Assignment No:- 1

Aim: Perform encryption and decryption using caser cipher algorithm.

Theory: The casar cipher is the simplest and oldest method of cryptography. The caser cipher method is used ~~t~~and it is based on mon-alphabetic cipher and called a shift cipher of additive cipher. cipher used the shift cipher to communicate with his offices for this reason this technique is called as the caser cipher

caser cipher is a weak method of cryptography, can be hacked easily, i.e. message decryption takes place easily.

Rules for caser cipher:

1. choose number between 1 & 25 i.e. shift value.
2. Write letters in alphabetical order, i.e., A-Z
3. shift each letter by shift value i.e., A = D (value = 3)
4. Encrypt your message by replacing letter's with shift letter.
5. To decrypt, simply reverse the process.

Algorithm for caser cipher:

1. Choose shift value from 1 & 25.
2. Write down alphabet in order from A to Z.

3. create a new alphabet by shifting each letter of original alphabet by shift value i.e. value = 3

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

4. Replace each letter of message with new alphabet i.e. "hello" = "khoor"

5. To decrypt message, reverse the process i.e. "khoor" = "hello".

X	Y	Z	A	B	C	D	E	F
A	B	C	D	E	F	G	H	I

Advantages:

1. Easy to implement and use.

2. can be physically implemented, such as with a set of rotating disks, known as scytale, which can be used in certain situation.

3. Require only small set of pre-shared information

4. can be modified easily to create more secure variant by multiple shift values or keywords.

Disadvantages:

1. Not secure against modern decryption methods.

3. The smaller number of keys means easily attackers can try to decrypt the message.
4. Not suitable for long text encryption
5. Not suitable for secure communication.

Conclusion:

Hence, we have performed encryption and decryption using casear cipher algorithm.

Assignment No :- 2

Aim: To perform encryption and decryption using play fair cipher.

Theory:

Playfair cipher is proposed by charles whetstone in 1889. But was named for one of his friends Lord Lyon playfair because he popularized its use. It is the most popular symmetric encryption technique that falls under the substitution cipher.

It is an encryption algorithm to encode a message, same as traditional cipher, only diffrence is it encrypts a diagraph instead of single letter. Initially creates a key-table of 5x5 matrix, contains alphabets which act as the key for encryption of plaintext.

Advantages :-

- Diverse ciphertext if we scrutinize the algorithm, we can notice at every stage we are getting diverse ciphertext, thus more trouble to cryptanalyst.
- Brute force attack does not affect it.
- Cryptanalyze is not possible.
- Overcomes the limitation of simple playfair square cipher.
- Easy to perform.

Limitations:

- only 25 alphabets are supported.
- Does not support numeric characters.
- only either uppercases or lower cases are are supported
- The use of special character is prohibited
- It does not support other languages, except English
- Encryption of media file is also not supported.

Rules :-

1. split plaintext in diagraphs. If plaintext has the odd numbers of letters, append the letter Z at the end of plaintext.

   i.e. MANGO → MANGOZ

2. so, after that break plaintext into diagraph If any two same letters come side by side put x at the place of second occurance

   i.e. COMMUNICATE → COMXMUNICATE
   JAZZ → JAZXZX
   GREET → GREXET

3. To determine the cipher text, first build a 5x5 key-matrix or key-table & filled it with letters of alphabets as:

   - Fill first row with letters of keyword If keyword have duplicate letters avoid them. After that fill remaining letters in alphabetic order.

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

→ Keyword "Athens" & others are alphabetics order letters without repeated.

4. There may be the following there conditions
(i) If a diagraph appears in the same row, then replace each letter of diagraph with letters immediately to their right & if not present replace it like, i.e.

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

(ii) If a diagraph appears in the same column, replace each letter immediately below them & if no letter below then replace top of same column like

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

Top of W is V

(iii) If a diagraph appears in different row & column, then select a 3*3 matrix from 5*5, such pair of 3x3 letters occupy two opposite corner of square within the matrix, where other cormer will be a cipher for the given diagraph i.e.

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

→3x 3 matrix

Conclusion :-

we have performed encryption & decryption using playfair cipher.

Assignment No: 3

Aim: perform encryption and decryption using Rail fence Technique (Row transposition technique)

Theory: The Rail fence Technique is a simple transposition cipher that encrypts a message by rearranging the order of the letters in a zigzag pattern. It is one of the oldest & simplest encryption techniques known, and is relatively easy to break, but it can still be useful for simple communicate where a high level of security is not required.

To encrypt a message using the Rail fen technique, you will need to choose a number of rails the most common is two rails, but you can use more or less depending on the derived leve of security.

Encryption algorithm:

1. Key setup:

ⓐ Determine number of rails to use for zig-zag pattern

ⓑ Create the rails by setting up as many empty lines as specified by the key

2. Text preparation:

ⓐ Remove any spaces and punctuation from the plaintext. you may also choose to convert the text to uppercase to simplify the process.

3. Encryption :-

ⓐ Start at top rail & write the first letter of the plaintext

ⓑ Move down to the next rail & write the first letter of the plaintext

ⓒ Continue moving down in a zigzag pattern, placing each letter of the ~~ap~~plaintext on the appropriate rail.

ⓓ when you reach the bottom rail, reverse direction & start moving upward.

ⓔ Repeat this process until you have placed all the letters of the plaintext on the rails.

4. Ciphertext formation :

ⓐ Read the letters from the rails in order, starting from the top rail to the bottom rail

ⓑ This forms the ciphertext.

Decryption Algorithm :

1. key setup :

ⓐ determine the number of rails or liner used for encryption.

2. Text preparation :

ⓐ Remove any spaces & punctuation from the ciphertext you may also choose to convert text to uppercase to simplify the process.

3. Decryption :

ⓐ create same no. of empty rail fence as of encryption process

ⓑ Filling the Rails.

ⓔ continue in the zigzag pattern, placing each ~~letter~~ letter of the ciphertext on appropriate rail

ⓕ when reach the bottom rail, reverse direction and start moving upward.

ⓖ Repeat the process until you place all letters of ciphertext on the rail.

4. Recovery of plaintext:

ⓐ Read the letters from the rails in the same zigzag pattern used during encryption.

ⓑ This forms the plaintext.

Plaintext T H I S I S A S E C R E T M E S S A G E

Rail	T				I				G				T		·	S	
fence		H		S		S		S		C		E		M	S	S		A E
Encoding key=3			I				A				R			~~E~~	E			G

ciphertext T I E T S H S S S C E M S A E I A R E G

Conclusion:

Hence, we have learned / performed encryption & decryption using Rail Fence technique.

Assignment No : 4

Aim : perform encryption and decryption using columnar transformation technique.

Theory : columnar transposition technique are a type of cipher that encrypts a message by rearranging the order of the letters in columns . the columns are then read in a diffrent order to produce the ciphertext

The technique can be used with any number of columns, but the more columns you use, the more difficult the cipher will be to break. However, even with a large number of columns, columnar transposition techniques are still relatively weak cipher and can be broken by a skilled cryptanalyst.

Additional Techniques :-

- Use a random number generator to generate the keyword
- use a keyword that is not related to the plaintext message
- Use a keyword with repeated letters
- Use a Combination of columnar transpostion and other technique. despite their weaknesses, columnar transposition techniques are still useful for simple communication when a high level of security is not required.

Encryption :

① The message is written out in rows of fixed length & then read out again by column & the columns are chosen in some scrambled order.

② width of the rows and the permutation of the columns are usually defined by a keyword.

③ Any spaces are filled with null or left black

④ Finally, the message is read-off- in columns in order specified

Decryption :

① To decipher it, work out the column lengths by dividing the message length by the key length

② ~~Then~~, write the message out in column again, then re-order the columns by reforming the keywords.

~~Color~~ Conclusion:-

Hence, we have performed encryption and decryption using columnar ~~t~~ransposition techniques.

Assignment No:- 5

Aim: Perform encryption & decryption using one time pad algorithm.

Theory:

One time pad algorithm (OTP) is a symmetric key where this algorithm uses a stream cipher derived from the XOR result between the plaintext bit and the key bit.

It is the only available algorithm, that unbreakable. It is one of the substitution technique which converts plaintext into ciphertext.

The two requirements for OTP are:-

- Key should be randomly generated & be long as the size of the message.
- Key is to be used to encrypt & decrypt a single message and then it is discarded.

So, encrypting every new message requires a new key of the same length as new message in OTP. The ciphertext generated by OTP is random, & so it does not have any statistical relation with plaintext.

i.e.	A	B	C	D	E	F	G	H	I	J	K
	0	1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Example:-

I/p :- message = HELLO
key = MONEY

O/P : Cipher = TSYPM

Explanation : ① plaintext to ciphertext

PT = HELLO → 7 4 11 14,
key = MONEY → 12 14 13 4 24

PT + key = 19 18 24 15 38 → 19 18 24 15 12   ∵ 38-26
ciphertex → TYPM

② Ciphertext to Message

CT = 19 18 24 15 12 → TSYPM,
key = MONEY → 12, 14, 13, 4, 24
CT - Key = 7 4 11 11 -12 → 7' 4 11 11 14
∵ -12+26=14

Plain text → 7 4 11 11 14 → HELLO

Advantages:

- OTP is only algorithm that is truly unbreakable and can be used for low bandwidth, channels requiring very high security.

Disadvantages :-

- There is the practical problem of making large quantities of random keys, Any heavily used system might require million of random characters on a regular basis.

conclusion:

Hence, we have performed encryption and decryption using one-time pad algorithm.

Assignment No:- 6

Aim :- write a program to implement extended euclidean algorithm.

Theory :- The basic euclidean algorithm is a way to find the greatest common divisor of two positive integer GCD of two numbers is the largest number that divides both of them A simple way to find GCD is the factorize both numbers and multiply common prime factors.

36 = 2×2×3×3
60 = 2×2×3×5

Multiplication of common factor : GCD = 2×2×3
= 12

Basic Euclidean algorithm for GCD :-

The algorithm is based on the below facts!

If we substract a smaller number from larger on . GCD doesn't change. so, if we keep substracting repeatedly the larger of two, we end up with GCD

Now, Instead of substraction, If we divide the smaller number, the algorithm stops when we find the remainder 0.

Example :-

Input : a=30 , b=20

Output: GCD = 10 , $x = 1$, $y = -1$
(Note that $30 * 1 + 20 * (-1) = 10$)

Input : $a = 35$, $b = 15$
Output : GCD = 5 , $x = 1$, $y = -2$
(Note that $35 * 1 + 15 \times (-2) = 5$)

How is Extended algorithm useful?

The extended euclidean algorithm is particularly useful when a & b are coprime since x is the modular multiplicative inverse of "a modulo b", and y is the modular multiplicative inverse of "b modulo a". In particular, the computation of the modular multiplicative inverse in an essential step in RSA public-key encryption key.

Conclusion :

Hence, we have performed a program to implement extended euclidean algorithm.