decryption machine. Hence he is able to choose ciphertext(s) and construct the corresponding plaintext(s).

In each case, the objective of the adversary is to determine the key that was used. This would allow the opponent to decrypt any cipher text strings that are encrypted using the same key. We first consider the weakest type of attack, namely the ciphertext-only attack.

# §2.2.2 Cryptanalysis of Substitution Cipher

Oscar received the following message (with spaces) and he knows that the Substitution Cipher is used to encipher the following message:

UZ QSO VUOHXMOPV GPOZPEVSG
ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ
HMDZSHZO WSFP APPD TSVP
QUZW YMXUZUHSX EPYEPOPDZSZUFPO
MB ZWP FUPZ HMDJ UD TMOHMQ

# §2.2.2 Cryptanalysis of Substitution Cipher

Oscar received the following message (with spaces) and he knows that the Substitution Cipher is used to encipher the following message:

UZ QSO VUOHXMOPV GPOZPEVSG
ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ
HMDZSHZO WSFP APPD TSVP
QUZW YMXUZUHSX EPYEPOPDZSZUFPO
MB ZWP FUPZ HMDJ UD TMOHMQ

As a cryptanalyst, how can Oscar find the key to decipher it?
Remember that it is almost impossible to write all possible permutations unlike in Shift Cipher.

# §2.2.2 Cryptanalysis of Substitution Cipher

The frequency analysis of this ciphertext is given below:

| letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 2 | 2 | 0 | 6 | 6 | 4 | 2 | 7 | 1 | 1 | 0 | 0 | 8 |

| letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 0 | 9 | 16 | 3 | 0 | 10 | 3 | 10 | 5 | 4 | 5 | 2 | 14 |

# §2.2.2 Cryptanalysis of Substitution Cipher

The frequency analysis of this ciphertext is given below:

| letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 2 | 2 | 0 | 6 | 6 | 4 | 2 | 7 | 1 | 1 | 0 | 0 | 8 |

| letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 0 | 9 | 16 | 3 | 0 | 10 | 3 | 10 | 5 | 4 | 5 | 2 | 14 |

Compare it with the frequency table for English language.

# §2.2.2 Cryptanalysis of Substitution Cipher

The frequency analysis of this ciphertext is given below:

| letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 2 | 2 | 0 | 6 | 6 | 4 | 2 | 7 | 1 | 1 | 0 | 0 | 8 |

| letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 0 | 9 | 16 | 3 | 0 | 10 | 3 | 10 | 5 | 4 | 5 | 2 | 14 |

Compare it with the frequency table for English language.

From the frequency table, one could make a guess that $P \longrightarrow e$.

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | e | | | | | | | |
| U | Z | | Q | S | O | | V | U | O | H | X | M | O | P | V | | | | | | |
| | e | | | e | | | | | | | | | | | | e | | e | | | |
| G | P | O | Z | P | E | V | S | G | | Z | W | S | Z | | O | P | F | P | E | S | X |
| | | | | | | | | | | | | | | | | e | | | | | |
| U | D | B | M | E | T | S | X | | A | I | Z | | V | U | E | P | H | Z | | | |
| | | | | | | | | | | | | e | | | e | e | | | | | |
| H | M | D | Z | S | H | Z | O | | W | S | F | P | | A | P | P | D | | | | |
| | | | e | | | | | | | | | | | | | | | | | | |
| T | S | V | P | | Q | U | Z | W | | Y | M | X | U | Z | U | H | S | X | | | |
| | e | | | e | | e | | | | | | | e | | | | | | | | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O | | M | B | | Z | W | P |
| | | e | | | | | | | | | | | | | | | | | | | |
| F | U | P | Z | | H | M | D | J | | U | D | | T | M | O | H | M | Q | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| * | * | * | * | P | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the frequency of Z, which is 14. So one can conjecture that $d_k(Z) = \{t, a, o, i, n, s, h, r\}$ in that order.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the frequency of Z, which is 14. So one can conjecture that $d_k(Z) = \{t, a, o, i, n, s, h, r\}$ in that order.

Since the code word ZWP occurs in the encrypted message, with the assumption that $d_k(P) = e$, one can conjecture that $d_k(\text{ZWP}) = \text{the}$, which is the most common trigram.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the frequency of Z, which is 14. So one can conjecture that $d_k(Z) = \{t, a, o, i, n, s, h, r\}$ in that order.

Since the code word ZWP occurs in the encrypted message, with the assumption that $d_k(P) = e$, one can conjecture that $d_k(\text{ZWP}) = \text{the}$, which is the most common trigram.

Hence we conjecture further that $d_k(Z) = t$ and $d_k(W) = h$.

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | t | | | | | | | | | | | | | e | | | | | | | |
| U | Z | | Q | S | O | | V | U | O | H | X | M | O | P | V | | | | | | |
| | e | | t | e | | | | | | t | h | | t | | | e | | e | | | |
| G | P | O | Z | P | E | V | S | G | | Z | W | S | Z | | O | P | F | P | E | S | X |
| | | | | | | | | | | | t | | | | | e | | t | | | |
| U | D | B | M | E | T | S | X | | A | I | Z | | V | U | E | P | H | Z | | | |
| | | | t | | | t | | | h | | | e | | | e | e | | | | | |
| H | M | D | Z | S | H | Z | O | | W | S | F | P | | A | P | P | D | | | | |
| | | | e | | | | t | h | | | | | | t | | | | | | | |
| T | S | V | P | | Q | U | Z | W | | Y | M | X | U | Z | U | H | S | X | | | |
| | e | | | e | | e | | t | | t | | | e | | | | | | t | h | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O | | M | B | | Z | W | P |
| | | e | t | | | | | | | | | | | | | | | | | | |
| F | U | P | Z | | H | M | D | J | | U | D | | T | M | O | H | M | Q | | | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | P | * | * | W | * | * | * | * | * | * | * | * | * | * | * | Z | * | * | * | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of S and

$$\text{Z W S Z} \longrightarrow \text{t h * t}$$

## §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of S and

$$\mathrm{Z\ W\ S\ Z} \longrightarrow \mathrm{t\ h\ {*}\ t}$$

and similarly by considering the frequencies of Q and U together with the four letter code

$$\mathrm{Q\ U\ Z\ W} \longrightarrow {*}\ {*}\ \mathrm{t\ h}$$

one can conjecture that:

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of S and

$$\text{Z W S Z} \longrightarrow \text{t h * t}$$

and similarly by considering the frequencies of Q and U together with the four letter code

$$\text{Q U Z W} \longrightarrow \text{* * t h}$$

one can conjecture that:

- $d_k(S) = a$

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of S and

$$\text{Z W S Z} \longrightarrow \text{t h * t}$$

and similarly by considering the frequencies of Q and U together with the four letter code

$$\text{Q U Z W} \longrightarrow \text{* * t h}$$

one can conjecture that:

- $d_k(S) = a$
- $d_k(Q) = w$ and

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of S and

$$\text{Z W S Z} \longrightarrow \text{t h * t}$$

and similarly by considering the frequencies of Q and U together with the four letter code

$$\text{Q U Z W} \longrightarrow \text{* * t h}$$

one can conjecture that:

- $d_k(S) = a$
- $d_k(Q) = w$ and
- $d_k(U) = i$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i | t |  | w | a |  |  |  | i |  |  |  |  |  | e |  |  |  |  |  |  |  |
| U | Z |  | Q | S | O |  | V | U | O | H | X | M | O | P | V |  |  |  |  |  |  |
|  | e |  | t | e |  |  | a |  |  | t | h | a | t |  |  | e |  | e |  | a |  |
| G | P | O | Z | P | E | V | S | G |  | Z | W | S | Z |  | O | P | F | P | E | S | X |
| i |  |  |  |  |  | a |  |  |  |  | t |  |  | i |  | e |  | t |  |  |  |
| U | D | B | M | E | T | S | X |  | A | I | Z |  | V | U | E | P | H | Z |  |  |  |
|  |  |  | t | a |  | t |  |  | h | a |  | e |  |  | e | e |  |  |  |  |  |
| H | M | D | Z | S | H | Z | O |  | W | S | F | P |  | A | P | P | D |  |  |  |  |
|  | a |  | e |  | w | i | t | h |  |  |  |  | i | t | i |  | a |  |  |  |  |
| T | S | V | P |  | Q | U | Z | W |  | Y | M | X | U | Z | U | H | S | X |  |  |  |
|  | e |  |  | e |  | e |  | t | a | t | i |  | e |  |  |  |  |  | t | h | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O |  | M | B |  | Z | W | P |
|  | i | e | t |  |  |  |  |  |  | i |  |  |  |  |  |  |  | w |  |  |  |
| F | U | P | Z |  | H | M | D | J |  | U | D |  | T | M | O | H | M | Q |  |  |  |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | * | * | * | P | * | * | W | U | * | * | * | * | * | * | * | * | * | * | Z | * | * | Q | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of O together with

$$\text{Q S O} \rightarrow \text{w a *}$$

one can conclude that

$$d_k(O) = s.$$

# §2.2.2 Cryptanalysis of Substitution Cipher

Now by considering the frequency of O together with

$$\text{Q S O} \rightarrow \text{w a *}$$

one can conclude that

$$d_k(O) = s.$$

Similarly by considering the code

$$\text{W S F P} \rightarrow \text{h a * e}$$

and the frequency of F, one can conclude that

$$d_k(F) = v.$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i | t | | w | a | s | | | i | s | | | | s | e | | | | | | | |
| U | Z | | Q | S | O | | V | U | O | H | X | M | O | P | V | | | | | | |
| | e | s | t | e | | | a | | | t | h | a | t | | s | e | v | e | | a | |
| G | P | O | Z | P | E | V | S | G | | Z | W | S | Z | | O | P | F | P | E | S | X |
| i | | | | | | a | | | | | t | | | i | | e | | t | | | |
| U | D | B | M | E | T | S | X | | A | I | Z | | V | U | E | P | H | Z | | | |
| | | | t | a | | t | s | | h | a | v | e | | | e | e | | | | | |
| H | M | D | Z | S | H | Z | O | | W | S | F | P | | A | P | P | D | | | | |
| | a | | e | | w | i | t | h | | | | | i | t | i | | a | | | | |
| T | S | V | P | | Q | U | Z | W | | Y | M | X | U | Z | U | H | S | X | | | |
| | e | | | e | s | e | | t | a | t | i | v | e | s | | | | | t | h | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O | | M | B | | Z | W | P |
| v | i | e | t | | | | | | | i | | | | | s | | | w | | | |
| F | U | P | Z | | H | M | D | J | | U | D | | T | M | O | H | M | Q | | | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | * | * | * | P | * | * | W | U | * | * | * | * | * | * | * | * | * | O | Z | * | F | Q | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice the top eight frequent letters (after P) in this enciphered text: $\{Z, S, U, M, O, H, D, E\}$.

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice the top eight frequent letters (after P) in this enciphered text: $\{Z, S, U, M, O, H, D, E\}$.

So $\{M, H, D, E\} \longrightarrow \{o, n, r\}$ Why?

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice the top eight frequent letters (after P) in this enciphered text: $\{Z, S, U, M, O, H, D, E\}$.

So $\{M, H, D, E\} \longrightarrow \{o, n, r\}$ Why?

Now by considering U D $\longrightarrow$ i *, one can conjecture that

$$d_k(D) = n \, (\text{Why?})$$

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice the top eight frequent letters (after P) in this enciphered text: $\{Z, S, U, M, O, H, D, E\}$.

So $\{M, H, D, E\} \longrightarrow \{o, n, r\}$ Why?

Now by considering U D $\longrightarrow$ i *, one can conjecture that

$$d_k(D) = n \, (\text{Why?})$$

One can also guess that

$$d_k(E) = r \, (\text{Hint: See O P F P E S X})$$
$$d_k(M) = o \, (\text{Hint: See M B})$$

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice the top eight frequent letters (after P) in this enciphered text: $\{Z, S, U, M, O, H, D, E\}$.

So $\{M, H, D, E\} \longrightarrow \{o, n, r\}$ Why?

Now by considering U D $\longrightarrow$ i *, one can conjecture that

$$d_k(D) = n \,(\text{Why?})$$

One can also guess that

$$d_k(E) = r \,(\text{Hint: See O P F P E S X})$$
$$d_k(M) = o \,(\text{Hint: See M B})$$

In addition,

$$d_k(X) = l \text{ and } d_k(B) = f$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i | t | | w | a | s | | | i | s | | l | o | s | e | | | | | | | |
| U | Z | | Q | S | O | | V | U | O | H | X | M | O | P | V | | | | | | |
| | e | s | t | e | r | | a | | | t | h | a | t | | s | e | v | e | r | a | l |
| G | P | O | Z | P | E | V | S | G | | Z | W | S | Z | | O | P | F | P | E | S | X |
| i | n | f | o | r | | a | l | | | | t | | | i | r | e | | t | | | |
| U | D | B | M | E | T | S | X | | A | I | Z | | V | U | E | P | H | Z | | | |
| | o | n | t | a | | t | s | | h | a | v | e | | | e | e | n | | | | |
| H | M | D | Z | S | H | Z | O | | W | S | F | P | | A | P | P | D | | | | |
| | a | | e | | w | i | t | h | | | o | l | i | t | i | | a | l | | | |
| T | S | V | P | | Q | U | Z | W | | Y | M | X | U | Z | U | H | S | X | | | |
| r | e | | r | e | s | e | n | t | a | t | i | v | e | s | | o | f | | t | h | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O | | M | B | | Z | W | P |
| v | i | e | t | | | o | n | | | i | n | | | o | s | | o | w | | | |
| F | U | P | Z | | H | M | D | J | | U | D | | T | M | O | H | M | Q | | | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | * | * | * | P | B | * | W | U | * | * | X | * | D | M | * | * | E | O | Z | * | F | Q | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

By considering next two letters in the frequency tables, one could consider

$$\{H, V\} \longrightarrow \{c, d\}$$

# §2.2.2 Cryptanalysis of Substitution Cipher

By considering next two letters in the frequency tables, one could consider

$$\{H, V\} \longrightarrow \{c, d\}$$

By considering the third word in the encrypted text, we can conjecture that

$$d_k(H) = c$$

$$d_k(V) = d$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i | t | | w | a | s | | d | i | s | c | l | o | s | e | d | | | | | | |
| U | Z | | Q | S | O | | V | U | O | H | X | M | O | P | V | | | | | | |
| | e | s | t | e | r | d | a | | | t | h | a | t | | s | e | v | e | r | a | l |
| G | P | O | Z | P | E | V | S | G | | Z | W | S | Z | | O | P | F | P | E | S | X |
| i | n | f | o | r | | a | l | | | | t | | d | i | r | e | c | t | | | |
| U | D | B | M | E | T | S | X | | A | I | Z | | V | U | E | P | H | Z | | | |
| c | o | n | t | a | c | t | s | | h | a | v | e | | | e | e | n | | | | |
| H | M | D | Z | S | H | Z | O | | W | S | F | P | | A | P | P | D | | | | |
| | a | d | e | | w | i | t | h | | | o | l | i | t | i | c | a | l | | | |
| T | S | V | P | | Q | U | Z | W | | Y | M | X | U | Z | U | H | S | X | | | |
| r | e | | r | e | s | e | n | t | a | t | i | v | e | s | | o | f | | t | h | e |
| E | P | Y | E | P | O | P | D | Z | S | Z | U | F | P | O | | M | B | | Z | W | P |
| v | i | e | t | | c | o | n | | | i | n | | | o | s | c | o | w | | | |
| F | U | P | Z | | H | M | D | J | | U | D | | T | M | O | H | M | Q | | | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | * | H | V | P | B | * | W | U | * | * | X | * | D | M | * | * | E | O | Z | * | F | Q | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

What is the decrypted text and the key?

# §2.2.2 Cryptanalysis of Substitution Cipher

What is the decrypted text and the key?

Spaces in the previous encrypted message have helped us to decrypt the message. In order to make the message more secure, mostly the encrypted messages do not contain spaces.

# §2.2.2 Cryptanalysis of Substitution Cipher

Substitution Cipher is used to encrypt the following message. Decrypt the message:

```
LNWRWDWAPRTHSAKSHCSD
WARKWRBJWXSKWVZWVBAY
XBIDWSHBNWVWWRZVIBIV
BNWAICNBSHBNWFWSFOWB
 SPOBWASABSPJSOIVNIB
```

# §2.2.2 Cryptanalysis of Substitution Cipher

The frequency table for the previous cipher text is given below:

| letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 7 | 12 | 2 | 3 | 0 | 2 | 0 | 4 | 6 | 2 | 3 | 1 | 0 |

| letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 6 | 3 | 3 | 0 | 5 | 11 | 1 | 0 | 6 | 17 | 2 | 1 | 2 |

# §2.2.2 Cryptanalysis of Substitution Cipher

The frequency table for the previous cipher text is given below:

| letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 7 | 12 | 2 | 3 | 0 | 2 | 0 | 4 | 6 | 2 | 3 | 1 | 0 |

| letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frequency | 6 | 3 | 3 | 0 | 5 | 11 | 1 | 0 | 6 | 17 | 2 | 1 | 2 |

From the frequency of W we might conjecture that $d_k(\mathrm{W}) = \mathrm{e}$.

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | e | | e | | e | | | | | | | | | | | | | |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | | | | e | | | | e | | | | e | | | e | | | | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | | | | e | | | | | e | | e | e | | | | | | | |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| | | e | | | | | | | | | | e | | e | | | | e | |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| | | | | e | | | | | | | | | | | | | | | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | e | | e | | e | | | | | | | | | | | | | |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | | | | e | | | | e | | | | e | | | e | | | | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | | | | e | | | | | e | | e | e | | | | | | | |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| | | e | | | | | | | | | | e | | e | | | | e | |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| | | | | e | | | | | | | | | | | | | | | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

The remaining cipher text characters that occur at least six times (each) are A, B, I, N, S, V. We might expect that these letters are encryptions of (a subset of) t, a, o, i, n, s, h, r, but the frequencies do not vary enough to tell us what might be the correspondence.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

The most common digrams of this type are NW and WA (four times each).

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

The most common digrams of this type are NW and WA (four times each).

Notice that the trigram BNW occurs three times. Also B occurs frequently.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

The most common digrams of this type are NW and WA (four times each).

Notice that the trigram BNW occurs three times. Also B occurs frequently.

So we might conjecture that

$$d_k(\mathrm{B}) = \text{ t and } d_k(\mathrm{N}) = \text{ h}$$

## §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

The most common digrams of this type are NW and WA (four times each).

Notice that the trigram BNW occurs three times. Also B occurs frequently.

So we might conjecture that

$$d_k(\mathrm{B}) = \texttt{t} \text{ and } d_k(\mathrm{N}) = \texttt{h}$$

The digram WA occurs frequently in the cipher text (four times) and `er` is a common digram.

# §2.2.2 Cryptanalysis of Substitution Cipher

Now consider the digrams of the form $*$W and W$*$.

The most common digrams of this type are NW and WA (four times each).

Notice that the trigram BNW occurs three times. Also B occurs frequently.

So we might conjecture that

$$d_k(\mathsf{B}) = \text{ t and } d_k(\mathsf{N}) = \text{ h}$$

The digram WA occurs frequently in the cipher text (four times) and `er` is a common digram.

So we might try $d_k(\mathsf{A}) = $ r.

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | h | e | | e | | e | r | | | | | | r | | | | | | |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | | | e | | t | | e | | | | e | | | e | | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | | | e | | | t | h | e | | e | e | | | | | t | | |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | | | h | t | | | t | h | e | | e | | | | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| | | | t | e | r | | r | t | | | | | | | | h | | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | W | * | * | N | * | * | * | * | * | * | * | * | * | A | * | B | * | * | * | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Since the frequency of the first letter L is 1, by checking low frequency letters in order, one can guess that

$$d_k(\mathsf{L}) = \ \mathsf{w}$$

and hence

$$d_k(\mathsf{R}) = \ \mathsf{n}$$

and

$$d_k(\mathsf{D}) = \ \mathsf{v}.$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | h | e | n | e | v | e | r | | n | | | | r | | | | | | v |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | n | | e | n | t | | e | | | | e | | | e | | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | | v | e | | | t | h | e | | e | e | n | | | | t | | |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | | | h | t | | | t | h | e | | e | | | | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| | | | t | e | r | | r | t | | | | | | | | h | | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| * | * | * | * | W | * | * | N | * | * | * | * | * | R | * | * | * | A | * | B | * | D | L | * | * | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

The remaining cipher text characters that occur at least six times (each) are I, S, V. We might expect that these letters are encryptions of (a subset of) a, o, i, s, and in particular, all of these are vowels a, o, i, or two of these are vowels a,o,i and one of them is s.

# §2.2.2 Cryptanalysis of Substitution Cipher

The remaining cipher text characters that occur at least six times (each) are I, S, V. We might expect that these letters are encryptions of (a subset of) a, o, i, s, and in particular, all of these are vowels a, o, i, or two of these are vowels a,o,i and one of them is s.

Notice that S H appears thrice and S H B N W ($\rightarrow$ * * t h e) twice, one could guess that

$$d_k(\text{S}) = \text{ o } \text{ (vowel)}$$

$$d_k(\text{H}) = \text{ f}$$

# §2.2.2 Cryptanalysis of Substitution Cipher

The remaining cipher text characters that occur at least six times (each) are I, S, V. We might expect that these letters are encryptions of (a subset of) a, o, i, s, and in particular, all of these are vowels a, o, i, or two of these are vowels a,o,i and one of them is s.

Notice that S H appears thrice and S H B N W ($\rightarrow$ * * t h e) twice, one could guess that

$$d_k(\mathsf{S}) = \text{ o (vowel)}$$

$$d_k(\mathsf{H}) = \text{ f}$$

Now we might expect that I and V are encryption of a subset of a, i, s. Due to W V W W $\longrightarrow$ e * e e, we may try that

$$d_k(\mathsf{V}) = \text{ s}$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | h | e | n | e | v | e | r | | n | | f | o | r | | o | f | | o | v |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | n | | e | n | t | | e | | o | | e | s | | e | s | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | | v | e | o | f | t | h | e | s | e | e | n | | s | | t | | s |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | | | h | t | o | f | t | h | e | | e | o | | | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| o | | | t | e | r | o | r | t | o | | | o | | | s | h | | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | W | H | * | N | * | * | * | * | * | R | S | * | * | A | V | B | * | D | L | * | * | * |

## §2.2.2 Cryptanalysis of Substitution Cipher

From the first line of the encrypted message. one can guess that P is an encryption of one of the remaining vowels a, i, u (Why?)

# §2.2.2 Cryptanalysis of Substitution Cipher

From the first line of the encrypted message. one can guess that P is an encryption of one of the remaining vowels a, i, u (Why?)

Since P occurs thrice, and so it is likely a or i. Now T occurs only once and hence represents a low frequency letter. So one can conjecture that
P R T $\rightarrow$ a n y

# §2.2.2 Cryptanalysis of Substitution Cipher

From the first line of the encrypted message. one can guess that P is an encryption of one of the remaining vowels a, i, u (Why?)

Since P occurs thrice, and so it is likely a or i. Now T occurs only once and hence represents a low frequency letter. So one can conjecture that
P R T → a n y

and hence

$$d_k(\mathrm{P}) = \text{ a}$$

This yields,

$$d_k(\mathrm{I}) = \text{ i}$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | h | e | n | e | v | e | r | a | n | y | f | o | r | | o | f | | o | v |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | n | | e | n | t | | e | | o | | e | s | | e | s | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | i | v | e | o | f | t | h | e | s | e | e | n | | s | i | t | i | s |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | i | | h | t | o | f | t | h | e | | e | o | | | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| o | a | | t | e | r | o | r | t | o | a | | o | | i | s | h | i | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| P | * | * | * | W | H | * | N | I | * | * | * | * | R | S | * | * | A | V | B | * | D | L | * | T | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

Next two letters in the frequency table of enciphered text are K and O (each appears thrice).

Their likely decryption are (according to frequency table):
( d, l) or if it fails, then to (c, u, m) in that order.

# §2.2.2 Cryptanalysis of Substitution Cipher

Next two letters in the frequency table of enciphered text are K and O (each appears thrice).

Their likely decryption are (according to frequency table):
( d, l) or if it fails, then to (c, u, m) in that order.

Possible conjectures:

$$d_k(\mathrm{K}) = \text{ m } (\textit{why?})$$

$$d_k(\mathrm{O}) = \text{ l } (\textit{why?})$$

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | h | e | n | e | v | e | r | a | n | y | f | o | r | m | o | f | | o | v |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | n | m | e | n | t | | e | | o | m | e | s | | e | s | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | i | v | e | o | f | t | h | e | s | e | e | n | | s | i | t | i | s |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | i | | h | t | o | f | t | h | e | | e | o | | l | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| o | a | l | t | e | r | o | r | t | o | a | | o | l | i | s | h | i | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| P | * | * | * | W | H | * | N | I | * | * | O | K | R | S | * | * | A | V | B | * | D | L | * | T | * |

# §2.2.2 Cryptanalysis of Substitution Cipher

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w | h | e | n | e | v | e | r | a | n | y | f | o | r | m | o | f | | o | v |
| L | N | W | R | W | D | W | A | P | R | T | H | S | A | K | S | H | C | S | D |
| e | r | n | m | e | n | t | | e | | o | m | e | s | | e | s | t | r | |
| W | A | R | K | W | R | B | J | W | X | S | K | W | V | Z | W | V | B | A | Y |
| | t | i | v | e | o | f | t | h | e | s | e | e | n | | s | i | t | i | s |
| X | B | I | D | W | S | H | B | N | W | V | W | W | R | Z | V | I | B | I | V |
| t | h | e | r | i | | h | t | o | f | t | h | e | | e | o | | l | e | t |
| B | N | W | A | I | C | N | B | S | H | B | N | W | F | W | S | F | O | W | B |
| o | a | l | t | e | r | o | r | t | o | a | | o | l | i | s | h | i | t | |
| S | P | O | B | W | A | S | A | B | S | P | J | S | O | I | V | N | I | B | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| P | * | * | * | W | H | * | N | I | * | * | O | K | R | S | * | * | A | V | B | * | D | L | * | T | * |

Find the key and decrypt the message.

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice that the cryptanalysis of Substitution Cipher depends on the language.

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice that the cryptanalysis of Substitution Cipher depends on the language.

**Advantage of Substitution Cipher:** Large key space

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice that the cryptanalysis of Substitution Cipher depends on the language.

**Advantage of Substitution Cipher:** Large key space

**Disadavange:**

- It is still relatively easy to decrypt, usually in few seconds by an efficient computer program, though it is hard to remember the key.

# §2.2.2 Cryptanalysis of Substitution Cipher

Notice that the cryptanalysis of Substitution Cipher depends on the language.

**Advantage of Substitution Cipher:** Large key space

**Disadavange:**

- It is still relatively easy to decrypt, usually in few seconds by an efficient computer program, though it is hard to remember the key.
- Our cryptanalysis method discussed for Substitution Cipher will not work well for lipogram texts that are unusually deviated from normal. For example, Gadsby is a 1939 novel written by Ernest Vincent Wright which does not include the letter 'e'.