

Date : / /

Page No.

Ashish Kumar

2019UCO1518

Assignment 1

(1) Key: ALGORITHM

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

(2) Plain text: I only regret that I have but one life to give for my country.

Diagrams

Fillers used = 'x' → if letters are same
'z' → complete pair.

io → ma	et → dh
nl → pa	og → no
yx → ze	iv → ca
eg → qh	ef → fj
ne → gj	ox → xa
tx → hw	my → jo
th → hm	co → fa
at → li	ur → np
ih → tm	tx → bl
av → ia	yz → zv

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

eb → jh

ut → pb

on → as

el → dg

if → mc

encrypted message !

mapazoghgjhw hm li tm ia jh pb as dg mcdh

hoca jna fo janip blzv.

(3)

$$C = E(K, P) = P \times K \text{ mod } 26$$

$$K = \begin{pmatrix} 7 & 3 \\ 2 & 5 \end{pmatrix}$$

$P =$ 'meet me at the usual place at ten rather than
light o clock

$$me = [12 \ 4] \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix} = [(12 \times 7 + 8) \ (36 + 20)]$$

$$= [84 + 8 \ 36 + 20] \Rightarrow [92 \ 56] \% 26 = [14 \ 4] = ee$$

$$et = [4 \ 19] [K] = [14 \ 3] \rightarrow od$$

$$mc = [12 \ 4] [K] = [14 \ 4] \rightarrow oe$$

$$at = [0 \ 19] [K] = [12 \ 17] \rightarrow mx$$

$$th = [19 \ 7] [K] = [17 \ 14] \rightarrow xo$$

$$lv = [4 \ 20] [K] = [16 \ 8] \rightarrow qi$$

$$su = [18 \ 20] [K] = [10 \ 24] \rightarrow ky$$

$$al = [0 \ 11] [K] = [22 \ 3] \rightarrow wd$$

$$pl = [15 \ 11] [K] = [23 \ 22] \rightarrow xv$$

$$ac = [0 \ 20] [K] = [4 \ 10] \rightarrow ek$$

$$ca = [4 \ 0] [K] = [2 \ 12] \rightarrow cm$$

$$tt = [19 \ 19] [K] = [15 \ 22] \rightarrow pr$$

$$cv = [4 \ 13] [K] = [2 \ 25] \rightarrow cz$$

$$ua = [17 \ 0] [K] = [15 \ 25] \rightarrow pz$$

$$th = [19 \ 7] [K] = [17 \ 14] \rightarrow xo$$

$$ur = [4 \ 17] [K] = [10 \ 14] \rightarrow kt$$

$$th = [19 \ 7] [K] = [17 \ 14] \rightarrow xo$$

$$an = [0 \ 13] [K] = [0 \ 13] \rightarrow an$$

$$li = [4 \ 8] [K] = [18 \ 0] \rightarrow sa$$

$$gh = [6 \ 7] [K] = [4 \ 1] \rightarrow eb$$

$$to = [19 \ 14] [K] = [5 \ 23] \rightarrow fr$$

$$cl = [2 \ 11] [K] = [10 \ 9] \rightarrow kj$$

$$oc = [14 \ 2] [K] = [21 \ 0] \rightarrow ya$$

$$px = [10 \ 23] [K] = [12 \ 15] \rightarrow mp$$

\Rightarrow eedoe mmoqi kywdmwsekcm pr cz pzro kt xo anxa ebfxkjyamp

Calculating above values after multiplying with matrix K

```

ashish.cpp  code.cpp  block ciepher and stream ciepher  input.txt  output.txt
1  #include <bits/stdc++.h>
2  using namespace std;
3
4
5
6  int main() {
7      int t; cin >> t;
8
9      while (t--) {
10         int a, b;
11         cin >> a >> b;
12
13         int val1 = 7 * a + 2 * b;
14         int val2 = 3 * a + 5 * b;
15
16         cout << val1 % 26 << " " << val2 % 26 << endl;
17     }
18     return 0;
19 }

```

input.txt	output.txt
1 24	1 14 4
2 12 4	2 14 3
3 4 19	3 14 4
4 12 4	4 12 17
5 0 19	5 17 14
6 19 7	6 16 8
7 4 20	7 10 24
8 18 20	8 22 3
9 0 11	9 23 22
10 15 11	10 4 10
11 0 2	11 2 12
12 4 0	12 15 22
13 19 19	13 2 25
14 4 13	14 15 25
15 17 0	15 17 14
16 19 7	16 10 19
17 4 17	17 17 14
18 19 7	18 0 13
19 0 13	19 18 0
20 4 8	20 4 1
21 6 7	21 5 23
22 19 14	22 10 9
23 2 11	23 24 0
24 14 2	24 12 15
25 10 23	25

Date: / /
 Page No.

Ques-4 word = "cryptographic"

 key = "eng"

⇒ key = e n g e n g e n g e n g e

 text = c r y p t o g r a p h i c

$$C_i = (P_i + K_{i \% 26}) \bmod 26$$

⇒ $K_{i \% 26}$	4	13	6	4	13	6	4	13	6	4	13	6	4
P_i	2	17	24	15	19	6	20	10	4	6	19	8	2
$C_i =$	6	4	4	19	6	12	24	23	10	10	20	10	6

⇒ g e e t g u k e g t u o g

⇒ geetgukegtuog

Question 5

```
#include <bits/stdc++.h>
using namespace std;

string encrypt(string &text , int k)
{
    string res = "" , word;

    stringstream X(text);

    while (getline(X , word, ' ')) {
        for (char c : word) {
            char new_char = 'a' + (c - 'a' + k) % 26 ;
            res.push_back(new_char);
        }
        res += " ";
    }
    return res;
}

string decrypt(string &text , int k)
{
    string res = "" , word;

    stringstream X(text);

    while (getline(X , word, ' ')) {
        for (char c : word) {
            char new_char = 'a' + (c - 'a' - k + 26 ) % 26 ;
            res.push_back(new_char);
        }
        res += " ";
    }
    return res;
}

int main() {

    string plain_text , encrypt_text , decrypt_text ;
    int test_case , key ;

    getline(cin , plain_text);
    cout << "Plain text is : " << plain_text << "\n\n" ;

    cin >> test_case ;

    for (int i = 1 ; i <= test_case ; i++) {
```

```

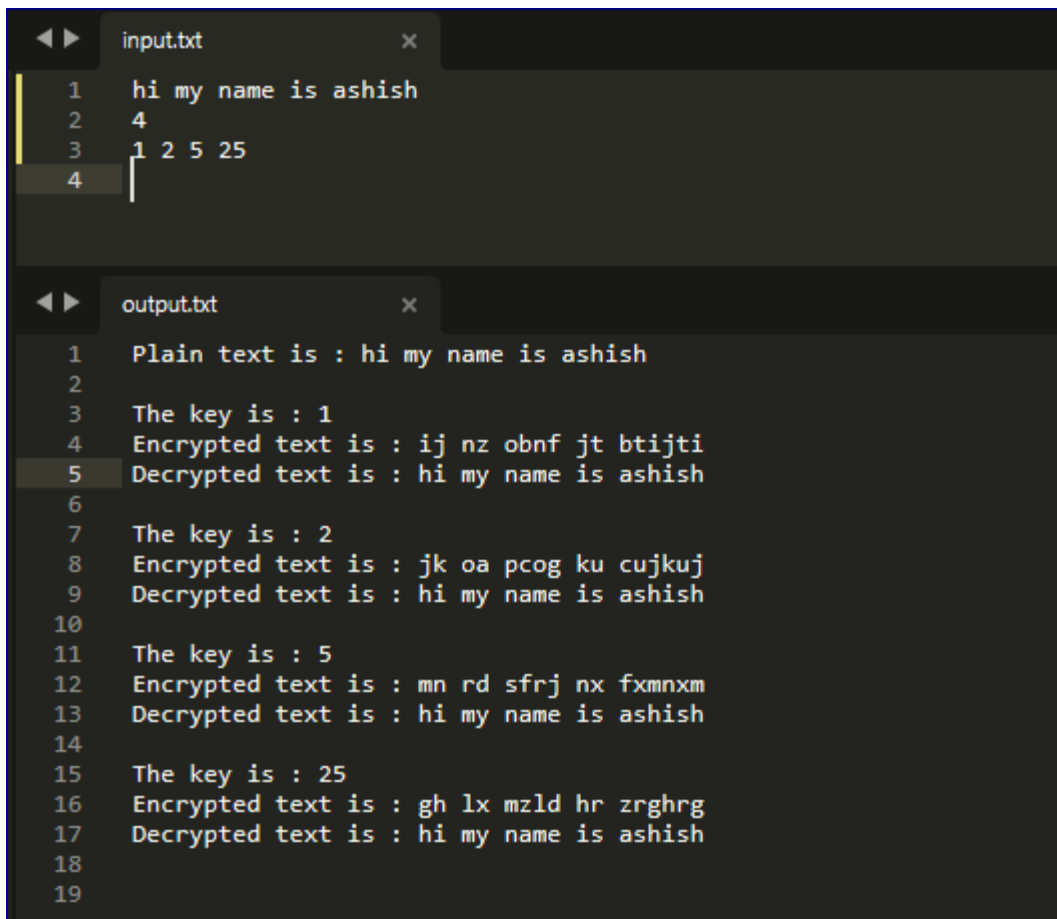
    cin >> key;
    cout << "The key is : " << key << endl;

    encrypt_text = encrypt(plain_text , key);
    cout << "Encrypted text is : " << encrypt_text << endl;

    decrypt_text = decrypt(encrypt_text , key);
    cout << "Decrypted text is : " << decrypt_text << "\n\n";
}
return 0;
}

```

Output:



The screenshot shows a code editor with two files: `input.txt` and `output.txt`. The `input.txt` file contains the following text:

```

1 hi my name is ashish
2 4
3 1 2 5 25
4

```

The `output.txt` file contains the following text:

```

1 Plain text is : hi my name is ashish
2
3 The key is : 1
4 Encrypted text is : ij nz obnf jt btijti
5 Decrypted text is : hi my name is ashish
6
7 The key is : 2
8 Encrypted text is : jk oa pcog ku cujkuj
9 Decrypted text is : hi my name is ashish
10
11 The key is : 5
12 Encrypted text is : mn rd sfrj nx fxmnm
13 Decrypted text is : hi my name is ashish
14
15 The key is : 25
16 Encrypted text is : gh lx mzld hr zrghrg
17 Decrypted text is : hi my name is ashish
18
19

```