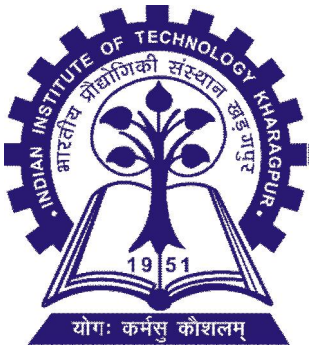
Cryptography and Network Security (CS60065)

AUTUMN, 2021-2022

TA: Tapadyoti Banerjee

Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India



TUTORIAL: 1
DATE: 25TH August 2021

QUESTION : 1 (The Shift Cipher)

Let P = C = K = $\mathbf{Z}_{26}$, where **Z** the set of integers. Consider the key for a Shift Cipher is K = 11, and the plaintext is "MEET". Find the corresponding ciphertext.

MEET - (13, 5, 5, 20) - 11 = (12, 4, 4, 19)

(23, 15, 15, 4)

⟶ XPPE

QUESTION : 2 (The Substitution Cipher)

Let P = C = K = $\mathbf{Z}_{26}$, where **Z** the set of integers. Consider the random permutation for encryption function as follows:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

And the ciphertext is “TVVM”. Find the corresponding plaintext.

The Affine Cipher

Let $P = C = K = \mathbf{Z}_{26}$, and let

$K = \{(a, b) \in \mathbf{Z}_{26} \times \mathbf{Z}_{26} : \gcd(a, 26) = 1\}$.

For $K = (a, b) \in K$, define

$$e_K(x) = (ax + b) \bmod 26$$

And $$d_K(y) = a^{-1}(y - b) \bmod 26$$

where $(x, y) \in \mathbf{Z}_{26}$

$a = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

affine func^n - $f(x_1, x_2 \cdots x_n) = A_1 x_1 + \cdots + A_n x_n$

a^{-1} → multiplicative inverse.

☆ remember modern algebra class.

$3^{-1} \equiv 9$ $\quad$ $7^{-1} \equiv 15$

QUESTION : 3 (The Affine Cipher)

Suppose that K = (7, 3), i.e., a = 7 and b = 3. Here all operations are performed in $\mathbf{Z}_{26}$, where $\mathbf{Z}$ the set of integers. verify that

$$d_K(e_K(x)) = x \text{ for all } x \in \mathbf{Z}_{26}.$$

$e_k(x) = 7x + 3 \pmod{26}$

$d_k(y) = 15(y - 3) \pmod{26}$

$d_k(e_k(x)) = 7 \times 15\, x \pmod{26}$

$= x \pmod{26} = x$

QUESTION : 4 (The Affine Cipher)

Suppose that K = (7, 3), i.e., a = 7 and b = 3. Here all operations are performed in $\mathbf{Z}_{26}$, where $\mathbf{Z}$ the set of integers. Now, encrypt the plaintext "MEET" by using the concept of Affine Cipher.

MEET = 12, 4, 4, 19

$e_k(m)$ = 87, 31, 31, 136

$e_k(m)$ = 9, 5, 5, 6

JFFG

QUESTION : 5 (The Vigenere Cipher)

Suppose that K = "POINT". Now, encrypt the plaintext "SOUTH EAST" by using the concept of ~~Affine~~ Cipher.

POINT - 15, 14, 8, 13, 19

SOUTH EAST -
+ 15 14 8 13 19 15 14 8 13

$|K| = 26^m$

QUESTION : 6 (The One-time Pad)

Suppose we encrypt the name “point” with a one-time pad (consider the length of the keyword is 5). To break the ciphertext by brute force attack, find the number of computations you need.

$(26)^5$

The Playfair Cipher

Suppose Key = ‘tutorials’, then 5 x 5 grid is as follows:

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

We want to encrypt the message “hide money”.
It will be written as − HI DE MO NE YZ
The encrypted Message is -- QC EF NU MF ZV

QUESTION : 7 (The Playfair Cipher)

Find the security value of the Playfair Cipher.

25 x 25 how ???

QUESTION : 8 (The Simple Transposition Cipher)

Suppose the secret random key is “five”, and the plaintext is “golden statue is in eleventh cave”. Determine the ciphertext.

QUESTION : 9 (The Permutation Cipher)

Suppose key = 6 and the key is the permutation for encryption is

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Determine the plaintext for the ciphertext:

EESLSHSALSESLSHBLEHSYEETHRAEOS