**Cryptography and System Security Lab**

**Exp1: Write a C program that contains a string (charpointer) witha value\Hello World’.The program should XOR each character in this string with 0 and display the result.**

#include<stdlib.h>

#include<stdio.h>

main()

{

char str[]="Hello World";

char str1[11];

int i,len;

len=strlen(str);

for(i=0;i<len;i++)

{

str1[i]=str[i]^0;

printf("%c",str1[i]);

}

printf("\n");

}

**Input:**

**Output:**

**Exp2:** **Write a C program that contains a string (char pointer) with a value \Hello World’. The program should AND and XOR each character in this string with 127 and 255 respectively display the result.**

#include<stdio.h>

#include<stdlib.h>

#include<string.h>

void main()

{

char str[]="Hello World";

char str1[11];

char str2[11];

int i,len;

len = strlen(str);

for(i=0;i<len;i++)

{

str1[i] = str[i]&127;

printf("%c",str1[i]);

}

printf("\n");

for(i=0;i<len;i++)

{

str2[i]=str[i]^255;

printf("%c",str2[i]);

}

printf("\n");

}

**Input :**

**Ouput:**

**Exp 3: Write a program in C to implement Caeser Cipher**

#include<stdio.h>

#include<ctype.h>

int main() {

char text[500], ch;

int key;

// Taking user input.

printf("Enter a message to encrypt: ");

scanf("%s", text);

printf("Enter the key: ");

scanf("%d", & key);

// Visiting character by character.

for (int i = 0; text[i] != '\0'; ++i) {

ch = text[i];

// Check for valid characters.

if (isalnum(ch)) {

//Lowercase characters.

if (islower(ch)) {

ch = (ch - 'a' + key) % 26 + 'a';

}

// Uppercase characters.

if (isupper(ch)) {

ch = (ch - 'A' + key) % 26 + 'A';

}

// Numbers.

if (isdigit(ch)) {

ch = (ch - '0' + key) % 10 + '0';

}

}

// Invalid character.

else {

printf("Invalid Message");

}

// Adding encoded answer.

text[i] = ch;

}

printf("Encrypted message: %s", text);

return 0;

}

**Exp 4: Write a program in C to implement Monoalphabetic substitution cipher**

#include<stdio.h>

char monocipher\_encr(char);

char alpha[27][3] = { { 'a', 'f' }, { 'b', 'a' }, { 'c', 'g' }, { 'd', 'u' }, {

'e', 'n' }, { 'f', 'i' }, { 'g', 'j' }, { 'h', 'k' }, { 'i', 'l' }, {

'j', 'm' }, { 'k', 'o' }, { 'l', 'p' }, { 'm', 'q' }, { 'n', 'r' }, {

'o', 's' }, { 'p', 't' }, { 'q', 'v' }, { 'r', 'w' }, { 's', 'x' }, {

't', 'y' }, { 'u', 'z' }, { 'v', 'b' }, { 'w', 'c' }, { 'x', 'd' }, {

'y', 'e' }, { 'z', 'h' } };

char str[20];

int main() {

char str[20], str2[20];

int i;

printf("\n Enter String..");

gets(str);

for (i = 0; str[i]; i++) {

str2[i] = monocipher\_encr(str[i]);

}

str2[i] = '\0';

printf("\n Before Decryption..%s", str);

printf("\n After Decryption..%s\n", str2);

}

char monocipher\_encr(char a) {

int i;

for (i = 0; i < 27; i++) {

if (a == alpha[i][0])

break;

}

return alpha[i][1];

}

**Exp 5: Write a program in C to implement Vigenere (Polyalphabetic ) Cipher**

#include<stdio.h>

#include<string.h>

int main(){

char msg[] = "THECRAZYPROGRAMMER";

char key[] = "HELLO";

int msgLen = strlen(msg), keyLen = strlen(key), i, j;

char newKey[msgLen], encryptedMsg[msgLen], decryptedMsg[msgLen];

printf("Length of message:%ld\n",strlen(msg));

printf("Length of key:%ld\n",strlen(key));

//generating new key

for(i = 0, j = 0; i < msgLen; ++i, ++j){

if(j == keyLen)

j = 0;

newKey[i] = key[j];

}

newKey[i] = '\0';

//encryption

for(i = 0; i < msgLen; ++i)

encryptedMsg[i] = ((msg[i] + newKey[i]) % 26) + 'A';

encryptedMsg[i] = '\0';

//decryption

for(i = 0; i < msgLen; ++i)

decryptedMsg[i] = (((encryptedMsg[i] - newKey[i]) + 26) % 26) + 'A';

decryptedMsg[i] = '\0';

printf("Original Message: %s", msg);

printf("\nKey: %s", key);

printf("\nNew Generated Key: %s", newKey);

printf("\nEncrypted Message: %s", encryptedMsg);

printf("\nDecrypted Message: %s", decryptedMsg);

return 0;

}

**Exp 6: Study of Packet Sniffer Tools: Wireshark**

1. **Download and install wireshark and capture icmp, tcp and http packets in promiscuous mode.**
2. **Explore how the packets can be traced based on different filters.**

[**https://www.varonis.com/blog/how-to-use-wireshark**](https://www.varonis.com/blog/how-to-use-wireshark)

**Exp 7: Study the Use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registers**