INTRODUCTION TO CRYPTOGRAPHY – LAB 1

B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of performance: 22/12/2021

Aim: To implement shift ciphers and to study various terms related to cryptography.

Code:

Language: C

Compiler: clang/ZSH

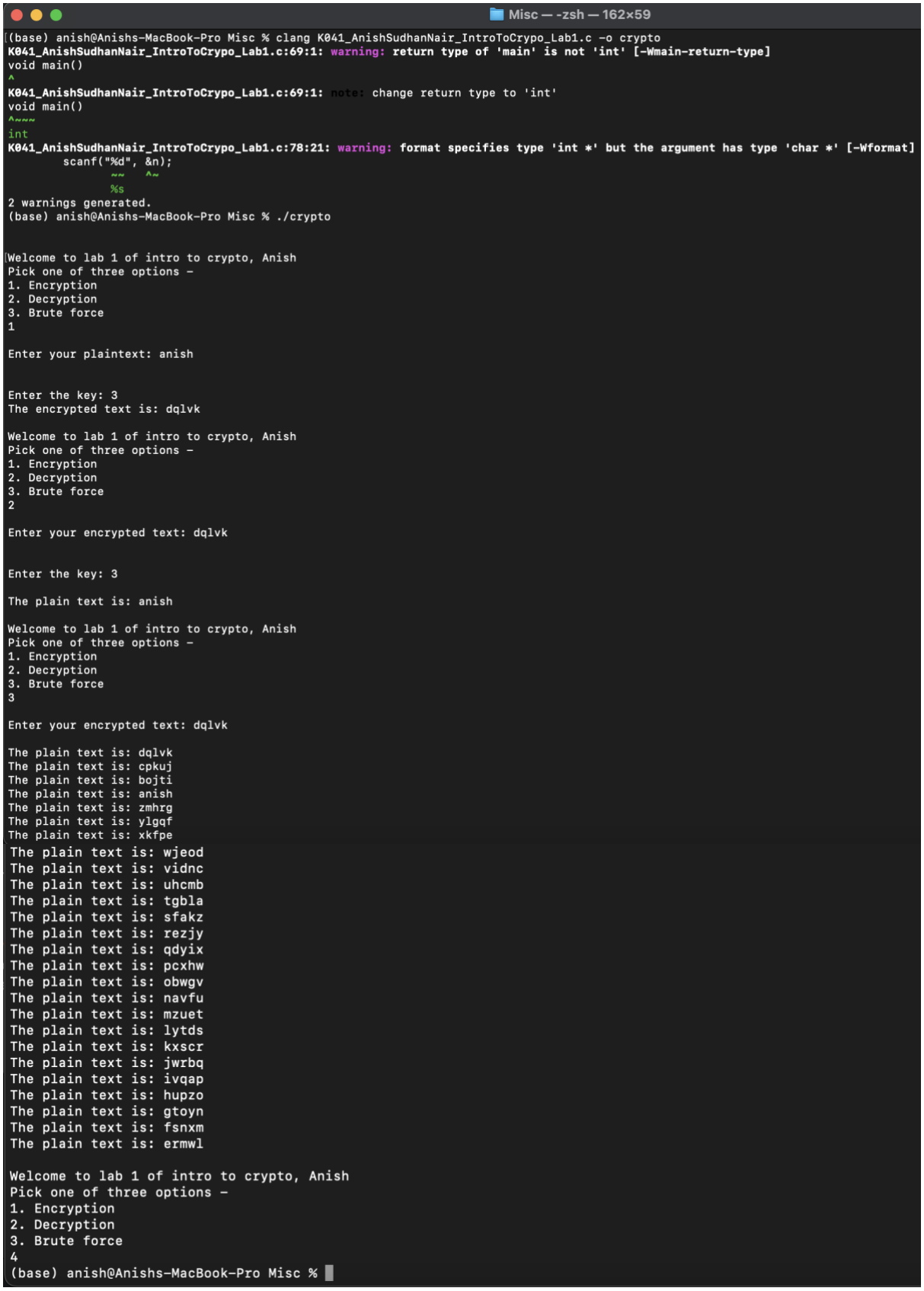
Editor: XCode

K041_AnishSudhanNair_IntroToCrypo_Lab1.c 〉 No Selection

```c
#include <stdio.h>
#include <ctype.h>

int key_check(int key)
{
    return key%26;
}
void encrypt(char pln_txt[100], int key)
{
    if (key>25)
    key_check(key);
    int temp;
    int ab=5;
    char new_txt[10]="";
    char ch, temp2;

    for (int i=0;pln_txt[i]!='\n';i++)
    {
        ch = tolower(pln_txt[i]);
        temp = (ch + key);
        if (temp>122)
            temp-=26;
        if (pln_txt[i]==' ')
        {
            new_txt[i]= ' ';
            continue;
        }
        temp2 = temp;
        new_txt[i]= temp2;
    }
    fflush(stdin);
    printf("The encrypted text is: ");
    printf("%s", new_txt);
}

void decrypt(char enc_txt[100], int key)
{
    if (key>25)
    key_check(key);
    int temp;
    char new_txt[10]="";
    char ch, temp2;

    for (int i=0;enc_txt[i]!='\n';i++)
```

```
    {
        ch = tolower(enc_txt[i]);
        temp = (ch - key);
        if (temp<97)
            temp+=26;
        if (enc_txt[i]==' ')
        {
            new_txt[i]= ' ';
            continue;
        }
        temp2 = temp;
        new_txt[i]= temp2;
    }
    fflush(stdin);
    printf("\nThe plain text is: ");
    printf("%s", new_txt);
}

void bruteforce(char enc_txt[100])
{
    for(int i=0;i<26;i++)
    decrypt(enc_txt, i);
}

void main()
{
    char n;
    int key;
    char pln_txt[100], enc_txt[100];

    do{
        printf("\n\nWelcome to lab 1 of intro to crypto, Anish");
        printf("\nPick one of three options - \n1. Encryption \n2. Decryption \n3. Brute force\n");
        scanf("%d", &n);
        while ((getchar()) != '\n');

        switch(n)
        {

            case 1:
            fflush(stdin);
            printf("\nEnter your plaintext: ");
            fgets(pln_txt, sizeof(pln_txt), stdin);
            while ((getchar()) != '\n');
                printf("\nEnter the key: ");
                scanf("%d", &key);
                encrypt(pln_txt, key);
                break;

                case 2:
                printf("\nEnter your encrypted text: ");
                fgets(enc_txt, sizeof(enc_txt), stdin);
                while ((getchar()) != '\n');
                printf("\nEnter the key: ");
                scanf("%d", &key);
                decrypt(enc_txt, key);
                break;

                case 3:
                printf("\nEnter your encrypted text: ");
                fgets(enc_txt, sizeof(enc_txt), stdin);
                bruteforce(enc_txt);
                break;
          }
      }while(n!=4);
}
```

Output:


Misc — -zsh — 162×59
(base) anish@Anishs-MacBook-Pro Misc % clang K041_AnishSudhanNair_IntroToCrypo_Lab1.c -o crypto
K041_AnishSudhanNair_IntroToCrypo_Lab1.c:69:1: warning: return type of 'main' is not 'int' [-Wmain-return-type]
void main()
^
K041_AnishSudhanNair_IntroToCrypo_Lab1.c:69:1: note: change return type to 'int'
void main()
^~~~
int
K041_AnishSudhanNair_IntroToCrypo_Lab1.c:78:21: warning: format specifies type 'int *' but the argument has type 'char *' [-Wformat]
scanf("%d", &n);
~~ ^~
%s
2 warnings generated.
(base) anish@Anishs-MacBook-Pro Misc % ./crypto
Welcome to lab 1 of intro to crypto, Anish
Pick one of three options -
1. Encryption
2. Decryption
3. Brute force
1
Enter your plaintext: anish
Enter the key: 3
The encrypted text is: dqlvk
Welcome to lab 1 of intro to crypto, Anish
Pick one of three options -
1. Encryption
2. Decryption
3. Brute force
2
Enter your encrypted text: dqlvk
Enter the key: 3
The plain text is: anish
Welcome to lab 1 of intro to crypto, Anish
Pick one of three options -
1. Encryption
2. Decryption
3. Brute force
3
Enter your encrypted text: dqlvk
The plain text is: dqlvk
The plain text is: cpkuj
The plain text is: bojti
The plain text is: anish
The plain text is: zmhrg
The plain text is: ylgqf
The plain text is: xkfpe
The plain text is: wjeod
The plain text is: vidnc
The plain text is: uhcmb
The plain text is: tgbla
The plain text is: sfakz
The plain text is: rezjy
The plain text is: qdyix
The plain text is: pcxhw
The plain text is: obwgv
The plain text is: navfu
The plain text is: mzuet
The plain text is: lytds
The plain text is: kxscr
The plain text is: jwrbq
The plain text is: ivqap
The plain text is: hupzo
The plain text is: gtoyn
The plain text is: fsnxm
The plain text is: ermwl
Welcome to lab 1 of intro to crypto, Anish
Pick one of three options -
1. Encryption
2. Decryption
3. Brute force
4
(base) anish@Anishs-MacBook-Pro Misc %

Questions:

1. What are the goals of cryptography?

The primary goal of cryptography is to facilitate secure communication that remains private between the concerned parties i.e., the sender and the receiver and is unable to be understood by any authorised third party.

2.Explain following terms wrt cryptography.

a. Plain text: This is any text that can be understood by humans in the native human alphabet and doesn't need to "decoded" in order to be comprehensible. This text is encoded using encryption techniques to derive encoded messages.
b. Cipher text: This is the encoded or encrypted text that needs to be decoded with the help of a particular key or technique known only to the sender and receiver in order to comprehend the message in normal alphabet.
c. Cipher: This is the technique or method of encryption/decryption comprising of algorithms and software that encodes a plain text message into cipher text.
d. Encryption: It is the process by which a plain text is encoded or converted into a cipher text(encrypted incomprehensible text) with the help of a cipher and the relevant key.
e. Decryption: It is the process by which the relevant cipher text is decoded or converted back to plain text with the help of the appropriate cipher and the key.
f. Key: It is a secret code or parameter employed by the relevant cipher to encode/decode a message. Keys are usually kept private to only the sender and receiver to ensure privacy of communication. In systems like RSA, which have a public key-private key system, the private key is always kept hidden.
g. Key space: It is the sample space or complete set of all possible keys for a particular cipher (or algorithm) that may be used for encryption/decryption.

3.What is brute force attack?

A brute force attack also known as an exhaustive key search in cryptographic contexts, is when every key or possible value/passkey for a given cipher(encryption) or authentication is tried sequentially one after the other. It is an attack that rests on guesswork and mathematical probability, trying all combinations until the right key/passkey is found.

4. Explain statistical analysis attack.

Statistical analysis attacks also known as frequency analysis is an integral part of cryptanalysis used against classical ciphers. It is executed by tabulating the frequency of characters appearing in a cipher text or encoded message and comparing it against the frequency tables of the relevant alphabet of the plain text. By comparing the frequencies of appearance of a character in an alphabet's literature, corresponding assumptions are drawn between the tables and the key is figured out so.