IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 64-71
www.iosrjournals.org

RDR Cube Cipher *an Extension to Vigenere Cipher*

Rahul Sourav Singh, Rupayan Das, Dipta Mukherjee, Prannay Bothra
Dept. of Computer Science & Engineering University of Engineering & Management, Jaipur, India

Abstract*: Vigenere Cipher is an encrypting method of alphabetic text using different Shift ciphers or additive based on letter of keywords [1]. It works on the set of 26 alphabets; however its scope is not just limited to English alphabets. Being an old method it's been vulnerable to many attacks. The proposed algorithm is to add a new dimension to this traditional method thus increasing its complexity and hence further reducing its vulnerability to different Vigenere Attacks. The keyword also called Encryption key used in Vigenere is used to select different table for encryption accordingly by the communicating parties using a modulus function. The more randomly the Table is varied based on the random selection of tables from a set of table virtually appearing like a cube more unpredictable the Encrypted text becomes hence increasing the complexity of the algorithm further. Different tables also reduces the variances of the characters hence making it more complex to analyze using the already existing Vigenere Analysis Algorithms.*
Keywords: *Vigenere Cipher, Cryptanalysts, Cryptography, Encryption, Encryption Key, Decryption.*

I. Introduction

Cryptology is a study of designing technique to encrypt messages using different algorithms and also regaining the original text using same or different algorithms. The normal messages also referred to as plain text is encoded based on some mathematical formula or algorithm to yield a coded message also called Cipher text. The algorithm used for performing the encryption is called Encryption Key. Again at the receiver end the Cipher Text is again processed or decrypted using the same or different algorithm to get the original text. Cryptanalysis is the study of designing system that will defeat such techniques to regain the message or forge the message. Together they came to be called as Cryptology. [1]With the dawn of computer and increasing dependency on it for communication also raised concerned about Information Security. Various security majors were introduced to ensure security of valuable information from being hacked or forged. Algorithms and methods were introduced to provide security at computer level, network level and internet level. Among various algorithm and techniques designed to provide Network Level and Internet Level Security Vigenere Cipher was one of them. However cryptanalyst designed techniques to defeat it.

In this paper, we propose an algorithm that will further improve the Vigenere Cipher Algorithm, making it less vulnerable to the attacks designed for it. The proposed algorithm focuses on the Encryption Key and the Vigenere Table. Unlike existing algorithm it is based on the elements of Encryption Key and introduces different 26 x 26 alphabet Table. This procedure is repeated number of times depending on the parameters selected by the communicating party. As a result the proposed algorithm makes the Encryption Key more complex and the Vigenere Table Formatting becomes dynamic resulting in an unpredictable encryption. The existing cryptanalysis algorithm designed for Vigenere Cipher algorithm are based on prediction of the letter based on the letter frequency calculated through different surveys. [1][2][3][4][5]

Rest of the paper is organized as follow. Section 2 describes the Vigenere Algorithm, the mathematical expression and the different attacks to break the cipher. Section 3 describes the proposed algorithm, its mathematical expression, block diagram. Section 4 describes the performance of the proposed algorithm and analysis of result. Conclusion is presented in Section 5.

II. Vigenere Cipher

Vigenere Cipher is a combination of several Shift Ciphers in a sequence with several shift values. [1][5] In shift ciphers each level is shifted by some value. If we shift letter D by 3 it becomes G. In Vigenere Cipher a sequence of such shift is organized in a table as shown in table 2.a. The table is called Tabula Recta or Vigenere Square or Vigenere Table. It's a 26 * 26 table where shift every row is equal to the number of the row.

Suppose a plaintext to be encrypted is:

MEET ME AT GROUND ZERO

And the keyword is "RELATION"; the keyword is repeated to match the length of the plaintext. To derive the Cipher text using the Vigenere table, for every letter in the plaintext, the intersection of row given by the keyword letter and the column given by the plaintext letter is chosen as Cipher text letter.

Keyword: RELAT IONSR ELATI ONR

Plaintext: MEETM EATGR OUNDZ ERO
Cipher text: DIPTF MOGXV ZUGLN RIS

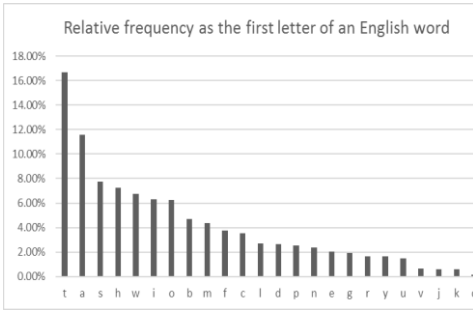

Figure 1

Decipherment of an encrypted message:

Keyword: RELAT IONSR ELATI ONR
Cipher text: DIPTF MOGXV ZUGLN RIS
Plaintext: MEETM EATGR OUNDZ ERO

Algebraic Description

In Vigenere Cipher the alphabets A to Z are considered as numbers 0 to 25, and addition operation is performed using modulo 26, then Vigenere encryption E using the key K can be written,

$C_i = E_k (M_i) = (M_i + K_i) \bmod 26$ (2.1a)

And decryption D using the key K,

$M_i = D_k (C_i) = (C_i – K_i) \bmod 26$ (2.1b)

Where $M = M_0M_1…..M_{n-1}M_n$ is the message,
$C = C_0 C_1…… C_{n-1}C_n$ is the Cipher text
And $K = K_0 K_1….. K_{m-1}K_m$ is the used key.

Cryptanalysis

There are many techniques developed to break a Vigenere Algorithm Encipherment. Different techniques are enlisted below:

Frequency Analysis:

Vigenere ciphers are very vulnerable to frequency analysis. Though it's a polyalphabetic cipher where by using matrix a one to many relations is created still after tracing frequency of a particular letter in a Cipher Text can help to detect which English alphabet it substitute. Frequency of English letters in a word had been calculated through various surveys. Here two bar charts chart 2.2.1a and chart 2.2.1b shows the relative frequency of each English alphabet in a text and the relative frequency of each English alphabet as the first character of a word respectively. [2][3][4][6][7] Comparing the Cipher text obtained from Vigenere Cipher Algorithm with the Frequency Chart enlisted here the original letters can be predicted.

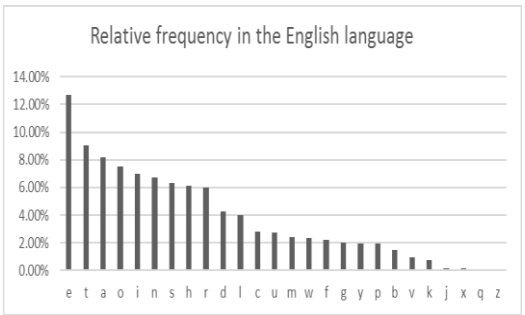

Figure 2

Kasiski Examination:

In Kasiski's method the distance between repeated bigrams are measured to find the length of the keyword. [8]

Friedman Test:
This test applies index of coincidence. It implies the unevenness of Cipher text Frequency to analyze the Cipher. The key length is calculated by using the mathematical expression:

$$\frac{K_p - K_r}{K_0 - K_r}$$

$$K_O = \frac{\sum_{i=1}^{c} n_i(n_i - 1)}{N(N-1)}$$

Where,
c is 26(for English alphabet)
N is equal to the length of the text
And N_1 to N_c are the Cipher text letter frequencies (integer)

III. Proposed Algorithm

3.1 Methodology:

The proposed methods employs a RDR (Rahul - Dipta - Rupayan) cube, Directory Table, Look-Up Table, Encryption Key and Plain Text. RDR cube have six different Vigenere Table like Tables of dimension 26 x 26 each having different orientation of alphabets. The users have the liberty to choose their own orientation of elements for tables present in each face of the RDR Cube but it has to be same per Encryption. Each face of the RDR cube is numbered from 0 to 5. Directory Table is a Table of size 26 containing English alphabets at different position. No repetition of alphabets are allowed. Users have the freedom to choose the position at which they want to store an alphabet but for a given Encryption – Decryption it has to be same. Look-Up Table containing English alphabets. No repetition of alphabets are allowed.

Each character of Encryption Key is searched in the directory and the position of the alphabet in the Directory Table is taken as its integer representation. Further modulo 6 operation is performed over the integer representation of selected Key character and the result of the operation is used to select the face of the RDR cube for it. The table in the selected face of the RDR Cube is used to encrypt the corresponding Plaint Text character in accordance with the selected character of the Key. This process is repeated for the encryption of each character present in the Plain Text.

For Decryption similar mechanism is followed. For each character of Encryption Key a face of RDR cube is selected based on modulo 6 operation over the integer representation of selected character of the Key. He table present in the selected face of the RDR Cube is used to decrypt the Cipher Text character corresponding to the selected Encryption Key character.

3.2 Implementation:

Data Structure:

- **A. RDR Cube:** 6 x 2D Matrices, each representing each side of the Virtual Cube represented by a 3D Array of dimensions [6 x 26 x 26]. Only two of the six matrices are included in the paper.
- **B. Look Up Table:** 2 x 1D used for mapping Plaintext and Key represented a matrix each.
- **C. Directory:** 1D Table of size 26 containing alphabets at different cell index matching the integer representation of each English alphabet selected by the user for the following encryption process.

Matrices:

Matrix 1

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

Matrix 2

Matrix 2:

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

3.2.1 Block Diagram:

Block diagrams of our proposed algorithm for encryption and decryption are given below

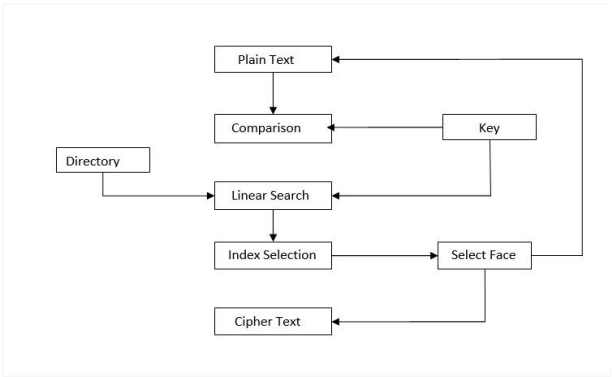

Fig 3.2.1 (A). Encryption Block

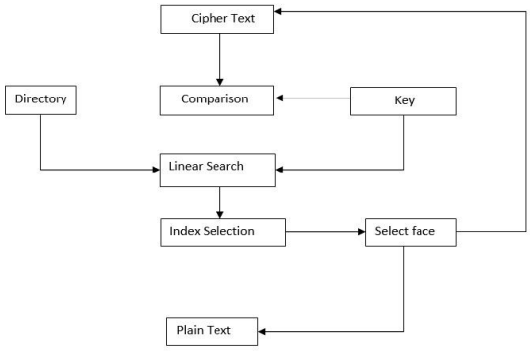

Fig 3.2.1 (B). Decryption Block

3.3 Mathematical Representation:

$D =$ Directory Table

$D = [A, B, C, D, E, F, G, H....Z]$

$\psi =$ Position of K_i in D

$n_i = (\psi) \bmod 6$

$F_{RDR} =$ RDR Cube Consists of Six faces

$f_i =$ It represents one face of a RDR cube at a time

$j =$ It is an integer number locates the current face of RDR cube

$J =$ Set of face pointers

$\delta =$ Key Length

$p =$ Plain Text

$cp =$ Cipher Text

$E(p) =$ Encryption Function

$D(cp) =$ Decryption Function

$\sigma_{face=n_i}(F_{RDR}) =$ Selecting the faces from F_{RDR}

$$if\ (\sum_{i=0}^{\delta} k_i \varepsilon D)$$

Now $\{\psi =$ Position of K_i in $D\}$

$$F = \coprod_{(j \varepsilon J)} f_i$$

Now where f_i is the co product of F

So the formula to encrypt the plain text is:

$$cp = E(p) = \{p,\ k_i,\ \sigma_{face=n_i}(F_{RDR})\}$$

So the formula to decrypt the Cipher text is:

$$p = D(cp) = \{cp, k_i, \sigma_{face=n_i}(F_{RDR})\}$$

IV. Result and Analysis:

A. Encryption using the proposed algorithm

Plain text "I WANDERED LONELY AS A CLOUD THAT FLOATS ON HIGH OVER VALES AND HILLS WHEN ALL AT ONCE I SAW A CROWD A HOST OF GOLDEN DAFFODILS" and a User defined

Key "RELATION" to prove our algorithm. The alphabet positions are taken according to their occurrence in English alphabet list.

Plain Text: IWAND EREDL ONELY ASACL OUDTH ATFLO ATSON HIGHO VERVA LESAN DHILL SWHEN ALLAT ONCEI SAWAC ROWDA HOSTO FGOLD ENDAF FODIL S

Key: RELATION

R	E	L	A	T	I	O	N

Numerical representation:

18	5	12	1	20	9	15	14

Modulo of 6:

0	5	0	1	2	3	3	2

Different face of the RDR cube calculated by modulo 6 of integer values for each character of key is selected for each character of the Encryption Key. Use the selected face to implement the Encryption using the table represented in that face of the cube. Performing the mentioned procedure for each character of the Plain Text we get:

Cipher Text: ZYLRF ATAUN ZRGHA WJCNP QQFPY CEJNK CPJQY LKCJK MGCZC HGORP OLKHN ONJNR CHNWK QYGGE UWNCN TQSFW YQDXQ BIKCF NRFWH BEFTP U

B. Encryption using Vigenere Cipher [1]

Plain Text: IWAND EREDL ONELY ASACL OUDTH ATFLO ATSON HIGHO VERVA LESAN DHILL SWHEN ALLAT ONCEI SAWAC ROWDA HOSTO FGOLD ENDAF FODIL S
Key: RELATION

Cipher Text: ZALNW MFRUP ZNXTM NJENL HCRGY EEFEW OGJSY HBOVB MICVT TSFRR OHBTZ FNLPN TTZNK SYCXQ GNNEN RHERN YSDTH NUBCH PNWIT SFHTL L

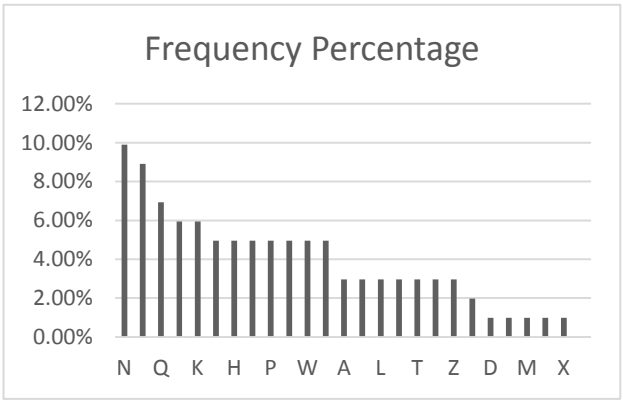

Fig 3.3 (A). Frequency Graph of Encryption using Proposed Algorithm

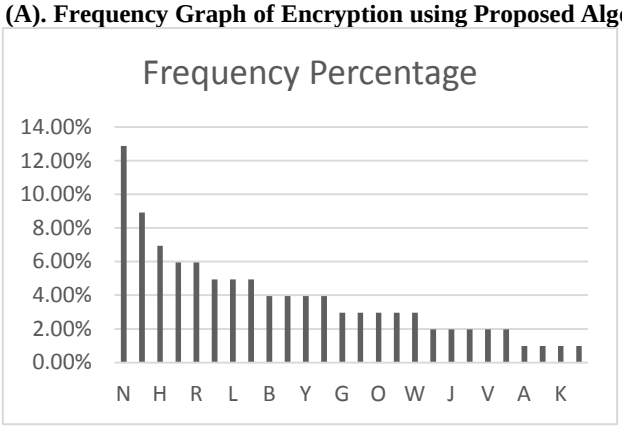

Fig 3.3 (B). Frequency Graph of Encryption using Vigenere Cipher

C. Decryption of Cipher Text generated by the proposed algorithm

Cipher text "ZYLRF ATAUN ZRGHA WJCNP QQFPY CEJNK CPJQY LKCJK MGCZC HGORP OLKHN ONJNR CHNWK QYGGE UWNCN TQSFW YQDXQ BIKCF NRFWH BEFTP U" and a User Defined Key "RELATION" to prove our algorithm.

Cipher Text: ZYLRF ATAUN ZRGHA WJCNP QQFPY CEJNK CPJQY LKCJK MGCZC HGORP OLKHN ONJNR CHNWK QYGGE UWNCN TQSFW YQDXQ BIKCF NRFWH BEFTP U

Key: RELATION

R E L A T I O N

Numerical representation:

18 5 12 1 20 9 15 14

Modulo of 6:

0 5 0 1 2 3 3 2

Now we need to select the different face of the cube calculated by modulo 6 of integer values for each character of key. Use the selected face to implement the Encryption using the table represented in that face of the cube. Performing the mention the procedure and by performing Vigenere Cipher we get respectively:

Plain Text Generated by Proposed Algorithm: IWAND EREDL ONELY ASACL OUDTH ATFLO ATSON HIGHO VERVA LESAN DHILL SWHEN ALLAT ONCEI SAWAC ROWDA HOSTO FGOLD ENDAF FODIL S

Plain Text Generated by Vigenere Cipher: IUARM SFNDJ ORNZM JSYCP XIRCH YTJUC OCSMN LRUVX VCRZJ ZSBAL DLRZZ BWFCR JZZJT MNGNW GJWYC TXKRJ HMSXX TUXLB CRMOT ONBIP B

Table 1:

Cryptanalysis	***Vigenere cipher***	***Proposed algorithm***
Index of Coincidence	*0.047*	*0.044*
Max probability of occurrence	*0.128*	*0.099*
Min probability of occurrence	*0.009*	*0.009*
Average probability of occurrence	*0.068*	*0.054*
Keyword Length	*1*	*1*
Variance	*0.005*	*0.002*
Standard Deviation	*0.068*	*0.054*

V. Conclusion

There is a 60% decrease in variance in the proposed algorithm compared to classical Vigenere Cipher. Inclusion of 6 different matrices for the calculation of cipher text have made the algorithm dynamic and also increased its complexity. We have tried the normal attacks meant for Vigenere cipher to decipher our algorithm. These algorithms failed to analyze the cipher text generated by our proposed algorithm. Also the contents of the matrices can be varied randomly and so the mod function meant to choose the matrices. Thus the complexity can further be enhanced.

References

[1] William Stallings: "Cryptography and Network Security: Principles and Practices 4th Edition, Prentice Hall"
[2] "What is the frequency of the letters of the alphabet in English?" Oxford Dictionary. Oxford University Press. Retrieved 29 December 2012.
[3] Mička, Pavel. "Letter frequency (English)". Algoritmy.net.
[4] Statistical Distributions of English Text
[5] Dara Kirschenbaum:"Advances in Cryptography History of Mathematics" Beker, Henry; Piper, Fred

[6] (1982) Cipher Systems: The Protection of Communications. Wiley-Interscience. p. 397. Table also available from Lewand, Robert (2000). Cryptological Mathematics. The Mathematical Association of America. p. 36. ISBN 978-0-88385-719-9.
[7] Calculated from "Project Gutenberg Selections" available from the NLTK Corpora
[8] Kasiski, F. W. 1863. Die Geheimschriften und die Dechiffrir-Kunst. Berlin: E. S. Mittler und Sohn
[9] Henk C.A. van Tilborg, ed. (2005). Encyclopaedia of Cryptography and Security (First Ed.). Springer. p. 115. ISBN 0-387-23473-X.
[10] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4
[11] Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. ISBN 978-0-19-162588-6.
[12] Smith, Laurence D. (1943). "Substitution Ciphers". Cryptography the Science of Secret Writing: The Science of Secret Writing. Dover Publications. p. 81. ISBN 0-486-20247-X.
[13] Knudsen, Lars R. (1998). "Block Ciphers— a survey". In Bart Preneel and Vincent Rijmen. State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptograph Leuven Belgium, June 1997 Revised Lectures. Berlin; London: Springer. p. 29. ISBN 3-540-65474-7.
[14] Singh, Simon (1999). "Chapter 2: Le Chiffre Indéchiffrable". The Code Book. Anchor Books, Random House. pp. 63–78. ISBN 0-385-49532-3.
[15] David, Kahn (1999). "Crises of the Union". The Codebreakers: The Story of Secret Writing. Simon & Schuster. pp. 217–221. ISBN 0-684-83130-9

Rahul Sourav Singh received his Bachelor in Technology from Rajiv Gandhi Technical University, Madhya Pradesh and Master in Technology degree in Computer Science & Engineering from West Bengal University of Technology, West Bengal. He has worked as an Assistant Professor at Institute of Engineering & Management Kolkata. Now, he is working as an Assistant Professor at University of Engineering and Management, Jaipur, India. Area of interest are Network Security, Cloud Computing, Image Processing, Neural Networks, Artificial Intelligence, Compiler, Theory of Computation, Natural Language Processing and Computer Architecture.

Rupayan Das: Assistant Professor at University of Engineering & Management (UEM), Jaipur. Has achieved Bachelor in Technology in Information Technology and Masters in Technology in Information Technology from West Bengal University of Technology and has worked as a teaching assistant at Institute of Engineering & Management (IEM).Interested in Network Security, Cloud Computing, and Image Processing.

Dipta Mukherjee received his Bachelor in Technology and Master in Technology degree in Computer Science & Engineering from Kalyani University, West Bengal. He has worked as an Assistant Professor at Institute of Engineering & Management Kolkata. Now, he is working as an Assistant Professor at University of Engineering and Management, Jaipur, India.

Prannay Bothra: Graduate student of Computer Science & Engineering, University of Engineering & Management, Jaipur