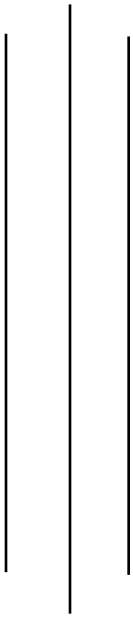


Programme Name: **BCS HONS**

Course Code: **CSC 2735**

Course Name: **Network And Data Security**

Assignment / Lab Sheet / Project / Case Study No. **2**

Date of Submission: **2020/1/5**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

1. **Write a program to implement a rail fence cipher algorithm. A program must implement encryption and decryption algorithm inside encrypt and decrypt function. Verify the implementation of an algorithm by passing a plain text as your name in encrypt function and decipher the generated cipher text using decryption function**

Solution:

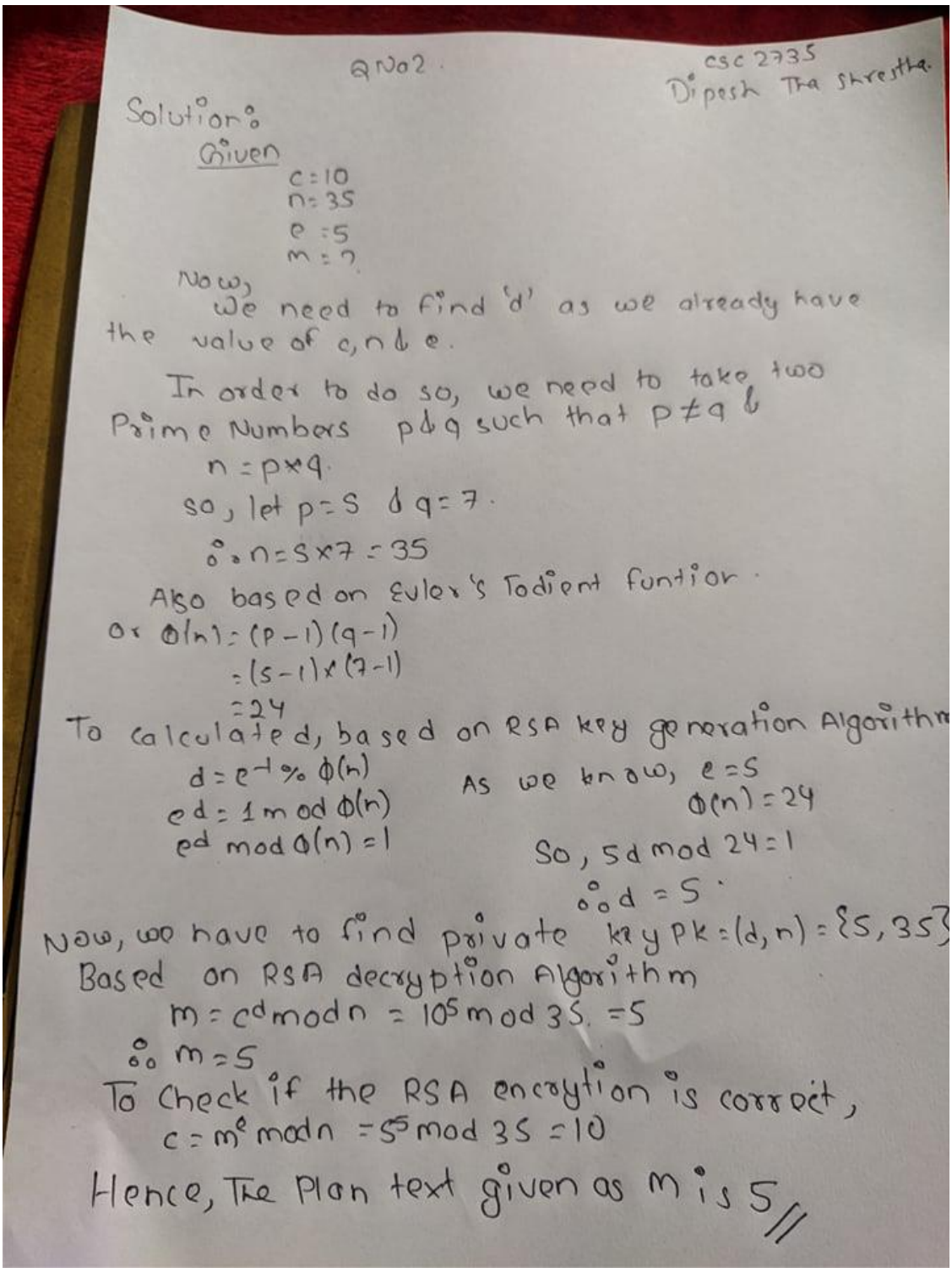
```
#include<stdio.h>
#include<string.h>

void encryptMsg(char msg[], int key){
 int msgLen = strlen(msg), i, j, k = -1, row = 0, col = 0;
char railMatrix[key][msgLen];

   for(i = 0; i < key; ++i)
for(j = 0; j < msgLen; ++j)
railMatrix[i][j] = '\n';

   for(i = 0; i < msgLen; ++i){
railMatrix[row][col++] = msg[i];

      if(row == 0 || row == key-1)
         k= k * (-1);

      row = row + k;
   }

   printf("\nEncrypted Message: ");
```

```
   for(i = 0; i < key; ++i)        for(j = 0;
j < msgLen; ++j)
if(railMatrix[i][j] != '\n')
printf("%c", railMatrix[i][j]);
}

void decryptMsg(char enMsg[], int key){
   int msgLen = strlen(enMsg), i, j, k = -1, row = 0, col = 0, m = 0;
char railMatrix[key][msgLen];

   for(i = 0; i < key; ++i)
for(j = 0; j < msgLen; ++j)
railMatrix[i][j] = '\n';

   for(i = 0; i < msgLen; ++i){
railMatrix[row][col++] = '*';

      if(row == 0 || row == key-1)
         k= k * (-1);

      row = row + k;
   }

   for(i = 0; i < key; ++i)
  for(j = 0; j < msgLen; ++j)
if(railMatrix[i][j] == '*')
railMatrix[i][j] = enMsg[m++];
```

```
   row = col = 0;
k = -1;

   printf("\nDecrypted Message: ");

   for(i = 0; i < msgLen; ++i){
printf("%c", railMatrix[row][col++]);
if(row == 0 || row == key-1)
          k= k * (-1);

       row = row + k;
   }
}

int main(){
  char msg[] = "Hello World";
char enMsg[] = "Horel ollWd";
int key = 3;

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

   encryptMsg(msg, key);
decryptMsg(enMsg, key);

   return 0;
}
```

2. **In a public key system using RSA you intercept a cypher text C:10 sent to a user whose public key is e:5, n:35. What is the plaintext M?**

Answer:



Q No 2.

CSC 2735
Dipesh Tha Shrestha.

Solution:

Given

c = 10
n = 35
e = 5
m = ?

Now,
We need to find 'd' as we already have the value of c, n & e.

In order to do so, we need to take two Prime Numbers p & q such that p ≠ q &

$n = p \times q$.

so, let p = 5 & q = 7.

$\therefore n = 5 \times 7 = 35$

Also based on Euler's Todient funtion.

$\phi(n) = (p-1)(q-1)$
$= (5-1) \times (7-1)$
$= 24$

To calculate d, based on RSA key generation Algorithm

$d = e^{-1} \% \phi(n)$
$ed = 1 \bmod \phi(n)$
$ed \bmod \phi(n) = 1$

As we know, e = 5
$\phi(n) = 24$

So, $5d \bmod 24 = 1$

$\therefore d = 5$.

Now, we have to find private key $pk = (d, n) = \{5, 35\}$

Based on RSA decryption Algorithm

$m = c^d \bmod n = 10^5 \bmod 35 = 5$

$\therefore m = 5$

To check if the RSA encryption is correct,

$c = m^e \bmod n = 5^5 \bmod 35 = 10$

Hence, The Plan text given as m is 5 //

3. **Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.**

Solution:

- **Confidentiality:**

To access card user must enter account number or a security password which is available only to authorized users and aimed at further enhancing the level of security. While securing the PIN of a respective card it is the responsibility of end user to ensure they use a strong pin. Banks also need to ensure privacy whenever a communication is happening in between Cash Deposit Machine and bank server to prevent hacking. The entire transaction needs to be properly secured so to avoid any kind of harm or hackers cracking the card pins and accessing.
Proper encryption of PIN ensures that high level of confidentiality is maintained while lack of attention towards the same could lead to breach of data or customer's information. Moreover, the policy related to changing PIN after regular intervals will help boost the customers and keep data and information secure.

- the communication channel between the Cash Deposit Machine and the bank must be encrypted.
- the PIN or account number must be encrypted (wherever it is stored).

- **Integrity:**

Use of advanced, efficient technology and proper optimization & Collaboration of Cash Deposit Machine's is necessary to ensure their integrity is maintained and customer's information is secure. Both in case of withdraw and deposit, systems must be updated chronologically with authentic data and does not affect the customer account in any manner. Withdrawals of money should reflect as debits on the account, deposit of funds would result in credit of account.

Moreover, a section or committee should be incorporated to handle queries of customers which are related with mismatch of account due to use of Cash Deposit Machine.

- **Availability:**

The frequency of Cash Deposit machine should enhance depending upon the demand of the customers and further should be frequently updated with cash to provide accurate services. While Cash Deposit Machine which is out of service could lead to customer dissatisfaction, that of Cash Deposit Machine with accuracy in services could attract more and more customers

- the system must be able to serve at least X concurrent users at any given time.
- the system must be available 99.9% of the time.