Nepalese Journal of Management Research
ISSN 2738-9618 (Print), ISSN 2738 -9626 (Online) **Website:** http://balkumaricollege.edu.np/journal
Volume : 4 **January 2024, Page No. 11-15**

Enhancing Security for Text Message Cryptography based on Basis Vectors

Ramesh Khanal
Teaching faculty of Applied Mathematics
Balkumari College
Email: khanalrk@outlook.com

ABSTRACT

Cryptography is the practice and study of hiding information from all but those with the means or key to decode the message. Also the area of cryptography employs many different means of transforming normal data in to unreadable form. This paper's aim of the study was how to keep the digital data secretly and sent it secretly through insecure channels based on basis vectors, that an activity builds around one of the techniques that illustrate an application of a set of basis vectors called matrix to cryptography The method involves two matrices of which one is used to encode the encoding matrix and the other one to decode the decoding matrix. The characters, in the original message or stream are assigned numerical values and the matrix must be row reduce echelon form for use in decoding. The proposed method is very simple in its principle and has great potential to be applied to other situations where the exchange of message is done confidentially.

Keywords: Cryptography, Matrix mapping, Row reduce echelon form, basis vectors.

Introduction

Cryptography (Rivest, 1991) was one such way of transferring the data in a secure way, a single key is for both encryption and decryption purposes. The sharing of this key becomes insecure sometimes. With the development of human intelligence, the art of cryptography has become more complex in order to make information more secure. Number theory (Koblitz, Some Topics in Elementary Number Theory, 2008), as discussed in Koblenz's work "Some Topics in Elementary Number Theory" from 2008, has implications in coding theory, particularly in the implementation and analysis of public-key cryptosystems. The Nepal Telecommunications Authority noted a surge in criminal activities, including cyber-attacks, due to the rapid expansion of information and communication technology. To mitigate these risks, new legislation includes provisions that mandate adherence by service providers. Despite Nepal's emphasis on security and privacy, there have been frequent media and police reports on cybersecurity breaches. Nepal faces a precarious and challenging IT landscape, and despite its respect for security and privacy, the existing cybersecurity policies have yet to effectively address the escalating concerns regarding cyber breaches among users (Subedi, 2019).

Therefore, this paper's aim of the study was how to keep the digital data secretly and sent it secretly through insecure channels based on basis vectors that an activity builds around one of the techniques that illustrate an application of a set of basis vectors called matrix to cryptography. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference that need to insure that this information is invulnerable to snoop, but denies the intelligible content to a would-be interceptor. For digital data exchange, an encryption scheme usually provides a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without controlling the key. A well-designed encryption technique, considerable computational resources and skills are required. An endorsed recipient can easily decrypt the message with the key provided by the creator to recipients but not to unauthorized users. Decryption is the method of encoded or encrypted text or other data and converting it back into plaintext that the computer can read and recognize. It may be accomplished manually or automatically and may also be performed with a set of keys or passwords.

Methodology

The text message of length one can be converted into a stream of numerals using an accessible scheme for both the sender and the receiver as below

Table no 1 represents the characters into numbers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	?	*	.	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

And # as 30. Consider the plain text massage P in coded matrix form of 3Further consider the basis of three dimension column vectors K= [a1 a2 a3] as key whose determinant is coprime to number of 31 codes. Multiply this message matrix P to the key basis matrix K of size 3 and get the encoded matrix C = KP (mod31) of size 3, m≥1. The message matrix C can be converted into the stream of numbers and convert this stream of numerals in to the text of the cypher text message, that contains the encrypted message and sent to the receiver. For decryption process. The encrypted message into a matrix can be placed by the encrypted stream of numbers. The augmented matrix [K: C] (mod31) can be change into row reduce Echelon form (RREF) (Joseph F., 2011) to get back the number matrix P. The matrix P can be converted into a stream of numbers with the help of the originally used method. Convert this stream of numerals in to the text of the original message. Data were computed by MatLab 2014b software. The procedure as follows

```
K= [1 3 2; 2 1 3; 3 2 1];                          % Basis vector as key
P= [13 00 22 28; 14 13 04 29; 29 18 17 19];     % Numerical plain text
C=K*P;                                       % Encrypted by key vector
C1=mod(C, 31)                                % Cypher text in numerical form
A= [K C1]                                    % Augmented data to be decryption
A(2,:)=A(2,:)-A(2,1)/A(1,1)*A(1,:); % Change second row by  pivot element.
A(3,:)=A(3,:)-A(3,1)/A(1,1)*A(1,:); % Change third row by  pivot element
A (2, :) =6*A (2, :);               %Multiplicative inverse of -5(mod31),6
A1=mod (A, 31);
A1(1,:)=A1(1,:)-A1(1,2)/A1(2,2)*A1(2,:);%Change first row by  pivot element
A1(3,:)=A1(3,:)-A1(3,2)/A1(2,2)*A1(2,:);% Change third row by  pivot element
A2=mod (A1, 31);
A2 (3, :) =29*A2 (3, :);      %% Multiplicative inverse of 15(mod31), 29
A2 (3, :) =mod (A2 (3,:),31);
A2(1,:)=A2(1,:)-A2(1,3)/A2(3,3)*A2(3,:);% Change first row by  pivot element
A2(2,:)=A2(2,:)-A2(2,3)/A2(3,3)*A2(3,:)% Change second row by  pivot element
A3=mod (A2, 31) % standard rref
```

we got P= [131429001318220417182]. The data set is rearranged in matrix size of 3×m, m≥1, and added numerical space value 29 if necessary in standard form of matrix multiplication. Thus the data set was P $=\begin{bmatrix} 13 & 0022 & 28 \\ 14 & 1304 & 29 \\ 29 & 1817 & 29 \end{bmatrix}$. Now data P was encrypted by key K. The cypher text was

C= [K*P] mod31 = $\begin{bmatrix} 113 & 7568 & 153 \\ 127 & 6799 & 142 \\ 96 & 4491 & 161 \end{bmatrix}$ mod 31= $\begin{bmatrix} 20 & 1306 & 29 \\ 03 & 0506 & 08 \\ 03 & 1329 & 06 \end{bmatrix}$ =

[200303130513060629290806]. Finally, the encrypted data was= [UDDNFNGG IG]. Moreover for decryption process by the same key K, the plaintext obtain by P=RREF [K, C] mod 31=

RREF $\begin{bmatrix} 1 & 3 & 220 & 1306 & 29 \\ 2 & 1 & 303 & 0506 & 08 \\ 3 & 2 & 103 & 1329 & 06 \end{bmatrix}$ mod 31 = $\begin{bmatrix} 1 & 0 & 0{-}576 & -341{-}319 & -375 \\ 0 & 1 & 0{-}699 & -421{-}399 & -467 \\ 0 & 0 & 1\ \ 29 & 18\quad 17 & 19 \end{bmatrix}$ mod 31=

$\begin{bmatrix} 1 & 0 & 013 & 0022 & 28 \\ 0 & 1 & 014 & 1304 & 29 \\ 0 & 0 & 129 & 1817 & 19 \end{bmatrix}$ = [131429001318220417282929] = NO ANSWER. Hence the encryption and decryption process is verified between sender and receiver by key as basis vector.

The above same plaintext data was also encrypted by 2×2 matrix K= $\begin{bmatrix} 02 & 03 \\ 07 & 08 \end{bmatrix}$ and decrypted by its inverse K^{-1} = $\begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix}$(Koblitz, Cryptography, 2008). Here the encryption procedure was same but cypher text was different due to key size.Decryption procedure was different by row reduce echelon form (RREF). In this paper, the data were calculated by MatLab 2014b and previous were manually.

Now, let us consider the encrypted data (message) by the same key matrix K is given byC=[R?N DIS R?N TTY TKP **.ZVX DKZDAL ERN MT. XA EA DY?*JQSLPFIH SMI #K#LE CBRSEEVRTEADXRMOTXFOYWYQRSIRB SRQ].This data in coded numerical form is[172613030818172613191924191015272728252123031025030011041713121928292300040029032426270916181115050807191208293029103011042929020117180404211719040003231712141923051424222416171808170229181716]. It is equivalent in standard matrix form is

$$C = \begin{bmatrix} 17 & 03 & 1719 & 19 & 22\ 25 & 03 & 0304 & 12 & 29\ 04\ 03 & 27 & 18 \\ 26 & 08 & 2619 & 10 & 2721 & 10 & 0017 & 19 & 23\ 00\ 24 & 09 & 11 \\ 13 & 18 & 1324 & 15 & 28\ 23 & 25 & 1113 & 28 & 00\ 29\ 26 & 16 & 15 \end{bmatrix}$$

$$\begin{bmatrix} 05 & 19 & 2910 & 04 & 02\ 18 & 21 & 0423 & 14 & 0522 & 17 & 1718 \\ 08 & 12 & 3030 & 29 & 01\ 04 & 17 & 0017 & 19 & 1424 & 18 & 0217 \\ 07 & 08 & 2911 & 29 & 17\ 04 & 19 & 0312 & 23 & 2416 & 08 & 2916 \end{bmatrix}$$

This encrypted message is decrypted with the help key K by changing RREF of [K: C]. The RREF matrix [K: C] is = $\begin{bmatrix} 1 & 0 & 0\ 19 & 29 & 1912 & 08 & 2929 & 06 & 00\ 29 & 00 & 07 \\ 0 & 1 & 0\ 07 & 12 & 0700 & 02 & 0800 & 17 & 19\ 01 & 13 & 29 \\ 0 & 0 & 1\ 04 & 00 & 0419 & 18 & 1829 & 04 & 04\ 17 & 02 & 14 \end{bmatrix}$

$$\begin{bmatrix} 05 & 02 & 1329 & 19 & 1429 & 29 & 2913 & 14 & 1819 & 13 & 1307 & 29 & 0817 & 28 \\ 29 & 08 & 0222 & 07 & 2008 & 22 & 0229 & 13 & 2000 & 29 & 2908 & 20 & 2118 & 29 \\ 18 & 04 & 0408 & 29 & 1919 & 04 & 0013 & 29 & 1808 & 08 & 1918 & 13 & 0404 & 29 \end{bmatrix}$$

Hence the original coded numerical message sent is P= [190704291200190704120019080218290818290029061704001904290117001302072914052918020804130204292208190729142019290819 292204 290200 132913 141329 182018 190008 132908 192919 070818 292013 082104 171804282929]. Finally original message is "**The Mathematics is a greatbranch of science without it we cannot sustain in this universe.**"

The matrix can use as the key for short or long text encrypted and the decrypted text retrieved by its inverse matrix for any change that convert integer numbers to letters (Mathivadhana & Sivasankari, 2018) (Prabhavathi & Chandrapushpam, 2018). But in this study the decrypted text retrieved the plain text by row reduce echelon form

Conclusion

This paper provides the methods of sending messages secretly. As both encryption and decryption methods are using mathematical techniques matrix multiplication and congruence modulo. They are considered to be best methods to decrypt the encoded message by the key matrix known as basis vector and congruence modulo must be known between the sender and the receiver, the sending messages can be kept secretly from others.

REFERENCE

Koblitz, N. (2008). Cryptography. In *A Course in Number Theory and Cryptography* (pp. 71-72). Springer.

Koblitz, N. (2008). *Some Topics in Elementary Number Theory.* Springer.

Mathivadhana, E., & Sivasankari, K. (2018). A Comparative Study of Matrix Encoding and Hill Cipher Algorithm. *International Journal of Scientific Research in Science and Technology, 4*(5), 813-816. Retrieved from https://www.academia.edu/36292090/A_Comparative_Study_of_Matrix_Encoding_and_Hill_Cipher_Algorithm?from=cover_page

Prabhavathi, S., & Chandrapushpam, T. (2018). Role of Matrix in Cryptography. *International Journal of Mathematics and Its Application, 6*(1), 25-28. Retrieved from http://www.ijmaa.in/v6n1-s/25-28.pdf

Rivest, R. L. (1991). Crypography. In *A Handbook of Theoretical Computer Science.* Elsevier.

SSubedi, R. H. (2019). *Cyber Security Situation in Nepal.* Retrieved from https://npcert.org/gcss2018/cyber-security-situation-in-nepal-dr-ramhari-subedi/

Zhang, W., & Zhi-liang, Z. (2015). An image encryption based on three-dimensional bit matrix permutation., *118*, pp. 36-50. Retrieved from https://sci-hub.scihubtw.tw/10.1016/j.sigpro.2015.06.008