CSS|01|Dheeraj Lalwani|1902085|C21

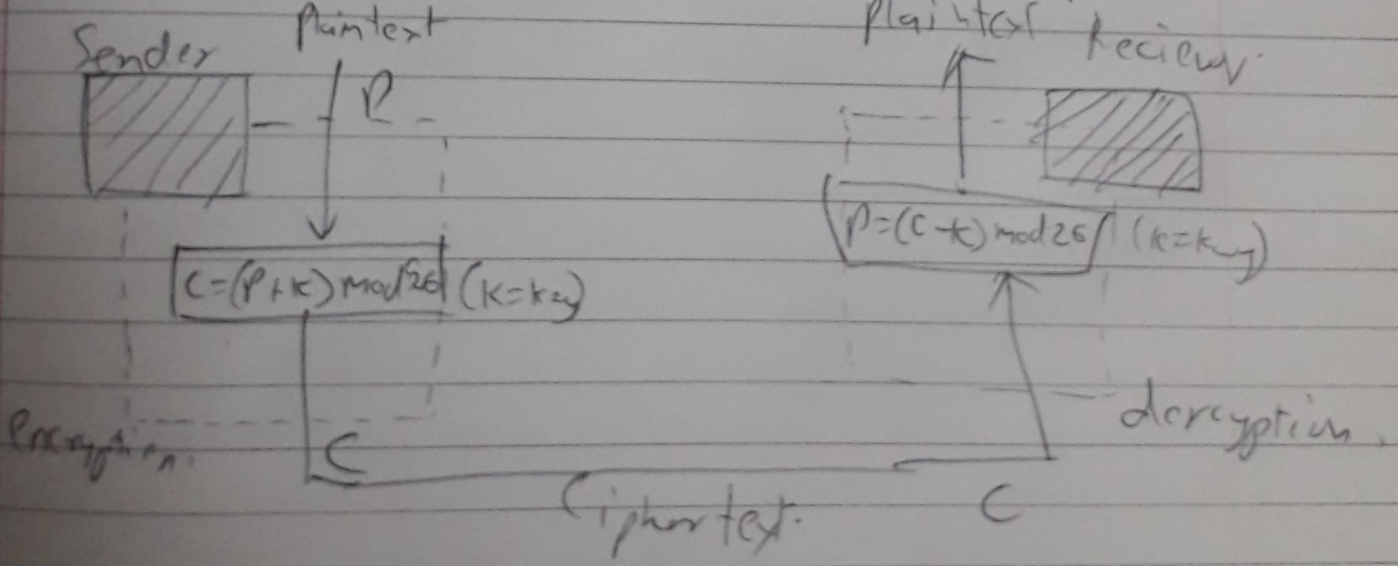
Page No.:
Date:

Assignment-1

Aim: To study, understand and implement Caesar Cipher using any programming language.

Theory:

1) The Caesar cipher technique is one of simplest method of encryption.
2) It's a type of substitution cipher which means that each text is replaced by some other text some fixed position.
3) For example, for a shift of 2
   A becomes C, B becomes D, ... etc.
4) Encryption and decryption process of Caesar Cipher uses modulo arithmetic.
5) Take a look at the diagram below.



CAESAR CIPHER

hello
holxox

Page No.
Date:
YOUVA

Example:- Use Caesar Cipher to encrypt and then decrypt the message "Water" with key = 10

W → 22 → (22+10)%26 → 6 → G
A → 00 → (00+10)%26 → 10 → K
T → 19 → (19+10)%26 → 3 → D
E → 04 → (4+10)%26 → 14 → O
R → 17 → (17+10)%26 → 01 → B

Encrypted String:- GKDOB

G → 6 → (6-10)%26 → 22 → W
K → 10 → (10-10)%(26) → 00 → A
D → 3 → (3-10)%(26) → 19 → T
O → 14 → (14-10)%26 → 04 → E
B → 01 → (1-10)%26 → 17 → R

Decrypted String:- WATER

Assignment 1

Caesar's Cipher (Implementation)

Code

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <ctype.h>

char *encrypt(char message[], int shift)
{
     int i;
     for (i = 0; i < strlen(message); i++)
     {
          // printf("Debug Original: %c = %d\n", message[i], message[i]);
          if ((int)message[i] == 32)
          {
               message[i] = message[i];
          }
        else if ((int)message[i] + shift > 126)
          {
               message[i] = (char)((((int)message[i] + shift) % 94));
          }
          else
          {
               message[i] = (char)((int)message[i] + shift);
          }
          // printf("Debug Encrypted: %c = %d\n", message[i], message[i]);
     }
     return message;
}

char *decrypt(char message[], int shift)
{
     int i;
     for (i = 0; i < strlen(message); i++)
     {
        // printf("Debug Original: %c = %d\n", message[i], message[i]);
        if ((int)message[i] == 32)
          {
               message[i] = message[i];
          }
          else if ((int)message[i] - shift < 32)
          {
               message[i] = (char)(126 - (32 - ((int)message[i] -
shift)));
          }
          else
          {
               message[i] = (char)((int)message[i] - shift);
          }
```

Dheeraj Lalwani
1902085

```
            // printf("Debug Decrypted: %c = %d\n", message[i], message[i]);
        }
        return message;
}

int main(int argc, char *argv[])
{
        if (strcmp(argv[1], "-e") == 0)
        {
                printf("You chose to encrypt data with a shift of %d\n",
atoi(argv[3]));
                printf("Original string: | %s |\n", argv[2]);
                printf("Encrypted string: | %s |\n", encrypt(argv[2],
atoi(argv[3])));
        }
        else if (strcmp(argv[1], "-d") == 0)
        {
                printf("You chose to decrypt data with a shift of %d\n",
atoi(argv[3]));
                printf("Original string: | %s |\n", argv[2]);
                printf("Decryped string: | %s |\n", decrypt(argv[2],
atoi(argv[3])));
        }
        else
        {
                printf("Please enter a valid option.");
        }

        return 0;
}
```

Output

```
C:\Users\USER\OneDrive\Desktop\practicals\CSS\CeasarCipher>gcc CaesarCipher.c -o CaesarCipher

C:\Users\USER\OneDrive\Desktop\practicals\CSS\CeasarCipher>CaesarCipher -e "Is your name Nikita?" 15
You chose to encrypt data with a shift of 15
Original string: | Is your name Nikita? |
Encrypted string: | X$ *~&# }p|t ]xzx%pN |

C:\Users\USER\OneDrive\Desktop\practicals\CSS\CeasarCipher>CaesarCipher -d "X$ *~&# }p|t ]xzx%pN" 15
You chose to decrypt data with a shift of 15
Original string: | X$ *~&# }p|t ]xzx%pN |
Decryped string: | Is your name Nikita? |
```