Assignment-02.

• Title :- Write a program that contains a string (char pointer) with a value 'Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

• Description :-

ⓐ String :-

- The string is one-dimensional array of characters terminated by the null ('\0')
- Each and every character in the array consumes one byte of memory, and the last character must always be 0
- The termination character ('\0') is used to identify where string ends.
- In C language string declaration can be done in two ways,
  - By char array
  - By string literal.
- Let, see example of declaring string by char array in C language.

char ch [10] = { 'o', 'p', 'a', 'r', 'n', 'a', 'x', 'y', 'c', 'o' }

- As we know, array index starts from 0, So, it will be,

0	1	2	3	4	5	6	7	8	9	10
'a'	'p'	'a'	'r'	'n'	'a'	'l'	'y'	'c'	'o'	\0

- Size is not mandatory.
- By string literal,
  Ex.,

  Char str[]= 'aparnalyco'

- '\0' will be appended at end of string of Compiler.

ⓑ ~~AND~~ XOR operation :-

- There are two inputs and one output in binary XOR operation.
- It is similior to ADD operation which takes two inputs and produces one result i.e one output.
- The input and result to binary XOR operation can only be 0 or 1.
- Binary XOR operations will always produce a 1 output if either of its inputs.

- XOR Truth table:

Input		Output
X	Y	
0	0	0
0	1	1
1	0	1
1	1	0

Ⓒ AND operation:

- There are two inputs and one outputs
- Inputs and result to binary AND operation can only be 0 and 1. The binary AND operation will always produce a 1 output if both inputs are 1 and will produce a 0 output if both inputs are 0
- For two different inputs, the output will be 0.
- Truth Table:

Input		Output
X	Y	
0	0	0
0	1	0

1	0	0
1	1	1

ⓓ XOR string with 127:

- A bit wise XOR with 127 will invert the 7 low bits of every character resulting in other characters which may be printable or not.
- That means when you print characters you will see "garbage".

- Conclusion :-

We had studied the AND and XOR of string with 127, and display output Success fully.

.Assignment-03.

- Title :-
  Design and implement a symmetric encryption algorithm based on Feistel structure.

- Description :-
  - Feistel cipher model is structure or design used to develop many block cipher such as DES.
  - Feistel cipher may have invertible, non-invertible and self invertible components in its design.
  - Same encryption as well as decryption algorithm is used.
  - A separate key is used for each round.
  - However same round key are used for encryption as well as decryption.

- Feistel cipher algorithm :-

  - Create a list of all the plain Text characters.

  - Convert plain text string into two halves:
    - left half (L1)
    - Right half (R1)

- Generate a random binary keys (K1 & K2) of length equal to the half length of Plain text for two rounds:-

① First round of Encryption:

- a. Generate function f1 using R1 and K1 as follows:

  f1 = XOR(R1, K1)

- b. Now the new left half (L2) and right half (R2) after round 1 are as follows:

  R2 = Xor (f1, L1)
  L2 = R1

② Second Round of Encryption:

- a. Generate function f2 using R2 and K2 as follows:

  f2 = XOR (R2, K2)

- b. Now the new left half (L3) and right half (R3) after round 2 are as follows

$R3 = Xor(f2, L2)$

$L3 = R2.$

- Concatenation of R3 to R3 is cipher Text

- Same algorithm is used for decryption to retriere the plain text from cipler Text.

- Conclusion :-

We had studied about feistel Cipher structure, working and application.

. Assignment - 04.

- Title :-

Implement DES and RSA algorithm.

- Description :-
- RSA algorithm in Cryptography :-

- It is an asymmetric cryptography algorithm.
- Asymmetric actually means that it works on two different keys i.e
    - Public keys
    - Private keys
- By the names, public key is given to everyone and private key is kept private.

- Example of asymmetric cryptography :-

① A client sends its public key to the server and requests some data.

② The server encrypts the data using client's public key and sends the encrypted data.

③ The client receives this data and decrypts it.

- Data encryption standard (DES):

- DES has been found vulnerable to very powerful attacks.
- DES is a block cipher and encrypt data in blocks of size of 64 bits each, which means 64 bits of plain text go as input to DES, which produces 64 bits of cipher text.
- Same algorithm and key are used for encryption and decryption with minor differences.
- The key length is 56 bits.
- Step:
  - Key transformation
  - Expansion permistation
  - S-box permutation
  - P-box permutaction
  - XOR and swap.

- Generating Public key :-

- select two prime no's Suppose P= 53 and Q : Now first part of public key: n= P*Q : we also need a small
- exponent say e : But e must be
- An Integer
- Not be a factor of n.
- $1 < e < \emptyset(n)$

- Generating Private key:-

- we need to Calculate $\phi(n)$:
- Such that $\phi(n) = (p-1)(q-1)$
  So, $\phi(n) = 3016$
- Now calculate private key, d:
  $d = (k * \phi(n) + 1) / e$ for some integer k
  for $k=2$, value of d is 2011

Now we are ready with our - public key ($n=$ 3127 and $e=3$) and private key ($d=2011$)
Now we will encrypt "Hi".

- Convert letters to numbers:
  $H=8$ and $I=9$
  Thus Encrypted Data $C = 89^e \bmod n$.
  Thus our Encrypted Data comes out to be 1394.

- Now, we will decrypt 1394:
  Decrypted Data $= c^d \bmod n$.
  Thus, our Encrypted Data comes out to be 89.

  $8=H$ and $I=9$ i.e "HI"

. Assignment -05 .

- Title :-

Demonstrate how diffie-Hellman exchange works with Man- In- Middle attack.

- Description :-

- Diffie- Hellman key exchange algorithm is an advanced cryptographic method used to establish a shared secret that can be perform secret Communication on public network betn Alice and Bob while preventing Eve.
- who can eavesdrop on all their communication, from learning generated secet.

- The key exchange procedure has two steps:-

1. One- time setup:
We define some public parameters that are used by everyone forever.

2. Protocol:
To generate new secret key, run a two-message key exchange protocol. This process is done using some simple algebra, prop. of

modular arithmetic.

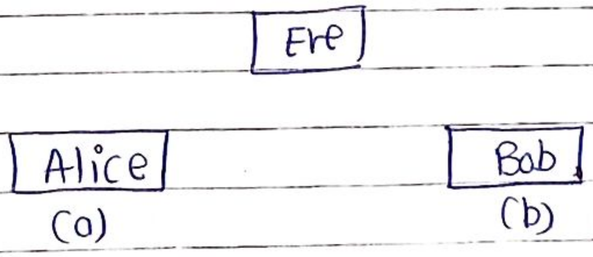
- Man-in-the-middle against Diffie-Hellman:-

– A malicious Malory, that has a MitM position, Can manipulate Communications betn Alice and Bobs and break security of key exchange.

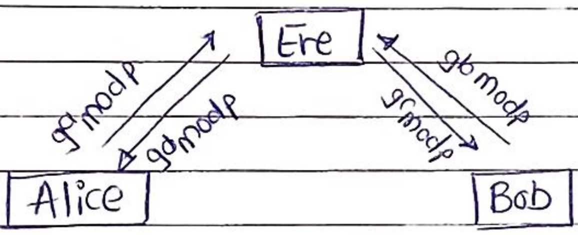
- Step by step explanation of this process:-

- Step 1:
  - selected public numbers p & g,
    p: prime number (Modulus)
    g: base.

- Step 2:
  - selecting private numbers.
  - Let Alice : a
    Bob : b
  - Malory picks 2 random numbers c and d.



- Step 3:
  - Intercepting public value
  - Alice's : g^a modp
    Bob's : g^c modp.
  - Malory intercepts
    Bob's = g^b modp
    Alice = g^d modp.



- Step 4:
- Computing secret key
  - Alice's key, $S_1 = g^{da}$ modp
    Bob's key, $S_2 = g^{cb}$ modp

- Step 5:
  - if Alice uses S_1 as key to encrypt later mssage to Bob, Malory can decrypt it, re-encrypt it using S_2 & send it to Bob.

- Alice and Bob won't notice any problem and may in reality, Mabry can decrypt, read, modify and then re-encrypt all conversation.

- Conclusion:

  We had studied the man-in-middle attack in Diffie Hellman using the problem.