Symmetric Encryption

Part 2

Symmetric Encryption

Outline

- Monoalphabetic Substitution Cipher
- Simple Substitution Cipher
- Frequency Analysis
- Polyalphabetic Substitution Cipher
- Vigenère Cipher
- Transposition Cipher
- Columnar Transposition Cipher

Monoalphabetic Substitution Cipher

- A monoalphabetic cipher is a simple form of substitution cipher in cryptography where each letter of the plaintext is replaced by a corresponding letter from a fixed substitution alphabet.
- In a monoalphabetic cipher, each letter in the plaintext alphabet is mapped to a unique letter in the ciphertext alphabet.
- For example, if the letter "A" in the plaintext is always replaced with the letter "D" in the ciphertext, every occurrence of "A" in the message will be substituted with "D".
- Monoalphabetic ciphers are relatively easy to understand and implement, but they are also highly vulnerable to frequency analysis attacks.
- Examples: Caesar Cipher, Simple Substitution Cipher, Atbash Cipher, Keyword Cipher, Pigpen Cipher.

Simple Substitution Cipher

- A Simple Substitution Cipher is a type of monoalphabetic cipher where each letter in the plaintext is replaced by a different letter in the ciphertext.
- To create a Simple Substitution Cipher, a substitution key or alphabet is chosen.
- This substitution key is a random permutation of the letters in the alphabet.
- Each letter in the plaintext is then replaced with its corresponding letter from the substitution key.

Simple Substitution Cipher

- Example: The substitution key is as follows –

Plaintext	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
Ciphertext	**D**	**K**	**V**	**Q**	**F**	**I**	**B**	**J**	**W**	**P**	**E**	**S**	**C**	**X**	**H**	**T**	**M**	**Y**	**A**	**U**	**O**	**L**	**R**	**G**	**Z**	**N**

- Using this substitution key, the following would be a plaintext to ciphertext mapping:

Plaintext	ifwewishtoreplaceletters
Ciphertext	**WIRFRWAJUHYFTSDVFSFUUFYA**

Simple Substitution Cipher

Security of Simple Substitution Cipher

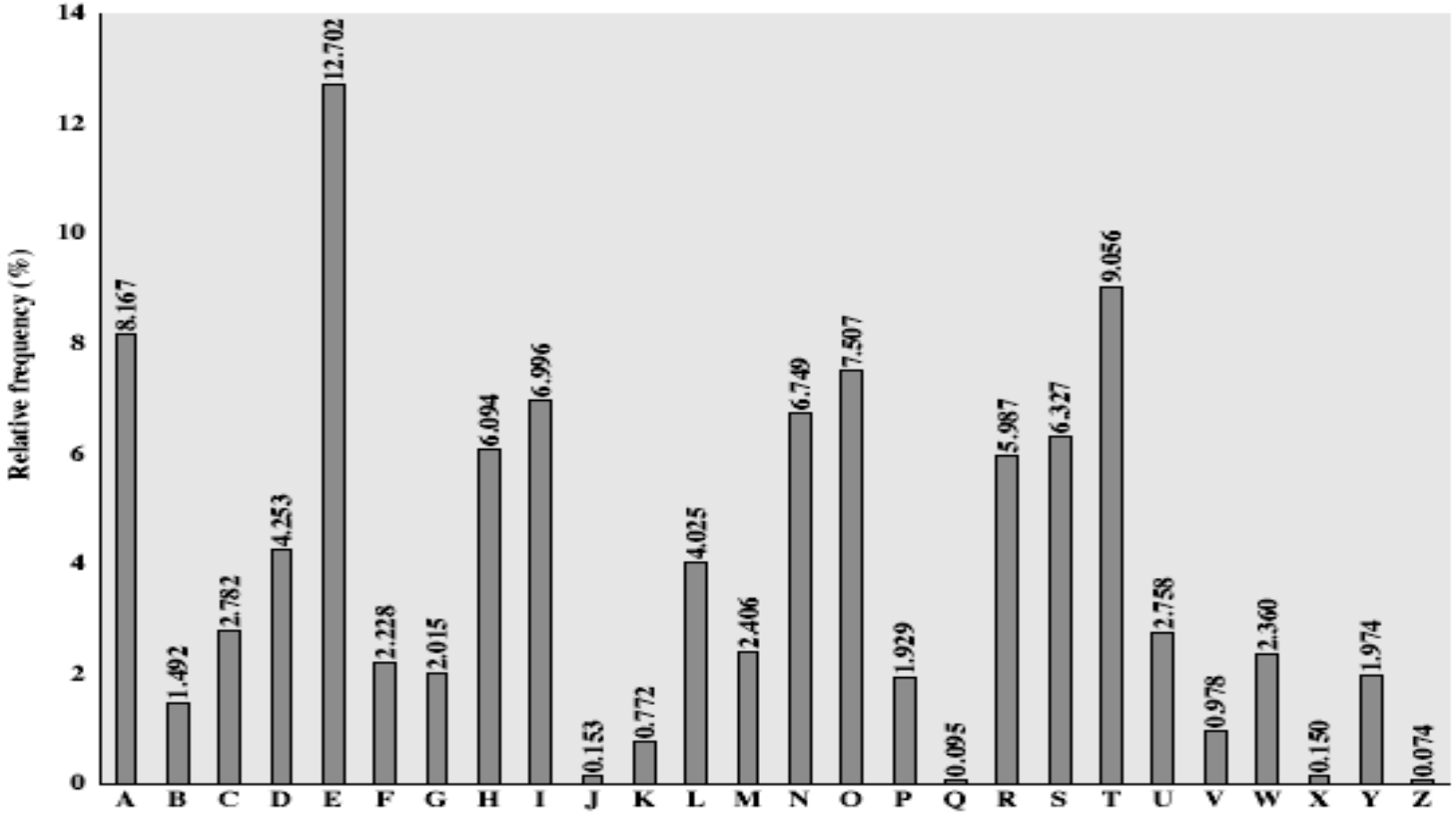
- Simple Substitution Cipher has a total of 26! keys.
- With so many keys, one can think Simple Substitution Ciphers are secure, but it is a wrong assumption.
- Simple Substitution Ciphers are vulnerable to frequency analysis attacks.

Frequency Analysis

- In cryptanalysis, **Frequency Analysis** is a technique of study of breaking codes and ciphers.
- It involves analyzing the frequency distribution of letters, symbols, or other linguistic units in a given piece of encrypted text (ciphertext) in order to gain insights about the underlying plaintext.
- The basic idea behind frequency analysis is that in any language, certain letters or symbols appear more frequently than others.
- For example, in English, the letter "E" is the most commonly used letter, followed by "T," "A," and so on.

Frequency Analysis

English Letter Frequencies



Frequency Analysis

- The key concept is that monoalphabetic substitution ciphers do not change relative letter frequencies.
- Discovered and studied extensive by Arab Muslim polymath Al-Kindi in 9^{th} century.
- By examining the frequency of letters or symbols in the ciphertext, an attacker can make educated guesses about the substitution pattern used in the encryption.

Frequency Analysis

Example Cryptanalysis

- Ciphertext:

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

- Count relative letter frequencies (see text)
- Assume 'P' and 'Z' are 'e' and 't'
- Guess 'ZW' is 'th' and hence 'ZWP' is 'the'
- Proceed with a trial-and-error approach.

Frequency Analysis

Example Cryptanalysis

- Ciphertext:

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

- Count relative letter frequencies (see text)
- Assume 'P' and 'Z' are 'e' and 't'
- Guess 'ZW' is 'th' and hence 'ZWP' is 'the'
- Proceed a trial-and-error to finally get the plaintext:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Frequency Analysis

Counter Measures

- To counter frequency analysis attacks, more complex encryption techniques such as polyalphabetic ciphers, transposition ciphers, or modern cryptographic algorithms like AES or RSA are used.
- These methods make it much more difficult to discern patterns in the ciphertext and prevent attackers from exploiting the frequency distribution of letters.

Polyalphabetic Substitution Cipher

- Polyalphabetic substitution cipher is a cryptographic technique that involves the use of multiple substitution alphabets.
- In a polyalphabetic substitution cipher, the substitution rules vary based on the position of the letter within the plaintext.
- This approach makes frequency analysis (cryptanalysis) harder with more alphabets to guess.
- Examples: Vigenère Cipher, Beaufort Cipher, Autokey Cipher, Playfair Cipher, and Hill Cipher.

Vigenère Cipher

- The most well-known example of a polyalphabetic cipher is the Vigenère cipher.
- The Vigenère cipher uses a keyword to determine the shifting of letters in multiple Caesar ciphers.
- The keyword is repeated to match the length of the plaintext, and each letter of the keyword determines the shift value for the corresponding letter of the plaintext.

Vigenère Cipher

Example

- Key: **deceptive**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- To encrypt the plaintext using the Vigenère cipher with the keyword "deceptive", repeat the keyword to match the length of the plaintext.

Key	deceptivedeceptivedeceptive
Plaintext	**wearediscoveredsaveyourself**
Ciphertext	**ZICVTWQNGRZGVTWAVZHCQYGLMGJ**

- To encrypt the first letter 'w', shift it by 3 positions (the position of 'd' in the alphabet), resulting in 'Z'. The second letter 'e' is shifted by 4 positions ('e' in the alphabet), resulting in 'I'. The process continues for each letter using the corresponding letter of the keyword for the shift value.

Vigenère Cipher

Exercise

- Key: **lemon**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Encryption:

Key	lemon
Plaintext	**a t t a c k a t d a w n**
Ciphertext	

Vigenère Cipher

Exercise

- Key: **lemon**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Key	l e m o n l e m o n l e
Plaintext	**a t t a c k a t d a w n**
Ciphertext	**L X F O P V E F R N H R**

- Encryption: To encrypt the first letter 'A', we shift it by 11 positions (the position of 'L' in the alphabet), resulting in 'L', The second letter 'T' is shifted by 4 positions ('E' in the alphabet), resulting in 'X', The process continues for each letter using the corresponding letter of the keyword for the shift value.

Vigenère Cipher

Exercise

- Key: **lemon**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Decryption: To decrypt the ciphertext back to the plaintext, the same keyword is used, but this time, the letters are shifted in the opposite direction.

Key	l e m o n l e m o n l e
Ciphertext	**L X F O P V E F R N H R**
Plaintext	**a t t a c k a t d a w n**

Transposition Cipher

- Transposition ciphers are a type of cryptographic technique that ***involves rearranging (i.e., permutations) the order of letters or characters in a message without altering the actual letters themselves***.
- Such ciphers aim to ***obscure the message's structure*** and make it more challenging to decipher without the knowledge of the specific transposition method used.
- Transposition ciphers can operate on individual letters, groups of letters, or even blocks of characters.
- The rearrangement of the text can occur horizontally (row-wise) or vertically (column-wise).
- A few common types of transposition ciphers are Columnar Transposition Cipher, Rail Fence Cipher, Route Cipher, and Scytale Cipher.

Columnar Transposition Cipher

- This type of cipher rearranges the characters of a plaintext message by writing it out in a grid of a fixed number of columns and then reading the ciphertext off column by column.
- The keyword determines the order in which the columns are read.

Columnar Transposition Cipher

Example 1:

- Plaintext: “hello world”
- Keyword: “**KEY**”
- No of rows: 4
- The plaintext is written into a grid with three columns according to the keyword.
- Rearrange the columns based on the alphabetical order of the keyword letters "E", "K", "Y".
- Read the columns from left to right, top to bottom.
- The ciphertext would be EOR#HLODLWL#

K	E	Y
h	e	l
l	o	w
o	r	l
d	#	#

E	K	Y
e	h	l
o	l	w
r	o	l
#	d	#

Columnar Transposition Cipher

- For decryption, reverse the steps using the same keyword “KEY”.

E	K	Y
e	h	l
o	l	w
r	o	l
#	d	#

- Read the rows from top to bottom, left to right.
- The plaintext would be “hello world”.

K	E	Y
h	e	l
l	o	w
o	r	l
d	#	#

Columnar Transposition Cipher

Example 2:

- Plaintext: `attack postponed until two am`
- Keyword: **`4312567`**
- Number of rows: 4
- The plaintext is written into a grid with three columns according to the keyword.
- Ciphertext:

  TTNAAPTMTSUOAODWCOI#KNL#PET#

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	#	#	#

Columnar Transposition Cipher

- Get the plaintext back from the ciphertext: solve it as an exercise.

Columnar Transposition Cipher

Example 3: Encryption

- Plaintext: `kindness echoes`
- Keyword: **`512634`**
- Number of rows: 3
- The plaintext is written into a grid with three columns according to the keyword.
- For encryption, columns are rearranged based on the sorted keyword.
- Ciphertext: ISSNE#NH#EO#KSEDC#

5	1	2	6	3	4
k	i	n	d	n	e
s	s	e	c	h	o
e	s	#	#	#	#

1	2	3	4	5	6
i	n	n	e	k	d
s	e	h	o	s	c
s	#	#	#	e	#

Columnar Transposition Cipher

Example 3: Decryption

- Ciphertext: ISSNE#NH#EO#KSEDC#
- Keyword: **512634**
- Number of rows: 3
- The ciphertext is written into a grid with three columns according to the sorted keyword.
- Plaintext: `kindness echoes`

1	2	3	4	5	6
i	n	n	e	k	d
s	e	h	o	s	c
s	#	#	#	e	#

5	1	2	6	3	4
k	i	n	d	n	e
s	s	e	c	h	o
e	s	#	#	#	#

Columnar Transposition Cipher

Example 4: Encryption

- Plaintext: `unity defines us`
- Keyword: **`351426`**
- Number of rows: 3
- The plaintext is written into a grid with three columns according to the keyword.
- For encryption, columns are rearranged based on the sorted keyword.
- Ciphertext:

  II#YE#UEUTN#NFSDS#

3	5	1	4	2	6
u	n	i	t	y	d
e	f	i	n	e	s
u	s	#	#	#	#

1	2	3	4	5	6
i	y	u	t	n	d
i	e	e	n	f	s
#	#	u	#	s	#

Columnar Transposition Cipher

Example 4: Decryption

- Ciphertext: II#YE#UEUTN#NFSDS#
- Keyword: **351426**
- Number of rows: 3
- The ciphertext is written into a grid with three columns according to the sorted keyword.
- Plaintext: unity defines us

1	2	3	4	5	6
i	y	u	t	n	d
i	e	e	n	f	s
#	#	u	#	s	#

3	5	1	4	2	6
u	n	i	t	y	d
e	f	i	n	e	s
u	s	#	#	#	#