Shift Cipher and its cryptanalysis

Math 4175

§2.1.1. Goal of the Cryptography

- Enable two people, Alice and Bob, to communicate in a secured coded way so that the opponent, Oscar, cannot understand it.

§2.1.1. Goal of the Cryptography

- Enable two people, Alice and Bob, to communicate in a secured coded way so that the opponent, Oscar, cannot understand it.
- In Oscar's point of view, how to decode the secured message.

§2.1.1. Goal of the Cryptography

- Enable two people, Alice and Bob, to communicate in a secured coded way so that the opponent, Oscar, cannot understand it.
- In Oscar's point of view, how to decode the secured message.

In this chapter, we will learn:

- different ways to code or encipher a message by using a cryptosystem, and

§2.1.1. Goal of the Cryptography

- Enable two people, Alice and Bob, to communicate in a secured coded way so that the opponent, Oscar, cannot understand it.
- In Oscar's point of view, how to decode the secured message.

In this chapter, we will learn:

- different ways to code or encipher a message by using a cryptosystem, and
- how to decode or decipher a message by using corresponding cryptanalysis.

§2.1.1 Caesar Cipher

Let us start with a simple cryptosystem used by Julius Caesar, called Caesar Cipher.

§2.1.1 Caesar Cipher

Let us start with a simple cryptosystem used by Julius Caesar, called Caesar Cipher.

> Caesar coded the message by replacing each letter by the letter three places beyond in Roman alphabet

§2.1.1 Caesar Cipher

Let us start with a simple cryptosystem used by Julius Caesar, called Caesar Cipher.

> Caesar coded the message by replacing each letter by the letter three places beyond in Roman alphabet

Though Caesar used Roman alphabet, we shall use the present day alphabet to illustrate it by enciphering the message:

I came I saw I conquered

§2.1.1 Caesar Cipher

First let us replace each letter of the alphabet by a number from 0 to 25 (A $=0$, B $=1$, C $=2$, $\cdots$, Z $=25$), and so:

i	c	a	m	e	i	s	a	w	
8	2	0	12	4	8	18	0	22	
i	c	o	n	q	u	e	r	e	d
8	2	14	13	16	20	4	17	4	3

§2.1.1 Caesar Cipher

First let us replace each letter of the alphabet by a number from 0 to 25 (A = 0, B = 1, C = 2, $\cdots$, Z = 25), and so:

i	c	a	m	e	i	s	a	w	
8	2	0	12	4	8	18	0	22	
i	c	o	n	q	u	e	r	e	d
8	2	14	13	16	20	4	17	4	3

Now we add 3 to each number:

§2.1.1 Caesar Cipher

i	c	a	m	e	i	s	a	w	
8	2	0	12	4	8	18	0	22	
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
11	5	3	15	7	11	21	3	25	
i	c	o	n	q	u	e	r	e	d
8	2	14	13	16	20	4	17	4	3
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
11	5	17	16	19	23	7	20	7	6

§2.1.1 Caesar Cipher

$$
\begin{array}{cccccccccc}
\text{i} & \text{c} & \text{a} & \text{m} & \text{e} & \text{i} & \text{s} & \text{a} & \text{w} & \\
8 & 2 & 0 & 12 & 4 & 8 & 18 & 0 & 22 & \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
11 & 5 & 3 & 15 & 7 & 11 & 21 & 3 & 25 & \\
\text{i} & \text{c} & \text{o} & \text{n} & \text{q} & \text{u} & \text{e} & \text{r} & \text{e} & \text{d} \\
8 & 2 & 14 & 13 & 16 & 20 & 4 & 17 & 4 & 3 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
11 & 5 & 17 & 16 & 19 & 23 & 7 & 20 & 7 & 6
\end{array}
$$

Then convert each letter to the corresponding alphabet and this process yields:

I came I saw I conquered (original)
L FDPH L VDZ L FRQTXHUHG (ciphered)

§2.1.1 Shift Cipher

Caesar used number 3 to add (for whatever reason), which is called the key of Caesar Cipher, though we could use any other number n where $1 \leq n \leq 25$. In this case, the cryptosystem is called the Shift Cipher with key n.

§2.1.1 Shift Cipher

Caesar used number 3 to add (for whatever reason), which is called the key of Caesar Cipher, though we could use any other number n where $1 \leq n \leq 25$. In this case, the cryptosystem is called the Shift Cipher with key n.

Encrypt 'take bus at the mall' by using shift cipher with the key 12.

§2.1.1 Shift Cipher

Caesar used number 3 to add (for whatever reason), which is called the key of Caesar Cipher, though we could use any other number n where $1 \leq n \leq 25$. In this case, the cryptosystem is called the Shift Cipher with key n.

Encrypt 'take bus at the mall' by using shift cipher with the key 12.

Oscar received the following message and he knows that the Shift Cipher is used to encipher this message.

§2.1.1 Shift Cipher

Caesar used number 3 to add (for whatever reason), which is called the key of Caesar Cipher, though we could use any other number n where $1 \leq n \leq 25$. In this case, the cryptosystem is called the Shift Cipher with key n.

Encrypt 'take bus at the mall' by using shift cipher with the key 12.

Oscar received the following message and he knows that the Shift Cipher is used to encipher this message.

BPM VMOWBQIBQWVA NWZ I AMBBTMUMVB WN BPM ABZQSM IZM IB IV QUXIAAM ZMKWUUMVL EM QVKZMIAM WCZ WNNMZ

§2.1.1 Shift Cipher

Caesar used number 3 to add (for whatever reason), which is called the key of Caesar Cipher, though we could use any other number n where $1 \leq n \leq 25$. In this case, the cryptosystem is called the Shift Cipher with key n.

Encrypt 'take bus at the mall' by using shift cipher with the key 12.

Oscar received the following message and he knows that the Shift Cipher is used to encipher this message.

BPM VMOWBQIBQWVA NWZ I AMBBTMUMVB WN BPM ABZQSM
IZM IB IV QUXIAAM ZMKWUUMVL EM QVKZMIAM WCZ WNNMZ

As a cryptanalyst, how can Oscar find the key to decipher it?
Hint: There are only 25 possible keys and so one can do exhaustive key search.

§2.1.1 Shift Cipher

Systematic way: Consider the first word of the message BPM.

§2.1.1 Shift Cipher

Systematic way: Consider the first word of the message BPM.

Key	Numbers			Word
	1	15	12	BPM
1	0	14	11	AOL
2	25	13	10	ZNK
3	24	12	9	YMJ
4	23	11	8	XLI
5	22	10	7	WKH
6	21	9	6	VJG
7	20	8	5	UIF
8	19	7	4	THE

§2.1.1 Shift Cipher

Systematic way: Consider the first word of the message BPM.

Key	Numbers			Word
	1	15	12	BPM
1	0	14	11	AOL
2	25	13	10	ZNK
3	24	12	9	YMJ
4	23	11	8	XLI
5	22	10	7	WKH
6	21	9	6	VJG
7	20	8	5	UIF
8	19	7	4	THE

It seems key is 8!!

§2.1.1 Shift Cipher

Alternate way: Consider the single letter word I, which should be replaced with either I or A. It cannot be I itself (why?). So I should be replaced with A and hence the key seems to be 8.

§2.1.1 Shift Cipher

Alternate way: Consider the single letter word I, which should be replaced with either I or A. It cannot be I itself (why?). So I should be replaced with A and hence the key seems to be 8.

Confirm it by looking at the two letter words IB and IV which should be replaced with AM, AN, AS or AT.

§2.1.1 Shift Cipher

Alternate way: Consider the single letter word I, which should be replaced with either I or A. It cannot be I itself (why?). So I should be replaced with A and hence the key seems to be 8.

Confirm it by looking at the two letter words IB and IV which should be replaced with AM, AN, AS or AT.

Now go through the details of decipherment process to get the message.

§2.1.1 Shift Cipher

Alternate way: Consider the single letter word I, which should be replaced with either I or A. It cannot be I itself (why?). So I should be replaced with A and hence the key seems to be 8.

Confirm it by looking at the two letter words IB and IV which should be replaced with AM, AN, AS or AT.

Now go through the details of decipherment process to get the message.

The second alternate method is possible due to the spaces in the encrypted text. So usually there will be no spaces in the ciphered texts.

§2.1.1 Shift Cipher

Consider the ciphered text:

$\boxed{\text{IQXOAYQFAODKBFASDMBTK}}$

§2.1.1 Shift Cipher

Consider the ciphered text:

$$\boxed{\text{IQXOAYQFAODKBFASDMBTK}}$$

Find the key and decipher the message.

§2.1.1 Shift Cipher

Consider the ciphered text:

$$\boxed{\text{IQXOAYQFAODKBFASDMBTK}}$$

Find the key and decipher the message.

Disadvantage of Shift Cipher;

- There are only 25 possible keys and so it is not difficult to decipher the text created by Shift Cipher.

§2.1.1 Shift Cipher

Consider the ciphered text:

$$\boxed{\text{IQXOAYQFAODKBFASDMBTK}}$$

Find the key and decipher the message.

Disadvantage of Shift Cipher;

- There are only 25 possible keys and so it is not difficult to decipher the text created by Shift Cipher.
- We only need to do the subtraction by at most $n = 1, 2, 3, \cdots, 25$ modulo 26.

§2.1.1 Shift Cipher

Consider the ciphered text:

$$\boxed{\text{IQXOAYQFAODKBFASDMBTK}}$$

Find the key and decipher the message.

Disadvantage of Shift Cipher;

- There are only 25 possible keys and so it is not difficult to decipher the text created by Shift Cipher.
- We only need to do the subtraction by at most $n = 1, 2, 3, \cdots, 25$ modulo 26.
- In order to create more secured encryption, we need to learn more modular arithmetic.

§2.1.1 Shift Cipher

Before proceeding to other cryptosystems, let us revisit Shift Cipher to express it in a formal definition.

§2.1.1 Shift Cipher

Before proceeding to other cryptosystems, let us revisit Shift Cipher to express it in a formal definition.

Notation: $\mathbb{Z}_{26} = \{0, 1, 2, 3, \cdots, 25\}$.

§2.1.1 Shift Cipher

Before proceeding to other cryptosystems, let us revisit Shift Cipher to express it in a formal definition.

Notation: $\mathbb{Z}_{26} = \{0, 1, 2, 3, \cdots, 25\}$.

One can define the addition and subtraction modulo 26 as follows:

- $18 + 14 = 32 = 6$ (modulo 26)
- $5 - 12 = -7 = 19$ (modulo 26)

§2.1.1 Shift Cipher

Before proceeding to other cryptosystems, let us revisit Shift Cipher to express it in a formal definition.

Notation: $\mathbb{Z}_{26} = \{0, 1, 2, 3, \cdots, 25\}$.

One can define the addition and subtraction modulo 26 as follows:

- $18 + 14 = 32 = 6$ (modulo 26)
- $5 - 12 = -7 = 19$ (modulo 26)

Hereafter we will use mod as a shorthand version for modulo. Also, we will use lower case letters for plaintext, and upper case letters for ciphered text to avoid confusion.

§2.1.1 Shift Cipher

In the Shift Cipher, we have the following:

- The plain text is formed from the set $\mathcal{P}$ of 26 alphabets which can be identified with $\mathbb{Z}_{26}$

§2.1.1 Shift Cipher

In the Shift Cipher, we have the following:

- The plain text is formed from the set $\mathcal{P}$ of 26 alphabets which can be identified with $\mathbb{Z}_{26}$
- The ciphered text is also formed from the set $\mathcal{C}$ of 26 alphabets that can be identified with $\mathbb{Z}_{26}$

§2.1.1 Shift Cipher

In the Shift Cipher, we have the following:

- The plain text is formed from the set $\mathcal{P}$ of 26 alphabets which can be identified with $\mathbb{Z}_{26}$
- The ciphered text is also formed from the set $\mathcal{C}$ of 26 alphabets that can be identified with $\mathbb{Z}_{26}$
- The key is coming from the set $\mathcal{K}$ of integers modulo 26. The key does not represent a letter; rather it represents the amount of shift of each letter in the plain text in order to encipher.

§2.1.1 Shift Cipher

In the Shift Cipher, we have the following:

- The plain text is formed from the set $\mathcal{P}$ of 26 alphabets which can be identified with $\mathbb{Z}_{26}$
- The ciphered text is also formed from the set $\mathcal{C}$ of 26 alphabets that can be identified with $\mathbb{Z}_{26}$
- The key is coming from the set $\mathcal{K}$ of integers modulo 26. The key does not represent a letter; rather it represents the amount of shift of each letter in the plain text in order to encipher.
- For each key $k \in \mathcal{K}$, the enciphering follows the rule:
$$\{e_k(x) = (x + k) \bmod 26 \mid k \in \mathcal{K}\}$$

§2.1.1 Shift Cipher

In the Shift Cipher, we have the following:

- The plain text is formed from the set $\mathcal{P}$ of 26 alphabets which can be identified with $\mathbb{Z}_{26}$
- The ciphered text is also formed from the set $\mathcal{C}$ of 26 alphabets that can be identified with $\mathbb{Z}_{26}$
- The key is coming from the set $\mathcal{K}$ of integers modulo 26. The key does not represent a letter; rather it represents the amount of shift of each letter in the plain text in order to encipher.
- For each key $k \in \mathcal{K}$, the enciphering follows the rule:
$$\{e_k(x) = (x + k) \bmod 26 \mid k \in \mathcal{K}\}$$
- For each $k \in \mathcal{K}$, the deciphering follows the rule:
$$\{d_k(y) = (y - k) \bmod 26 \mid k \in \mathcal{K}\}$$

§2.1.1 Formal Definition of Cryptosystem

A cryptosystem (short for cryptographic system) consists of five parts:

- $\mathcal{P}$ is a finite set of possible plain texts.
- $\mathcal{C}$ is a finite set of possible cipher texts.
- $\mathcal{K}$, the key space, is a finite set of possible keys.
- $\mathcal{E}$ is the set of *encryption rules*. For every key k in $\mathcal{K}$, there is an encryption rule $e_k \in \mathcal{E}$ which is a function $e_k : \mathcal{P} \to \mathcal{C}$ that converts a plain text into a cipher text.
- $\mathcal{D}$ is the set of *decryption rules*. For every key k in $\mathcal{K}$, there is a corresponding decryption rule $d_k \in \mathcal{D}$ which is a function $d_k : \mathcal{C} \to \mathcal{P}$ that converts a cipher text into a plain text.
  Furthermore, for obvious reasons, we require that for every plaintext $x \in \mathcal{P}$ and for every key $k \in \mathcal{K}$, $d_k(e_k(x)) = x$.

§2.1.1 Formal Definition of Cryptosystem

Now we can formally define Shift Cipher as follows:

Shift Cipher is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For each $0 \leq k \leq 25$,

$$e_k(x) = (x + k) \bmod 26$$

$$d_k(y) = (y - k) \bmod 26$$

where $x, y \in \mathbb{Z}_{26}$.