International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Encryption of Text Message Using A Combined Approach of Hexadecimal and Binary in GUI

Shefali Gulati[1], Urvashi Garg[2]

[1]M. Tech Scholar, [2]A.P, CSE Dept, HCTM, Kaithal, Haryana, India

Abstract— **In different cases of data transmission in a communication system the most widely used approach is encryption which is considered by far a necessary step. Encryption in simple words is locking of information in a box which needs a key to unlock; now it all depends upon the type of technique and its necessary awareness becomes a mandatory part of complete communication systems. Cryptography involves a 5-tuple (P, K, C, and E, D) consisting of the plain text or message P, set of keys K, cipher text C, encryption algorithm E and decryption algorithm D. An Original message is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as enciphering or encryption; restoring the plaintext from the cipher text is deciphering or decryption. The many scheme used for encryption constitute the area of study known as cryptography. In our research work we propose a new scheme which encrypts the text message in decrypt form by executing some steps. We expect that results of this technique are very fruitful with good accuracy level.**

Keywords—**Encryption, Decryption, Hexadecimal, Binary, Text**

I. Introduction To Cryptography Elements

Cryptography is the science of techniques and protocols intended to ensure information security. Cryptanalysis is the art of analysing and breaking secure communication; it consists in attacking cryptographic methods. Cryptography is practiced by cryptographers and cryptanalysis is practiced by cryptanalysts (attackers). Cryptology encompasses the branches of cryptography and cryptanalysis [1]. The purpose of cryptography is to provide a range of features for information security. The most important of them are [2]:

- Confidentiality (privacy) provides the secrecy of information content. It transforms the meaningful data into senseless message. Ciphers are the cryptographic algorithms used to guarantee this characteristic.
- Data integrity means its protection from unauthorized access and alteration. Possible changes in the original data are insertion and deletion. Integrity is achieved through cryptographic hash functions.
- Authentication is the identification of the transmitted information and of the parts engaged into a communication.
- Non-repudiation means to respect the obligations of a contract. This property can be obtained by using signatures.

Data that has perceptual meaning for us is called clear text or plain text. Transformation of the plaintext into an unreadable file is called encryption. Encrypted plaintext becomes cipher text. In order to obtain the original clear text, the process of decryption is applied on the cipher text data. These two processes of encryption and decryption are compositional parts of a cryptographic algorithm named cipher. A cipher is applied on the data together with a secret key. Cryptosystem includes encryption, decryption, key generation algorithm and all the necessary protocols to ensure secure communication [3]. The key space is the number of elements in the alphabet raised to the power of the key length. Key space is important for cryptanalysis; it gives the number of all the possible keys that can be as well the secret key.

Introduction notions and fundamental knowledge of information security is well covered in [1]. A comprehensive survey about security of data communications and networks is W. Stallings book [4]. Another reference which presents techniques and algorithms of greatest interest is [5]. A broad overview of computer security is presented in [6].

II. Hexadecimals

A Hexadecimal Number is based on the number 16. There are 16 Hexadecimal digits. They are the same as the decimal digits up to 9, but then there are the letters A, B, C, D, E and F in place of the decimal numbers 10 to 15:

Hexadecimal: 0 1 2 3 4 5 6 7 8 9 A B C D E F
Decimal: 0 1 2 3 4 5 6 7 8 9 101112131415

So a single Hexadecimal digit can show 16 different values instead of the normal 10.

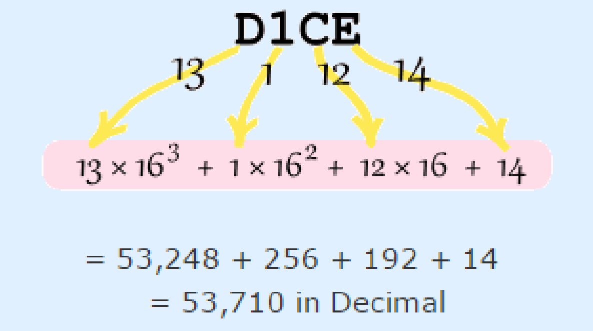


Figure 1 What is the decimal value of the hexadecimal number "D1CE"

III. USE CASE DIAGRAM

The diagram describes the capabilities expected from the system. For this purpose use-cases were used, which show typical interactions between the user and the system under development. The purpose was to capture each possible task that a user can perform with the system in a use-case. All the use-cases together should describe the full system functionality [7, 8]. Fig. 2 presents the use-case diagram for the proposed cipher program

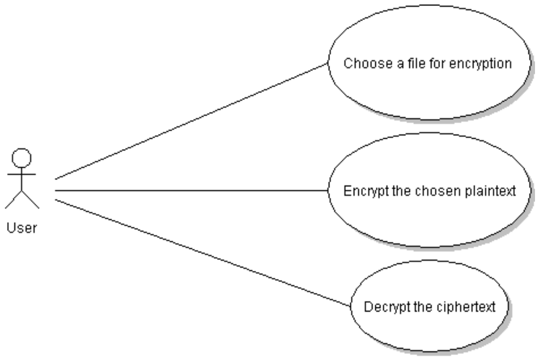
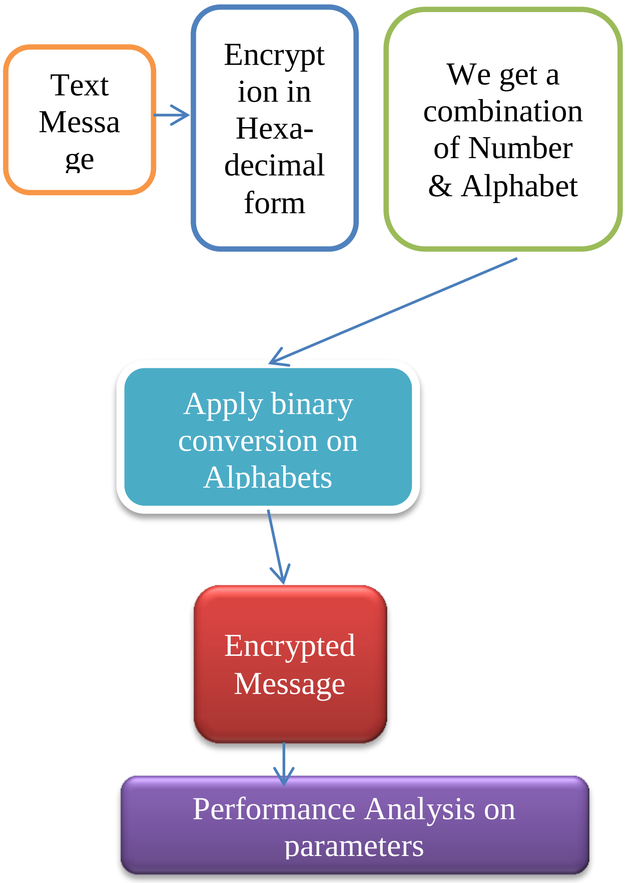


Figure 2 Use Case Diagrams

IV. CONCEPTUAL FRAMEWORK


Text Messa ge
Encrypt ion in Hexa-decimal form
We get a combination of Number & Alphabet
Apply binary conversion on Alphabets
Encrypted Message
Performance Analysis on parameters

V. TOOL USED FOR IMPLEMENTATION

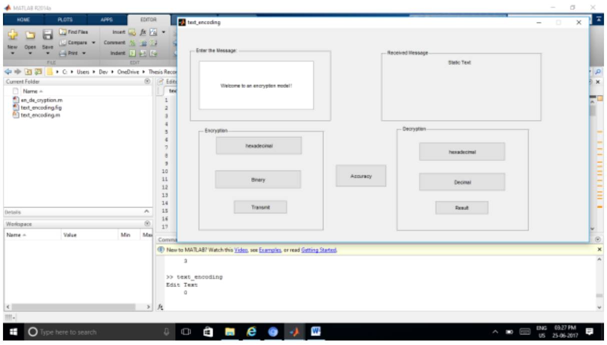
MATLAB (MATRIX LABORATORY) is providing an environment for computation in numerical form and we can say it a programming language of 4th generation. Math Works developed it, there is matrix manipulations, interaction with user, create functions, compatible with other languages as like C, C++ etc. By survey it found that near about one million users are available in market which follows MATLAB for programming and numerical computing. Students from any stream like engineering, science etc can use this tool for implementation of proposed algorithm. Many research institutes also use MATLAB as research platform tool.

In technical computing MATLAB perform a vital role. It provides a integration of three environment as like computation, visualization, and programming. There many in built data types and functions that are very useful for developer and make it easy to perform. This also support object oriented programming. Due to these types of tools MATLAB is point of attraction for all researchers. We also choose the MATLAB tool as programing of our proposed work. MATLAB is short form of Matrix Laboratory. The following windows are common in starting of Matlab platform:

- *Desktop:* Desktop represents the basic windows and folders that are open and ready to use for user. Current folder, Command window, Workspace etc comes in desktop.
- *Figure Window:* when a programmer run the program then some outputs generated that are represented in figure window. The color of this window is gray and background is white.
- *Editor Window:* all files written and edited in this window which have extension .m.

VI. RESULT ANALYSIS

We create a GUI to make it user friendly. GUI attracts the all functions and features of model at a single platform. So we initial our project with GUI interface.



Welcome to an encryption model!!

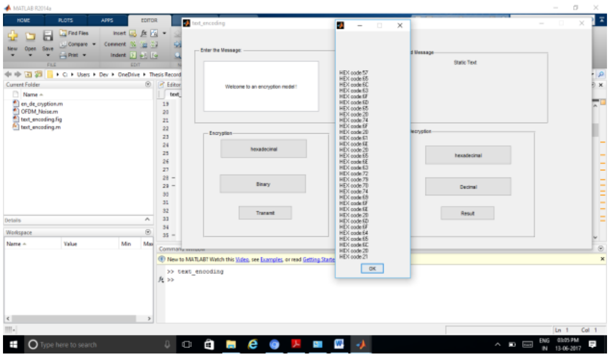
New to MATLAB? Watch this Video, see Examples, or read Getting Started.

```
      3

>> text_encoding
Edit Text
      0
```

Figure 3 GUI interface of model

Now we need a text message which want to encrypt. So we type text “Welcome to an encryption model!” in edit box shown in figure.



text_encoding

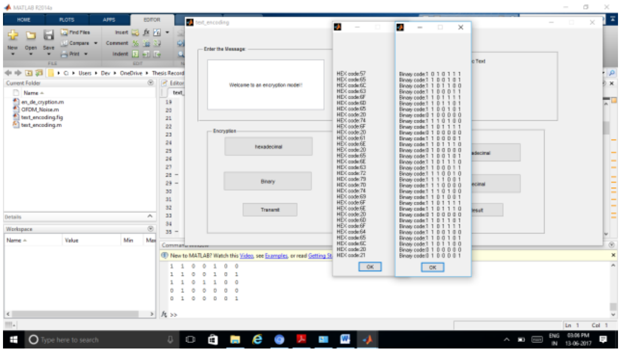
Enter the Message: Welcome to an encryption model!

```
HEX code:57
HEX code:65
HEX code:6C
HEX code:63
HEX code:6F
HEX code:6D
HEX code:65
HEX code:20
HEX code:74
HEX code:6F
HEX code:20
HEX code:61
HEX code:6E
HEX code:20
HEX code:65
HEX code:6E
HEX code:63
HEX code:72
HEX code:79
HEX code:70
HEX code:74
HEX code:69
HEX code:6F
HEX code:6E
HEX code:20
HEX code:6D
HEX code:6F
HEX code:64
HEX code:65
HEX code:6C
HEX code:20
HEX code:21
```

```
>> text_encoding
>>
```

Figure 4 Conversion in Hexadecimal process performed

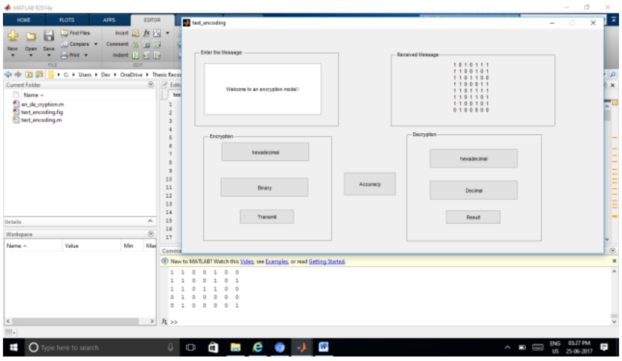
The output comes from this process is work as like input of proceeding step.



```
Binary code:1 0 1 0 1 1 1
Binary code:1 1 0 0 1 0 1
Binary code:1 1 0 1 1 0 0
Binary code:1 1 0 0 0 1 1
Binary code:1 1 0 1 1 1 1
Binary code:1 1 0 1 1 0 1
Binary code:1 1 0 0 1 0 1
Binary code:0 1 0 0 0 0 0
Binary code:1 1 1 0 1 0 0
Binary code:1 1 0 1 1 1 1
Binary code:0 1 0 0 0 0 0
Binary code:1 1 0 0 0 0 1
Binary code:1 1 0 1 1 1 0
Binary code:0 1 0 0 0 0 0
Binary code:1 1 0 0 1 0 1
Binary code:1 1 0 1 1 1 0
Binary code:1 1 0 0 0 1 1
Binary code:1 1 1 0 0 1 0
Binary code:1 1 1 1 0 0 1
Binary code:1 1 1 0 0 0 0
Binary code:1 1 1 0 1 0 0
Binary code:1 1 0 1 0 0 1
Binary code:1 1 0 1 1 1 1
Binary code:1 1 0 1 1 1 0
Binary code:0 1 0 0 0 0 0
Binary code:1 1 0 1 1 0 1
Binary code:1 1 0 1 1 1 1
Binary code:1 1 0 0 1 0 0
Binary code:1 1 0 0 1 0 1
Binary code:1 1 0 1 1 0 0
Binary code:0 1 0 0 0 0 0
Binary code:0 1 0 0 0 0 1
```

Figure 5 Conversion in binary form

In this step perform transmission process and the message got at receiving side is as following



text_encoding

Enter the Message: Welcome to an encryption model!

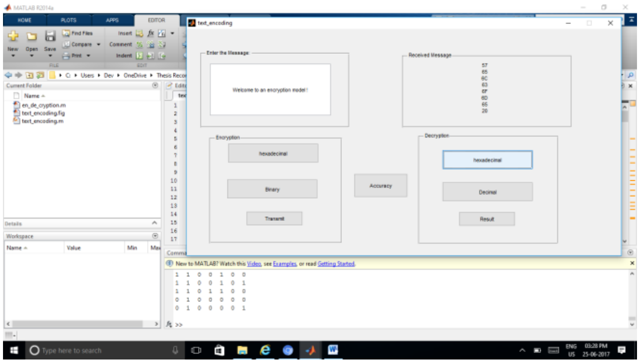
Received Message:

```
1 0 1 0 1 1 1
1 1 0 0 1 0 1
1 1 0 1 1 0 0
1 1 0 0 0 1 1
1 1 0 1 1 1 1
1 1 0 1 1 0 1
1 1 0 0 1 0 1
0 1 0 0 0 0 0
```

```
1   1   0   0   1   0   0
1   1   0   0   1   0   1
1   1   0   1   1   0   0
0   1   0   0   0   0   0
0   1   0   0   0   0   1
>>
```

Figure 6 Encrypted Message received at other side

Again decrypt message from binary to hexa-decimal form



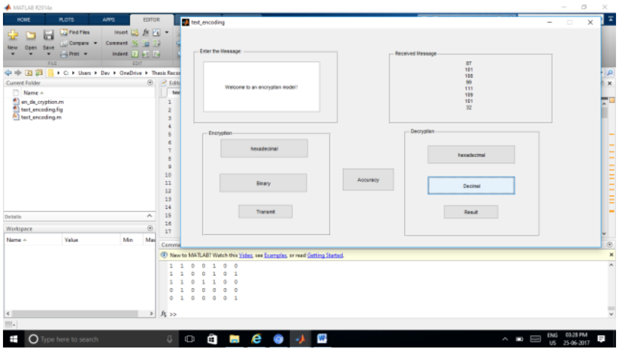
text_encoding

Enter the Message: Welcome to an encryption model!

Received Message:

```
57
65
6C
63
6F
6D
65
20
```

Figure 7 Binary to hexadecimal process



text_encoding

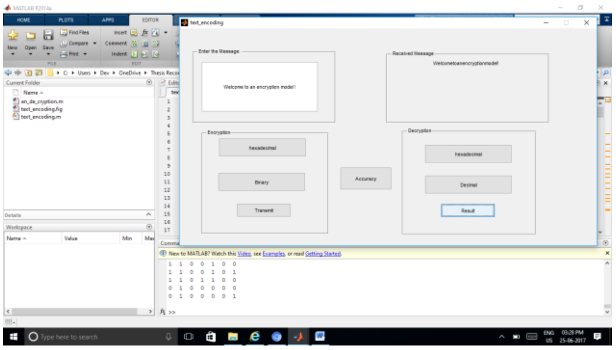
Enter the Message: Welcome to an encryption model!

Received Message:

```
87
101
108
99
111
109
101
32
```

Figure 8 Convert hexadecimal to decimal form

We get the text same as original on receiving side by using decryption process. Now we work to measure accuracy of this model.



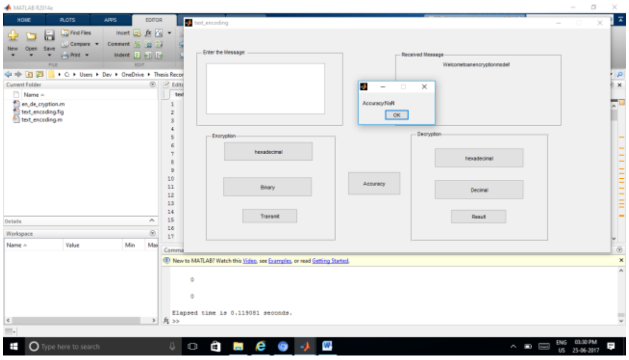
text_encoding

Enter the Message: Welcome to an encryption model!

Received Message: Welcometoanencryptionmodel!

Figure 9 After complete process check accuracy

Accuracy of this model varies as per entered text. If we put ‘enter the message’ box empty then accuracy is shown none and elapsed time is 0.119081 seconds.



Accuracy:NaN

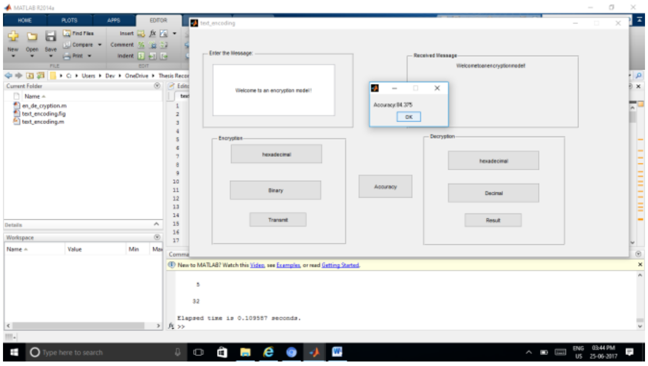
```
     0

     0

Elapsed time is 0.119081 seconds.
>>
```

Figure 10 accuracy for null text in edit box

Now we entered the text as like 'Welcome to an Encryption Model!' then we calculate accuracy and elapsed time of this model. Elapsed time is 0.109587 seconds.



Welcome to an encryption model!

Accuracy:84.375

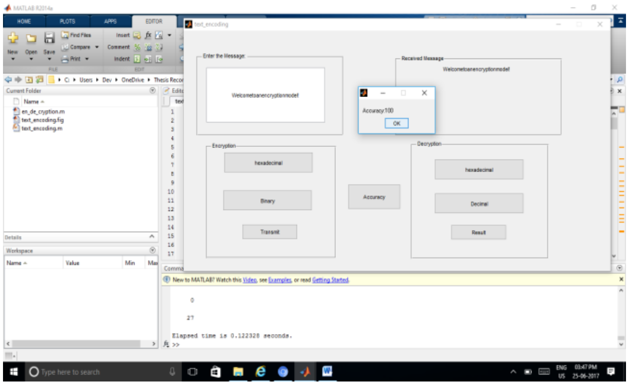
```
     5

    32

Elapsed time is 0.109587 seconds.
>>
```

Figure 11vaccuracy of text with space in edit box

At last we enter the text without space between words and calculate accuracy and time of this model. Elapsed time is 0.122328 seconds.



Welcometoanencryptionmodel!

Accuracy:100

```
     0

    27

Elapsed time is 0.122328 seconds.
>>
```

Figure 12 accuracy for text without space in edit box

Limitation of Encryption Model

As we performed the text encryption on this model, some issues created in it. First of we introduce the problem of handling space. This model is not compatible with space between words. It treats space as nothing for encryption and decryption. So the output displayed at decryption side all words combined and saw as a single word. Use of space is affecting the accuracy of model. As number of space increase in text the graph of accuracy goes in down.

VII. CONCLUSIONS

The internet usage and network system is growing rapidly. So there are some additional requirements to secure the data transmitted over different networks using different services. To afford the security to the network and data different encryption methods are used. In our research work we proposed a combined approach of Hexadecimal and binary technique. The encryption model becomes powerful but with a limitation that it do not consider space between words. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

REFERENCES

[1] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons Inc., 1996

[2] Tom St Denis, "Cryptography for Developers", Syngress Publishing, Inc., 2007

[3] Phil Zimmermann, "An introduction to cryptography", PGP Corporation, 2004

[4] W. Stallings, "Cryptography and Network Security: Principles and Practice", (5th Ed.), Prentice Hall, 2011.

[5] A. Menezes, P. Van Oorschot, S. Vanstone, "Handbook of applied cryptography", CRC Press, 1996

[6] National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook", NIST Special Publication 800–12, October 1995

[7] K. Barclay, J. Savage, "Object-Oriented Design with UML and Java", Elsevier, 2004

[8] Steven Gordon, "Key Management and Distribution", courses on Security and Cryptography", Sirindhorn International Institute of Technology, January 2011.