VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

File Data Encryption and Decryption Using Rabin Cryptosystem

A project submitted

in partial fulfilment of the requirements for the degree of

Bachelor of Technology in Computer Science and Engineering

By

VARUN KAUSHIK (17BCE0182)

Course Instructor

Prof. Ramani S.

UNDERTAKING

This is to declare that the project entitled "File Data Encryption and Decryption Using Rabin Cryptosystem" is an original work done by undersigned, in partial fulfillment of the requirements for the degree "Bachelor of Technology in Computer Science and Engineering" at School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore.

All the analysis, design and system development have been accomplished by the undersigned. Moreover, this project has not been submitted to any other college or University.

VARUN KAUSHIK

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. The necessity and the fact that exchanged messages are exposed to other people during the transmission promoted the creation of encryption systems, enabling just the recipients to interpret the exchanged information. This report considers an overview of cryptographic schemes, in particular the Rabin cryptosystem. The report deals with the underlying principles of Rabin Cryptosystem, importance of Rabin cryptosystem and the implementation of Rabin cryptosystem is done in C++ programming language, and in my project, I have Encrypted and Decrypted the file data using Rabin cryptosystem. My proposed method to overcome Rabin cryptosystem decryption shortcoming, and the report concludes the different potentials uses of the application.

However, the Rabin cryptosystem has the advantage that it has been mathematically proven to be computationally secure against a chosen-plaintext attack as long as the attacker cannot efficiently factor integers, while there is no such proof known for RSA. In addition, me proposed methods produce a unique decryption result without decryption failure and are indeed as intractable as the integer factorization problem.

2. An overview of Rabin Cryptosystem

Data protection has been traditionally ensured with cryptography which plays a major role throughout many applications such as e-commerce, e-mail, mobile phone communication, Pay-Tv, sending financial information and so forth. Cryptography can be defined as the science of implementing and developing techniques to encrypt a message in a way that could be impossible to get altered or misused by the third party. The algorithm used here is Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However, the Rabin cryptosystem has the advantage that the problem on which it relies has been proved to be as hard as integer factorization, which is not currently known to be true of the RSA problem. It has the disadvantage that each output of the Rabin function can be generated by any of four possible inputs; if each output is a cipher text, extra complexity is required on decryption to identify which of the four possible inputs was the true plaintext.

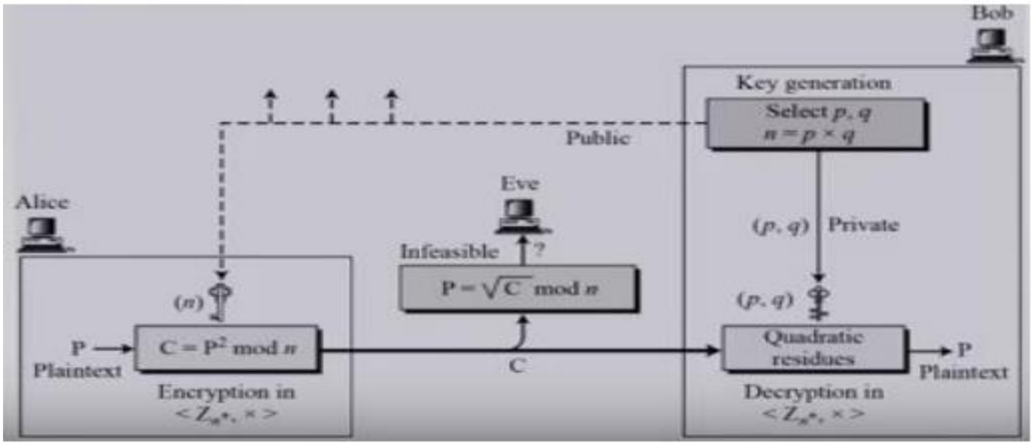


Figure-2.1

The most important aspect in our daily life is data communication. The main issue in data communication is data security to preserve its availability, integrity, proper access control as well as confidentiality. Therefore, Data protection is essential from misuse. The Rabin system uses both a public and a private key. The public key is necessary for later encryption and can be published, while the private key must be possessed only by the recipient of the message.

2.1 OBJECTIVES

- Its working and applications in different areas like to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

- To refine the Rabin encryption scheme in order to defeat all the previous drawbacks of its original design and its variants.

- Present efficient and practical methods to overcome Rabin cryptosystem decryption failure without using the Jacobi symbol, message redundancy technique or sending extra information in order to specify the correct plaintext.

- In addition, I have proposed methods to produce a unique decryption result without decryption failure and are indeed as intractable as the integer factorization problem.

- Implement a file encryption technique using RABIN CRYPTOSYSTEM for the windows platform.

- The encryption would be for the files like txt and doc file.

3. METHODOLOGY

The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. HoIver the Rabin cryptosystem has the advantage that the problem on which it relies has been proved to be as hard as integer factorization, which is not currently known to be true of the RSA problem. It has the disadvantage that each output of the Rabin function can be generated by any of four possible inputs; if each output is a cipher text, extra complexity is required on decryption to identify which of the four possible inputs was the true plaintext.

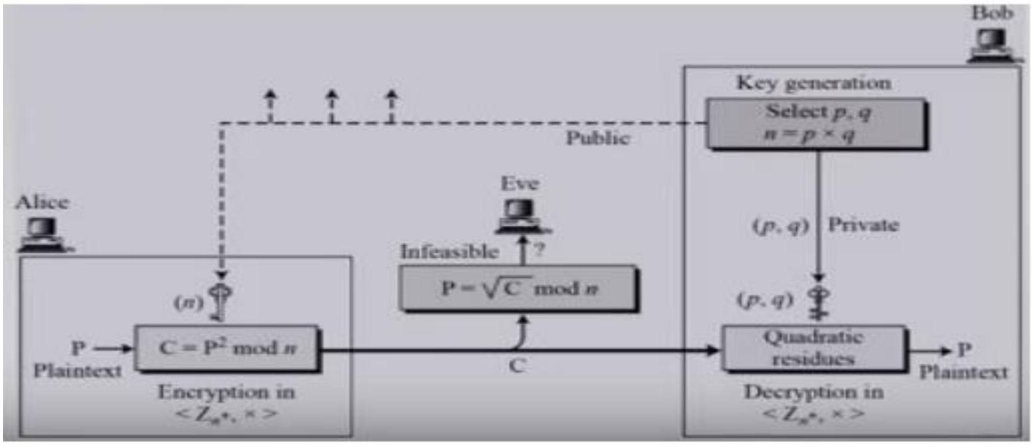
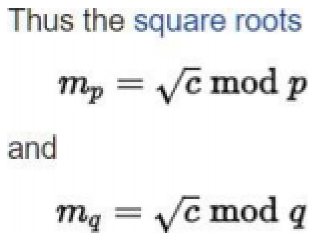


Figure-3.1

The Rabin system uses both a public and a private key. The public key is necessary for later encryption and can be published, while the private key must be possessed only by the recipient of the message.

Choose two large distinct primes p and q, which act as private keys, n=p*q where n is the public key. To encrypt a message only the public key n is needed. To decrypt a cipher text the factors p and q of n are necessary. Cipher text c is determined by c=m2 mod n, where m ϵ Plaintext.

If c and n are known, the plaintext is then m2≅ c mod n



Thus the square roots

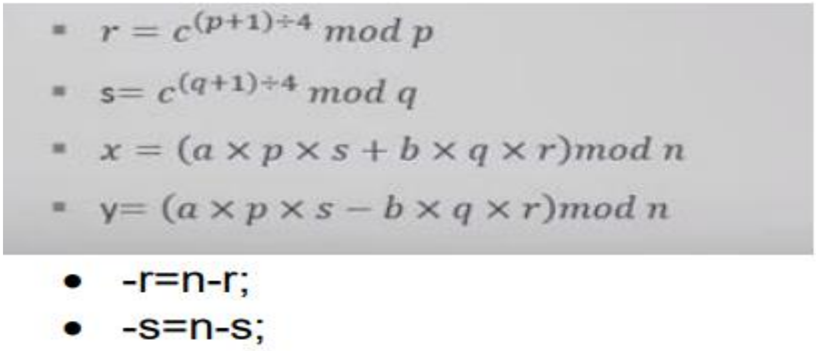
$$m_p = \sqrt{c} \bmod p$$

and

$$m_q = \sqrt{c} \bmod q$$

By applying the extended Euclidean algorithm, I find (a) and (b)such that a*p + b*q=1.

Using Chinese remainder theorem, four square roots are:



- $r = c^{(p+1)\div 4} \, mod\, p$
- $s = c^{(q+1)\div 4} \, mod\, q$
- $x = (a \times p \times s + b \times q \times r) mod\, n$
- $y = (a \times p \times s - b \times q \times r) mod\, n$

- -r=n-r;
- -s=n-s;

Figure-3.2

One of these square roots mod n is the original plaintext m. Finding the factorization of n is possible. If both r and s can be computed, as gcd(|r-s| , n) is either p or q.

3.1 LITERATURE SURVEY

[1] **Security Systems: A concept through Encrypting File System** by Shruti Jain, Chintal Kumar Patel et al. used Advance key management scheme to provide a high grade of security while remaining transparency and usability.

The advantage is it makes crucial distinction between the kernel and user- space from a security perspective. Realization in a distributed Storage-area network (SAN) file system.

[2] **CifrarFS – Encrypted File System Using FUSE** by Anagha Kulkarni, Vandana Inamdar et al. made an an encrypted file system using 'File system in USEr space (FUSE)' maintains all the files in a specific directory in an encrypted form and decrypts them on demand. It gives the advantage that It gives an extra security to the user against offline attacks. But it does have cons like Does not handle integrity of encrypted files in a more efficient way.

[3] **Efficient methodology for implementation of Encrypted File System in** User Space by Dr. Shishir Kumar ed al. did implementation of EFS in user space using faster cryptographic algorithms on UNIX Operating system . the pros of this were Implementing EFS in user space makes it portable & flexible; Kernel size will also not increase resulting in more reliable & efficient Operating System and con being It has shortcomings of a user-level NFS server based implementation

[4] Cryptfs: A Stackable Vnode Level Encryption File System by Erez Zadok, Ion Badulescu ed al. It is designed as a stackable Vnode layer loadable kernel module. Cryptfs operates by "encapsulating" a client file system with a layer of encryption transparent to the user. Cryptfs performs better than user-level or NFS based file servers such as CFS It is 2 to 37 times faster on micro-benchmarks such as read and write properly handling them requires some manipulation of lower level file systemsit forced us to maintain lots of state

[5] A survey of File encryption and decryption system based on Rabin cryptosystem by Suli Wang, Ganlai Liu used the Rabin public key encryption algorithm can be more convenient to communicate and manage easily communicate data and text files under the environment which demand a high security.

[6] Providing Data Protection User by Sunumol Cherian, Kavitha Murukezhan authentication, data protection, security are the key areas we consider. User authentication is provided using alphanumeric password and graphical password, security is provided using encryption of the file using key. Key management is an important concept used for the protection of data. Overall transactions are viewed by an auditor.

[7] Rabin Cryptosystem by Mamta jain and Saroj kumar, Rabin cryptosystem is an efficient factoring-based scheme, hoIver, its decryption produces 4-to-1 output, which leads to decryption failure. Many research projects discuss that variety of attacks that Rabin cryptosystem can fall prey to such as radio frequency attacks. Several attempts were made by researchers with the objectives to turn the Rabin cryptosystem to be as practical and implementable as the RSA cryptosystem. All the previous attempts made seem to utilize one or more additional techniques in order to obtain a unique decryption result, at the same time resulting in a free decryption failure Rabin-like cryptosystem. Some of the techniques to accomplish this are through manipulation of the Jacobi symbol during the key generation process, provide extra information and also use the concept of message padding during the encryption process. Also, it can be accomplish by designing an encryption function with a special message structure. Holver, at the same time all of the designs are losing the computational advantage of the original Rabin's encryption over the RSA cryptosystem.

3.3 TOOLS USED:

- Code blocks

4. CODE SNIPPET:

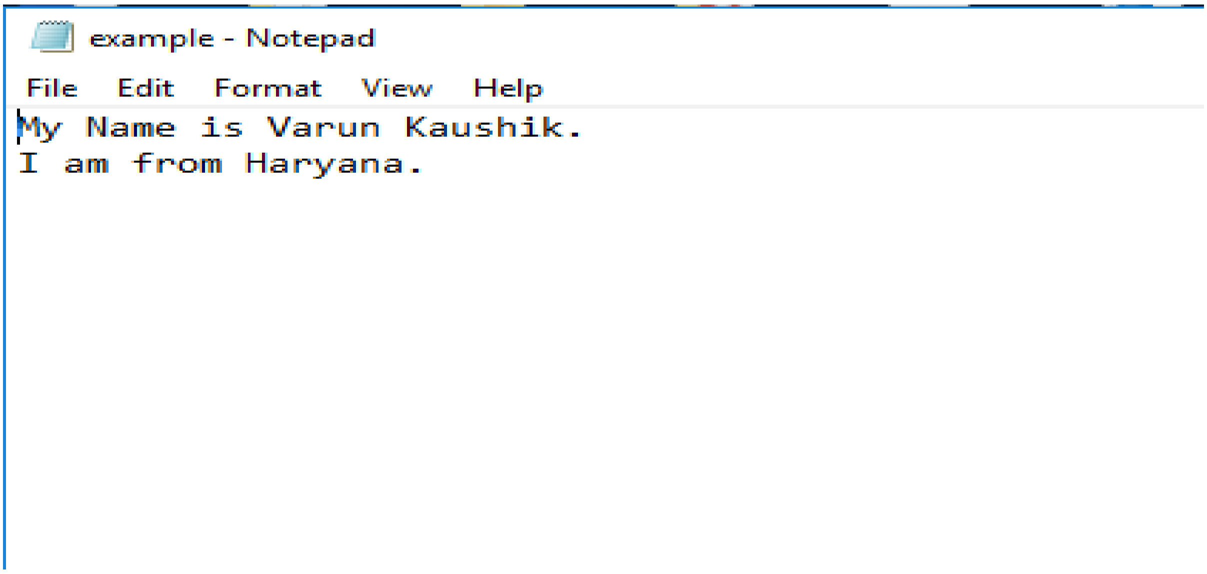
```
int modulo (int a, int b)

{

return a >= 0 ? a % b : ( b - abs ( a%b ) ) % b;

}

void encode(string s)

{
```

```
vector<int>l;

for(int i = 0; i < strlen(s.c_str()); i++)

{

l.push_back((int)s[i]);

}

copy(l.begin(), l.end(), ostream_iterator<int>(cout, ""));

}

void decode(vector<int> s)

{

vector<char>l;

for(int i = 0; i < s.size(); i++)

{

l.push_back(char(s[i]));

}

copy(l.begin(), l.end(), ostream_iterator<char>(cout, ""));

}

int encrypt(int m, int p, int q)

{

int c = (m * m)%n;

return c;

}

int mod(int k, int b, int m)

{

int i=0;

int a=1;

vector<int> t;

while(k>0)

{

t.push_back(k%2);

k=(k-t[i])/2;

i++;

}

for(int j=0; j<i; j++)

{
```

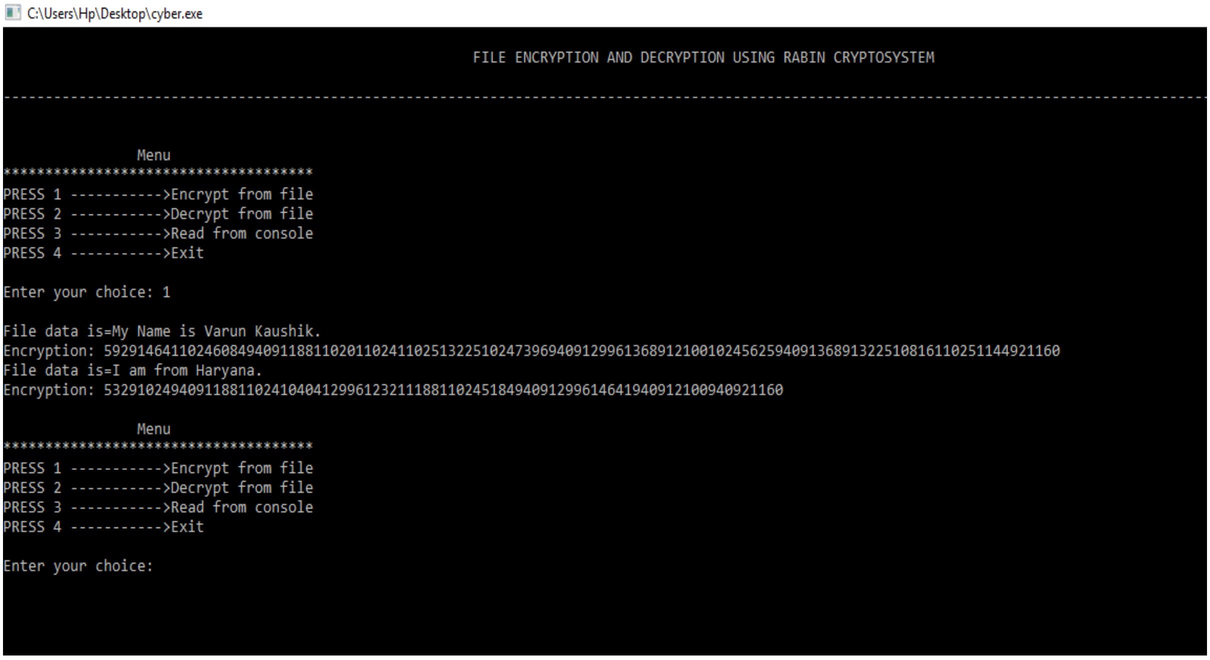
```
if(t[j]==1)
{
a=(a*b)%m;
b=(b*b)%m;
}
else
{
b=(b*b)%m;
}
}
return a;
}
vector<int> eea(int a, int b)
{
if (b>a)
{
int temp=a;
a=b;
b=temp;
}
int x=0;
int y=1;
int lastx=1;
int lasty=0;
while (b!=0)
{
int q= a/b;
int temp1= a%b;
a=b;
b=temp1;
int temp2 = x;
x=lastx-q*x;
lastx = temp2;
int temp3 = y;
```

```
y = lasty-q*y;
lasty=temp3;
}
vector<int>arr(3);
arr[0] = lastx;
arr[1] = lasty;
arr[2] = 1;
return arr;
}
int decrypt(int c, int p, int q)
{
int mp = mod((p+1)/4, c, p);
int mq = mod((q+1)/4, c, q);
vector<int> arr = eea(p, q);
int pp = arr[0]*p*mq;
int qq = arr[1]*q*mp;
double r = modulo((pp+qq), n);
if( r < 128)
return r;
int negative_r = n - r;
if (negative_r < 128) return negative_r;
int s = modulo((pp-qq), n);
if( s < 128)
return s;
int negative_s = n - s;
if( negative_s < 128)
return negative_s;
}

string console()
{
 string x;
 getline(cin,x);
 return x; }
```

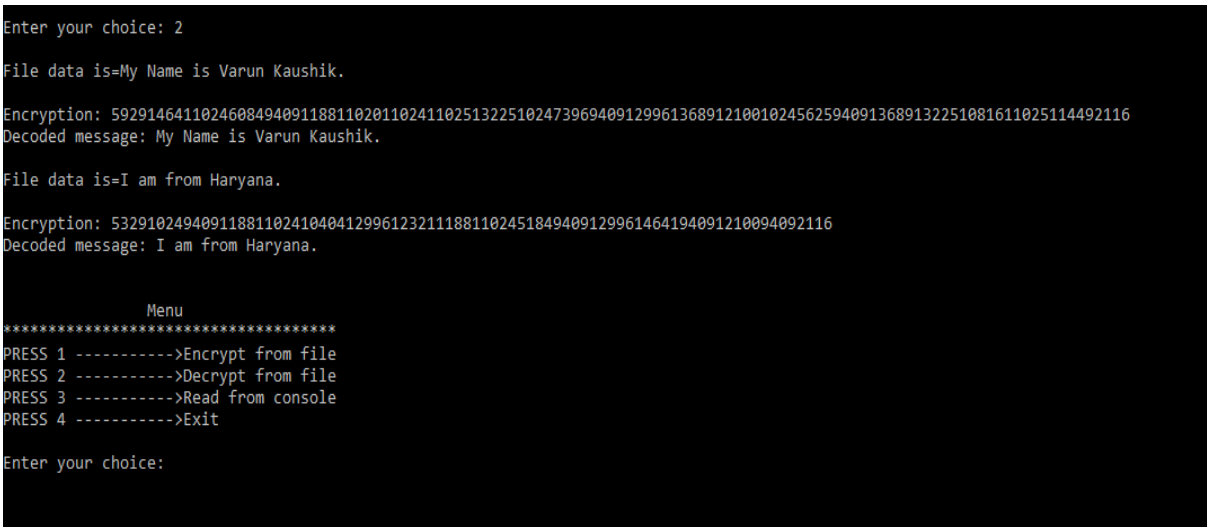
4.1 OUTPUT:



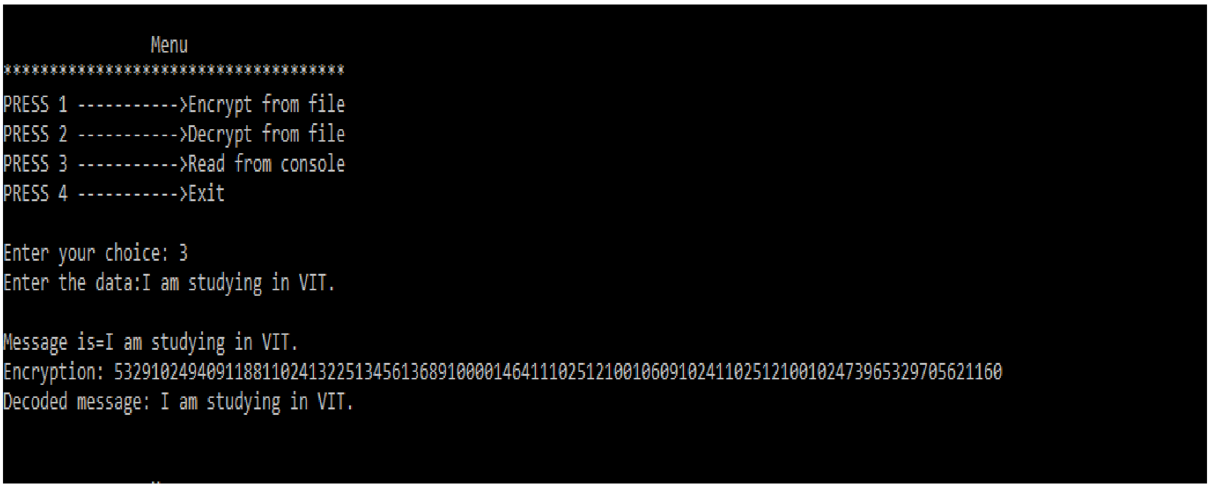
```
My Name is Varun Kaushik.
I am from Haryana.
```



```
                                                          FILE ENCRYPTION AND DECRYPTION USING RABIN CRYPTOSYSTEM

------------------------------------------------------------------------------------------------------------------------------------------------


                Menu
*************************************
PRESS 1 ----------->Encrypt from file
PRESS 2 ----------->Decrypt from file
PRESS 3 ----------->Read from console
PRESS 4 ----------->Exit

Enter your choice: 1

File data is=My Name is Varun Kaushik.
Encryption: 592914641102460849409118811020110241102513225102473969409129961368912100102456259409136891322510816110251144921160
File data is=I am from Haryana.
Encryption: 53291024940911881102410404129961232111881102451849409129961464194091210094092116 0

                Menu
*************************************
PRESS 1 ----------->Encrypt from file
PRESS 2 ----------->Decrypt from file
PRESS 3 ----------->Read from console
PRESS 4 ----------->Exit

Enter your choice:
```



```
Enter your choice: 2

File data is=My Name is Varun Kaushik.

Encryption: 59291464110246084940911881102011024110251322510247396940912996136891210010245625940913689132251081611025114492116
Decoded message: My Name is Varun Kaushik.

File data is=I am from Haryana.

Encryption: 5329102494091188110241040412996123211188110245184940912996146419409121009409211 6
Decoded message: I am from Haryana.


                Menu
*************************************
PRESS 1 ----------->Encrypt from file
PRESS 2 ----------->Decrypt from file
PRESS 3 ----------->Read from console
PRESS 4 ----------->Exit

Enter your choice:
```



```
              Menu
**************************************
PRESS 1 ----------->Encrypt from file
PRESS 2 ----------->Decrypt from file
PRESS 3 ----------->Read from console
PRESS 4 ----------->Exit

Enter your choice: 3
Enter the data:I am studying in VIT.

Message is=I am studying in VIT.
Encryption: 532910249409118811024132251345613689100001464111025121001060910241102512100102473965329705621160
Decoded message: I am studying in VIT.
```

5. FUTURE STUDY

This concept can be used in offices which requires highly secured files like Banks, Defense, Medical History documentations etc. Also prevents the attack if the attacker physically approaches the file hence this system is also used in publicly accessible computers like on Railways stations. These items cannot be encrypted: Compressed files, System files, System directories, Root directories Transactions. So in the further application we would try to make the file encryption and decryption possible for all of them. If someone gains the administrator rights can use it for the wrong.

5.1 CONCLUSION

Decoding produces three false results in addition to the correct one, so that the correct result must be guessed. I have proposed two efficient methods to overcome the Rabin cryptosystem decryption failure. In the proposed methods, I managed to not using the Jacobi symbol, message redundancy technique or sending extra information in order to specify the correct plaintext. So, in this way I overcome decryption failure of the Rabin cryptosystem in the most effective manner as opposed to existing methods and securing the file data using Rabin cryptosystem.

6. REFERENCES

- **A concept through Encrypting File System** by Shruti Jain, Chintal Kumar Patel.
- **CifrarFS – Encrypted File System Using FUSE** by Anagha Kulkarni, Vandana Inamdar
- **Efficient methodology for implementation of Encrypted File System in** User Space by Dr. Shishir Kumar
- **Cryptfs: A Stackable Vnode Level Encryption File System by** Erez Zadok, Ion Badulescu
- **A survey of File encryption and decryption system based on Rabin cryptosystem by** Suli Wang, Ganlai Liu.
- **Providing Data Protection User by** Sunumol Cherian, Kavitha Murukezhan
- **Rabin Cryptosystem by** Mamta jain and Saroj kumar