



A Secure Algorithm of Encryption and Decryption for Text Transmission

H M Tiwari¹, Vinay Kumar Patel²

¹Mathematics Department, Bhilai Institute of Technology, Raipur, INDIA

²Electronics & Telecommunication Department, Bhilai Institute of Technology, Raipur, INDIA

¹ toravi.tiwari@gmail.com; ² vinaypatel.elex@gmail.com

Abstract— Security of information plays a vital role in Data Communication through Internet. Data may exist in many forms like Text, Images, Audio, and Video etc. Definitely there is a need to protect the data from unauthorized access. Cryptography plays an important role to encode and decode the Information. This proposed algorithm offers a technique to encrypt the information in MATLAB using matrices and generates a password to decrypt the information. Since matrices have unique powerful concept, which can be easily understood and can be applied efficiently for encrypting and storing information. The proposed algorithm generates a key matrix which depends on rank of input matrix, is used for encryption and matrix addition is employed for encrypting the information. Within the same manner decryption is done at receiver end by subtracting by Key matrix, after entering the correct password only.

Keywords— Encryption, Decryption, Cipher, Decipher, MATLAB.

I. INTRODUCTION

Nowadays communication is a very important aspect in our daily life. Therefore security plays an important role in transferring the information. Cryptography is one of the most important methods to secure information. Cryptography is a technique which allow human-being to encrypt the data in such a way that the decryption can be performed without the aid of sender. There are several encryption and decryption algorithms available for encrypting the data at sender end and decrypting the same at receiver side ensuring secure data transformation. All have the same basics of cryptography shown in figure1. We have proposed a new algorithm for encryption and decryption of text message which is explained in section II.

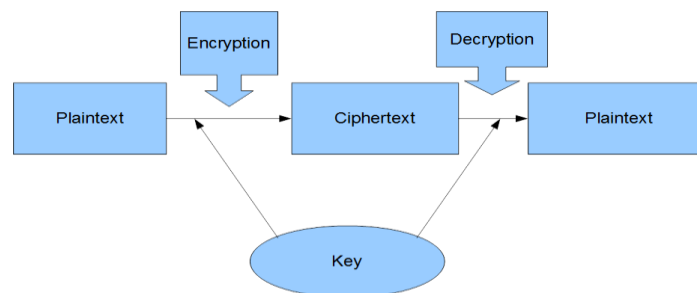


Fig.(1) Encryption & Decryption Process.

II. PROPOSED CRYPTOSYSTEM

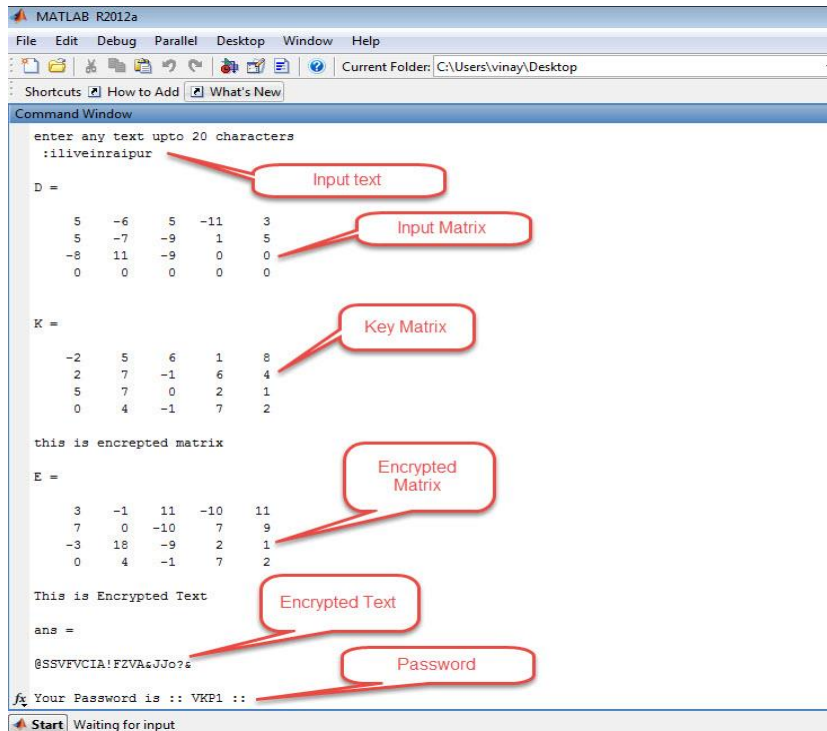
A. Algorithm for Encryption

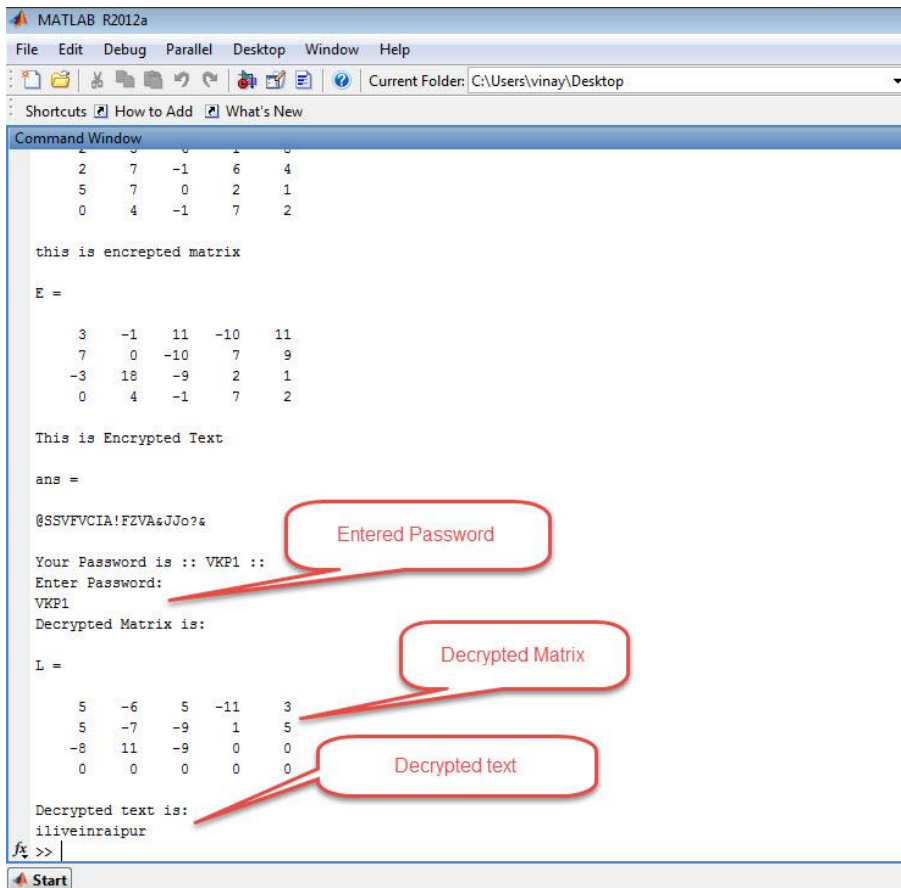
- i. Maximum number of character 20 (Case sensitive).
- ii. Define alphabets to numbers as:
 $a=1, b=-1, c=2, d=-2, e=3, f=-3, g=4, h=-4, i=5, j=-5, k=6, l=-6, m=7, n=-7, o=8, p=-8, q=9, r=-9, s=10, t=-10, u=11, v=-11, w=12, x=-12, y=13, z=-13.$
- iii. Input Text.
- iv. Decimal format for input text:
- v. All the characters will arranged in of 4×5 matrix say it D .
- vi. Find Rank R of D and use it to find Key matrix $K = \begin{pmatrix} 1-R & 2+R & 3+R & 4-R & 5+R \\ 5-R & 4+R & 2-R & 3+R & 1+R \\ 2+R & 1+2R & 3-R & 5-R & 4-R \\ 3-R & 1+R & 2-R & 4+R & 5-R \end{pmatrix}$ of 4×5 and also use Rank to generate password for decryption of text.
- vii. Add matrix D to Matrix K to find encrypted matrix E (i.e. $E=D+K$).
- viii. Numeric range of matrix input in E is -16 to 22 . Define different characters to each number.
- ix. Converting matrix input to text form we get encrypted text

B. Algorithm for Decryption

- i. Enter the password.
- ii. Find Matrix L by Subtracting key matrix K from E i.e. $L=E-K$. Compare with D we get input matrix D .

III. MATLAB IMPLEMENTATION





IV. CONCLUSION

The proposed algorithm presents a text encryption and decryption method based on simple matrix operations like addition and Subtraction. Experiment results show that the proposed encryption and decryption method is reasonably feasible and effective that can be extensively used for the purpose of secure data storage and transmission.

V. FUTURE WORK

In this paper length of text is limited to 20 characters but it can be extended to n characters by taking larger input matrix, and input matrix can be used as Key matrix so that its input numbers range is between -3 to 9 using mathematical operation. Also input numbers range can be extended by defining extra characters.

REFERENCES

- [1]. Saraswati Singh, Nilmani Verma, Vinay Kumar, "A Survey Report on Video Encryption and Decryption Techniques" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014, pg. 270-274.
- [2]. Saraswati Singh, Nilmani Verma, Vinay Kumar, "Efficient and Secure Video Encryption and Decryption using Neural Network", International Journal of Advanced Research in Computer Science, Volume 6, No. 1, Jan-Feb 2015, pg-37-42.
- [3]. Shipra Sahu, Jai Singh, Javed Ashraf, "Encryption and Decryption of Text data with RSA Cryptography using MATLAB", International Journal of Science and Engineering, Volume 3, Special Number ICRAESM – 2015, pg-104-110.
- [4]. Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. Dubey, "Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique ID", IJCSMC, Vol. 4, Issue. 8, August 2015, pg.66 – 71.
- [5]. Stephen J. Chapman, 'MATLAB Programming for Engineers'.
- [6]. Rudra Pratap, 'Getting Started with MATLAB', Oxford University Press.



H. M. Tiwari received M.Phil. Degree in Mathematics from D.A.V.V., Indore (M.P.), India in 2007. He is currently working as a HOD and Sr. Assistant Professor in Department of Mathematics at BIT Raipur, Chhattisgarh. His research interest includes Mathematical Modeling and simulation, Functional Analysis and Hypergeometric function etc.



Vinay Kumar received M.Tech. Degree in ECE from National Institute of Technology, Kurukshetra Haryana, India in 2009. He is currently working as a Sr. Assistant Professor in Department of Electronics and telecommunication at BIT Raipur. His research interest includes image enhancement, noise reduction, image segmentation, 3D visualization, communication and cryptography etc.