DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 19CS2109
COMPUTER NETWORKS AND SECURITY

CLASSIC ENCRYPTION TECHNIQUES#7

Date of the Session: ___/___/___ **Time of the Session:** _____to_____

Learning outcomes:

- To Understand Classical Encryption Techniques.
- To implement the concept of Substitution cipher Techniques
- To implement the concept of Transposition cipher Techniques.

1900320022

PART A:

Substitution ciphers:

IN-TUTORIAL:

1. Harry Potter and his friends, Ron and Hermione often exchanged secret magical spells and messages in an encrypted form using the Caesar cipher method.Help Draco to Encrypt and Decrypt messages using Caesar cipher method

   Encrypt the following secret messages

   a. Text: AVADA KEDAVRA
   Shift: +3

   Solution: DYDGD NHGDYUD

   b. Text: DOBBY IS A FREE ELF
   Shift: +12

   Solution: PANNK UE M RDGQ QXR

Decrypt the following messages

c. Text: OBLIVIATE
Shift: +7

Solution: HUEBOBTMX

d. Text: HOGWARTS IS MY HOME
Shift: +25

Solution: IPHXBSUT JT NZ IPNF

e. Text: EXPELLIARMUS
Shift: +5

Solution: ZSKZGGDVMHPN

f. **The following are the plain text and cipher texts. Shift is ____**

Plain text: espntaspcsldmppymczvpy
Cipher text: the cipher has been broken

Solution: The numerical vale of e is 5 & t is 19. So the shift is 19-5+1=15

5. The Marauder's map is a magical map of Hogwarts School of Witchcraft and Wizardry. The map is normally disguised as a blank piece of parchment. To view the map, one must tap it with one's wand and recite,
"I SOLEMNLY SWEAR THAT IM UP TO NO GOOD".
Harry Potter wants to encrypt this phrase so that no professor of Hogwarts could be able to reveal it.
So, using Playfair cipher with a key = "MAP", help Harry to encrypt the phrase

Solution:

key = "MAP"

initial entries are 'm', 'A', 'p'

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

Now, divide plain text into pair of letters

IS|OL|EM|NL|YS|WE|AR|TH|AT|IM|UP|TO|NO|GO|OD

IS → LQ (Draw Rectangle)
OL → IN (same row, so take right character to that character)
EM → DA (Draw Rectangle)
NL → ON (same row)
YS → XT
WE → AK (same column)
AR → EW
TH → UG
AT → BR
IM → QD
UP → SC
TO → UN
NO → OI
GO → HN
OD → IH

CIPHER TEXT = LQINDAONXTAKEWUGBRQDSC
UNOIHNIH

5. The Marauder's map is a magical map of Hogwarts School of Witchcraft and Wizardry. The map is normally disguised as a blank piece of parchment. To view the map, one must tap it with one's wand and recite,
"I SOLEMNLY SWEAR THAT IM UP TO NO GOOD".
Harry Potter wants to encrypt this phrase so that no professor of Hogwarts could be able to reveal it.
So, using Playfair cipher with a key = "MAP", help Harry to encrypt the phrase

Solution:

Key = "MAP"

initial entries are 'm', 'A', 'P'

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

Now, divide plain text into pair of letters

IS | OL | EM | NL | YS | WE | AR | TH | AT | IM | UP | TO | NO | GO | OD

IS → LQ (Draw Rectangle)
OL → IN (same row, so take right character to that character)
EM → DA (Draw Rectangle)
NL → ON (same row)
YS → XT
WE → AK (same column)
AR → EW
TH → UG
AT → BR
IM → QD
UP → SC
TO → UN
NO → OI
GO → HN
OD → IH

CIPHER TEXT = LQINDAONXTAKEWUGBRQDSC
UNOIHNIH

6. a) How do we construct a matrix in Playfair cipher? Construct the Playfair square(matrix) for "FINGERPRINT" as a key using PLAYFAIR cipher algorithm.
b) Encrypt the plain text message "BIOMETRICS" using Play fair Cipher method, by using the above key. Show step by step process of encrypted text message.

Solution:

a) In playfair cipher we use 5X5 matrix.

The matrix is

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

b) Key = FINGERPRINT. TEXT = BIOMETRICS

Divide plain text into pair of letters

BI | OM | ET | RI | CS

BI = PE

OM = QO

ET = NB

RI = PF

CS = KM

The encrypted text is PEQONBPFKM

POST-TUTORIAL:

1. Julius Caesar and Cleopatra often exchanged messages in an encrypted form using the Caesar cipher method. Write a python code for encryption and decryption of a message using Caesar cipher.

Sample Input:

Original Message – SECRET

Shift Value – 9

Sample Output:

Encrypted Message- BNLANC

Solution:

```
def encrypt (text,s):
    ans = ""
    for i in range(len(text)):
        x = text[i]
        if (x.isupper()):
            ans += chr( (ord(x)+s-65)%26 +65)
        else:
            ans += chr ((ord(x)+s-97)%26+97))
    return ans
def decrypt (text,s):
    s=26-s
    return encrypt(text,s)

text = "SECRET"
s = 9
print("Encrypted message: " + encrypt(text,s))
print ("Decrypted message: " + decrypt(text,s))
```

2. a. While constructing key matrix in Playfair, what to do if letters in plain text reoccur?
   b. Construct the matrix for "AVENGERSMARVEL" as a keyword by using PLAYFAIR cipher and
   c. Encrypt the plain text message "AVENGERS ASSEMBLE".
   d. Decrypt the cipher text message "VGFCERCBQVREEY"

Solution:

a. If a letter reoccurs while constructing a key matrix, then we should avoid that multiple occurrence. Matrix should only have unique values.

b. KEY = "AVENGERSMARVEL"

Key

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

c) Divide plain text as pair of characters

AV | EN | GE | RS | AS | SE | MB | LE

AV = VE
EN = NG
GE = AN
RS = SM
AS = VR
SE = MV
MB = LR
LE = MN

Encrypted message: VENGANSMVRMVLRMN

d) Divide plain text

VG | FC | ER | CB | QV | RE | EY

VG = AN
FC = DI
ER = AM
CB = IR
QV = ON
RE = MA
EY = NX

Decrypted message: ANDIAMIRONMANX

Dyer

becomes equal to original message length. For encryption take first letter of message and new key i.e. T and G. Take the alphabet in the table where T row and G column coincides i.e. Z. Do this for all the letters. You will now get the encrypted clue and you inscribe it on the walls of your ship (including the key) so that your followers can find it easily.

i. Perform encryption.

ii. Help the alien cryptanalyst decrypt the clue using the same key.

(i) Plain text = THEEASTWALL

Key = GUARD

T H E E A S T W A L L

New key = G U A R D G U A R D G

Encrypted text = Z B E V O Y N W R O R

(ii) Decryption:-

Cipher text = Z B E V O Y N W R O R

key = G U A R D G U A R D G

Check in table, when row 'G' was taken, where would we get value 'Z'. for first char it will be 'T'.

Plain text = T H E E A S T W A L L

PART B

Transposition ciphers:

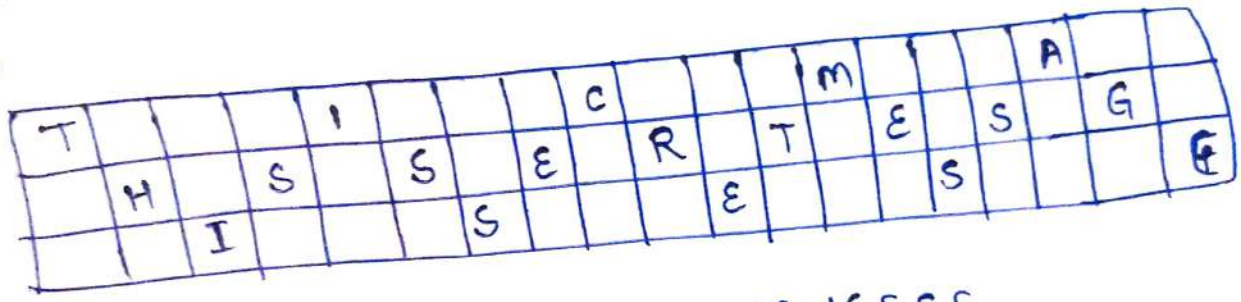
IN-TUTORIAL:

1. Given below is the plain text. Find the cipher text using Rail Fence technique.

Plain Text: THIS IS SECRET MESSAGE
a) If key=3
b) If key=4
NOTE: Neglect spaces when encrypting.

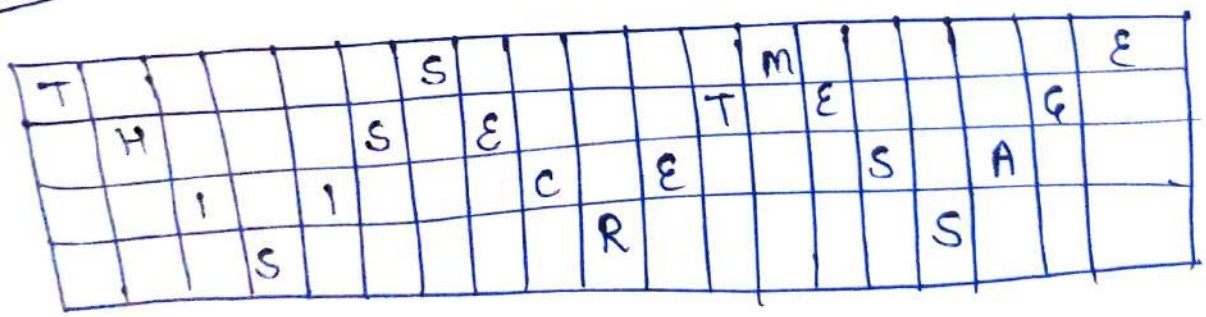
Solution:

Key=3



Cipher text = T I C M A H S S E R T E S G I S E S E

Key=4



Cipher text = T S M E H S E T E G I I C E S A S R S

2. A cipher with three rails is used to encrypt the following message. Find the plain text using Rail Fence technique.
Ciphertext: 1 5 9 13 2 4 6 8 10 12 14 3 7 11 15

Solution:

Key = 3

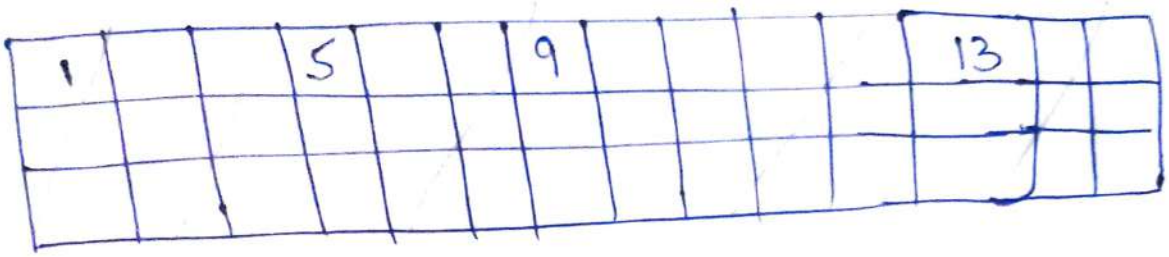
Ciphertext: 1 5 9 13 2 4 6 8 10 12 14 3 7 11 15

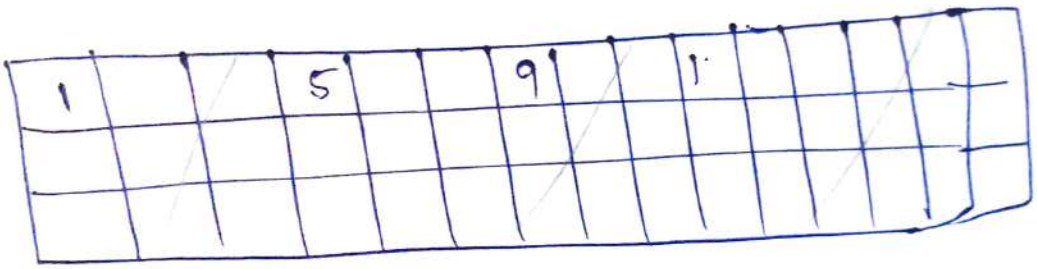
2. A cipher with three rails is used to encrypt the following message. Find the plain text using Rail Fence technique.
Ciphertext: 1 5 9 13 2 4 6 8 10 12 14 3 7 11 15

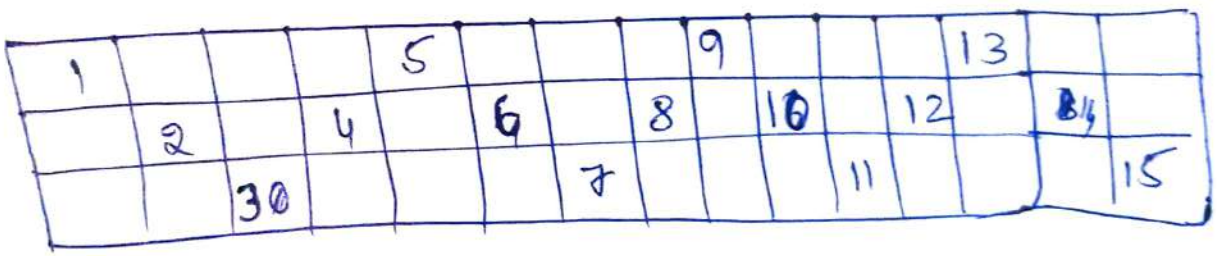
Solution:

Key = 3

Ciphertext: 1 5 9 13 2 4 6 8 10 12 14 3 7 11 15







plain text = 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

3. Two friends Chandler Bing and Rachel Green wants to communicate anonymously. Help them in Encrypting the Plain text into cipher text. (using Columnar Encryption Technique).
Plain text: "DO NOT GOOGLE IT"
Key: "FAKE"

Solution:

TEXT = "DO NOT GOOGLE IT"

KEY = "FAKE"

So length of rows = 4

The permutation will be = 3 1 4 2 (Alphabetical order of letters in key)

F	A	K	E
3	1	4	2
D	O	—	N
O	T	—	G
O	O	G	L
E	—	I	T

~~Encrypted text = DOOE OTO - - - GINGLT~~

Encrypted text = OTO_NGLTDOOE__GI

POST-TUTORIAL:

1. A. Write the algorithm for rail fence.
   B. Encrypt NOTHING IS AS IT SEEMS by taking depth=2. (Rail Fence Technique).

Solution:

A. Algorithm for rail fence (Encryption):-

*) In the rail fence cipher, the plain text is written downwards and diagonally on successive rails of an imaginary fence.

*) When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in zig-zag manner.

*) After each alphabet has been written, the individual rows are combined to obtain the cipher text.

B.

NOTHING IS AS IT SEEMS

N T I G , S A S , T S E E M S
O H N I A I S E S

Cipher text = NTIGSSTEMOHNIAISES

2. a. An encrypted message has been sent to Monica Geller from Joey. Help Monica to decrypt the cipher text to plain text. (using Columnar Decryption technique).
Cipher text: LTEYBEOUIERRLHFO
Key: FAKE

b. Implement a python code for Columnar Transposition technique.

Solution:

@ key = FAKE

cipher text = LTEYBEOUIERRLHFO

3	1	4	2
F	A	K	E
L	T	E	Y
B	E	O	U
I	E	R	R
L	H	F	O

Plaintext = TEEHYUROLBILEORF

Program for Columnar Transposition Cipher

```python
# Program for Columnar Transposition Cipher
import math
key = "FAKE"

# Encryption
def encryptMessage(msg):
    cipher = ""
    k_indx = 0
    msg_len = float(len(msg))
    msg_lst = list(msg)
    key_lst = sorted(list(key))

    col = len(key)

    row = int(math.ceil(msg_len / col))

    fill_null = int((row * col) - msg_len)
    msg_lst.extend('_' * fill_null)

    matrix = [msg_lst[i: i + col]
              for i in range(0, len(msg_lst), col)]

    for _ in range(col):
        curr_idx = key.index(key_lst[k_indx])
        cipher += ''.join([row[curr_idx]
                           for row in matrix])
        k_indx += 1

    return cipher

# Decryption
def decryptMessage(cipher):
    msg = ""

    k_indx = 0
    msg_indx = 0
    msg_len = float(len(cipher))
    msg_lst = list(cipher)

    col = len(key)
    row = int(math.ceil(msg_len / col))
    key_lst = sorted(list(key))

    dec_cipher = []
    for _ in range(row):
        dec_cipher += [[None] * col]
    for _ in range(col):
        curr_idx = key.index(key_lst[k_indx])

        for j in range(row):
            dec_cipher[j][curr_idx] = msg_lst[msg_indx]
            msg_indx += 1
        k_indx += 1
    try:
        msg = ''.join(sum(dec_cipher, []))
    except TypeError:
        raise TypeError("exception")

    null_count = msg.count('_')

    if null_count > 0:
        return msg[: -null_count]

    return msg

# Driver Code
msg = "ABCDEFGHI"

cipher = encryptMessage(msg)
print("Encrypted Message: {}".format(cipher))

print("Decryped Message: {}".format(decryptMessage(cipher)))

```

Result

CPU Time: 0.06 sec(s), Memory: 8384 kilobyte(s)

```
Encrypted Message: BF_DH_AEICG_
Decryped Message: ABCDEFGHI
```

3.
a. Write the algorithm for Columnar Encryption Technique.
b. Encrypt "NOTHING IN THE WORLD IS MORE DANGEROUS THAN SINCERE IGNORANCE AND CONSCIENTIOUS STUPIDITY" with key k= "PLANE" using Rail fence with key=2

Solution:

a) Algorithm:-

1) The message is written out in rows of a fixed length, and then read out again column by column & the columns are chosen in some scrambled order.
2) Width of the rows & the permutations of the columns are usually defined by a keyword.
3) Any spare spaces are filled with nulls or left blank or placed by a character
4) Finally, the message is read off in columns, in the order specified by the keyword.

b) N O T H I N G , I N T H E W O R L D I S M O R E D A N G E R O U S T H A

N S , I N C E R E I G N O R A N C E A N D C O N S C I E N T I O U S S T U P I D I T Y

Cipher text = N T I G N H W R D S O E A G R U T A S N E E G O A C A

D O S I N I U S U I I Y O H N I T E O L I M R D N E O S H N I C R I N R N

E N C N C E T O S T P D T

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured: _____ out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation: