*CPUH-Research Journal:* **2017,** ***2(2),*** 41-44
***ISSN (Online): 2455-6076***
***http://www.cpuh.in/academics/academic_journals.php***

# A Secure Cryptosystem Based on Normal Bases over Finite Fields

**P.L. Sharma* & Kiran Devi**

*Department of Mathematics and Statistics, Himachal Pradesh University, Shimla 171005, INDIA*
*E-mail: plsharma1964@gmail.com*

**ABSTRACT: Cryptography provides the security to the messages which travel over the insecure channels. Normal bases are widely used in various cryptographic functions and ciphers to provide the confidentiality, integrity and security to the messages. We propose a secure cryptosystem using Hill cipher and normal bases over finite fields.**

**Keywords:** Normal basis; trace mapping; normal element; finite field; hill cipher.

**INTRODUCTION:** The secure communication of text information is of prime importance. Cryptography helps to protect data which travels through the internet and intranet. Various branches of mathematics like matrix analysis, number theory, finite fields, and logical operators are used to form the cryptosystems, see [5-8, 10, 14, 15, 17] help to provide security in emails, ATM machines, cellular phones, e- commerce, digital signatures and online transactions in banking sectors.

Hill cipher is a block cipher algorithm in which plain-text is divided into equal size of blocks. It is based on matrix transformation which gives symmetric cipher. Hill cipher is invented by Lester S. Hill in 1929 [4]. Various cryptosystem based on Hill cipher and matrices are helpful in providing frequency analysis, high speed and simplicity. In cryptosystem based on Hill cipher decryption is possible if the key matrix is invertible. Hill cipher is secured by the dynamic key matrix obtained by random permutations of columns and rows of the master key matrix [9]. The modification in previous Hill cipher is done by Chefranov [1]. Hill cipher is further improved using pseudo random permutation generator [10]. Affine and matrix transformation gives more secure cryptosystem by increasing the security of Hill cipher [16, 18, 20].

Many researchers have contributed to improve the security of Hill cipher using different techniques. Sharma et al. [11-13] used finite field and logical operator to make the cipher more secure. Normal bases are used in squaring and multiplication of an element in finite field which can be easily done by a cyclic bit shift of binary digits [2, 16]. Due to fast exponentiation and cyclic bit shift operations normal bases are used at large scale. We proposed a cryptosystem by improving the security of Hill cipher and it contain mainly generation of secret key, encryption and decryption process by using normal bases over finite fields and triangular matrix.

**Normal basis:** Let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$. Then the basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{n-1}}\}$, consisting of suitable element $\alpha \in \mathbb{F}_{q^n}$ and its conjugates with respect to $\mathbb{F}_q$ is called the normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

**Normal element:** An element $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is called the normal element if the polynomials $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \ldots + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime.

**Trace mapping:** The mapping from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is called trace mapping if

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}},$$

where $\alpha \in \mathbb{F}_{q^n}$.

**PROPOSED ALGORITHM:** This algorithm involves the two different keys. One key is obtained by using normal elements in trace mapping and other is obtained by using the triangular matrix.

**Encryption**

(i) First consider the text message that we have to encrypt. Find the total length of data in text message.

(ii) Take the normal basis set of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ where $n$ is equal to the length of text message.

(iii) First consider the matrix $U$ of size $n \times n$ from the trace mapping of normal elements such that $|U| \neq 0$.

(iv) Let $u_i = Tr(\alpha^{2^{2i}-2^i+1})$, be the trace mapping, where $\alpha$ is the normal element. Further, find the coefficients of the set $U = u_0, u_1, u_2, \ldots, u_{n-1}$ where $n$ is equal to the order of key matrix $U$.

(v) Form the circulant matrix of the set $U$ and denote it by $U_c = circ(u_0, u_1, u_2, \dots, u_{n-1})$ and keep this as a secret key.

(vi) Consider upper triangular matrix as another key matrix which is non-singular matrix and is used as public key.

(vii) Further calculate the key

$$K = TUT^{-1} mod(2^n - 1).$$

(viii) Take $P$ as a plaintext of size $n$, $C$ as a cipher text and find $C = KP + U_{c_1}^t \ mod(2^n - 1)$ , where $U_{c_1}^t$ is the transpose of first row of secret key matrix $U$.

(ix) After reducing the value of column matrix $C$ with $mod(2^n - 1)$, sender converts reduced numerical values into text to get the final cipher text.

**Decryption**

Secret key is used in decryption process to find the original cipher text.

(i) The receiver receives the message and changes it into numerical values.

(ii) Further receiver calculates

$$K^{-1} = TU^{-1}T^{-1} mod(2^n - 1).$$

(iii) Then he finds the value

$$P = K^{-1}\left(C - U_{c_1}^t\right) mod(2^n - 1).$$

(iv) After that receiver converts the entries of $P$ in text using Table (a) to get the plaintext. Let the letters of the alphabets and some more symbols be associated with integers as given in Table 1.

**Table 1: Numerical values for alphabets and some symbols used in the paper**

| @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ! | # |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

**ILLUSTRATION OF THE ALGORITHM**

Let us illustrate the algorithm with the help of following example:

**Encryption**

(i) Let '**INDIA**' is the word that travels through the insecure channel and length of the plain text is five.

(ii) The values of $u_i$ , $i = 0,1,...,4$ in set $U = \{u_0, u_1, u_2, u_3, u_4\}$ are equal to $\{1,0,1,1,0\}$ after using the trace mapping $u_i = Tr(\alpha^{2^{2i}-2^i+1})$, where $0 \le i \le 4$ and normal element $\alpha^2 + 1$ is taken in place of $\alpha$ from elements of $F_{2^5}$ over $F_2$.

(iii) Now, the sender form the circulant matrix by using the elements of the set $U$ as below

$$U_c = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

and keep that secret.

(iv) Consider the $5 \times 5$ non-singular upper triangular matrix

$$T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which is used as a public key.

(v) Further he calculates the key

$$K = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} mod(31)$$

$$= \begin{bmatrix} 3 & 1 & 29 & 1 & 2 \\ 1 & 2 & 30 & 1 & 2 \\ 2 & 2 & 29 & 1 & 2 \\ 1 & 1 & 29 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

(vi) Then senders form the plaintext as given below for the encrypted message alphabets from the Table 1.

$$P = \begin{bmatrix} 9 \\ 14 \\ 4 \\ 9 \\ 1 \end{bmatrix}$$

(vii) Now, senders calculates the cipher text

$$C = \begin{bmatrix} 3 & 1 & 29 & 1 & 2 \\ 1 & 2 & 30 & 1 & 2 \\ 2 & 2 & 29 & 1 & 2 \\ 1 & 1 & 29 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 9 \\ 14 \\ 4 \\ 9 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} mod\ (31)$$

$$= \begin{bmatrix} 45 \\ 44 \\ 50 \\ 35 \\ 14 \end{bmatrix} mod\ 31 = \begin{bmatrix} 14 \\ 13 \\ 19 \\ 4 \\ 14 \end{bmatrix}.$$

(vii) Then numerical values are converted into text using the Table (a). So the cipher text is NMSDN.

**Decryption**

(i) The receiver receives the message and converts the message in numerical values using Table 1.

(ii) After this he finds the value of

$$K^{-1} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{-1}{3} & \frac{-1}{3} & \frac{2}{3} & \frac{2}{3} & \frac{-1}{3} \\ \frac{-1}{3} & \frac{-1}{3} & \frac{-1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{-1}{3} & \frac{-1}{3} & \frac{-1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & \frac{-1}{3} & \frac{-1}{3} & \frac{-1}{3} \\ \frac{-1}{3} & \frac{2}{3} & \frac{2}{3} & \frac{-1}{3} & \frac{-1}{3} \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} mod\ (31)$$

$$= \begin{bmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & -2 & 0 & 1 \\ \frac{2}{3} & \frac{2}{3} & \frac{-5}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{-1}{3} & \frac{2}{3} & \frac{1}{3} & \frac{-1}{3} & \frac{-4}{3} \end{bmatrix} mod\ (31).$$

$$= \begin{bmatrix} 1 & 0 & 30 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 29 & 0 & 1 \\ 11 & 11 & 19 & 11 & 11 \\ 10 & 11 & 21 & 10 & 9 \end{bmatrix}.$$

(iii) Further he calculates the plaintext

$$P = \begin{bmatrix} 1 & 0 & 30 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 29 & 0 & 1 \\ 11 & 11 & 19 & 11 & 11 \\ 10 & 11 & 21 & 10 & 9 \end{bmatrix} \left( \begin{bmatrix} 14 \\ 13 \\ 19 \\ 4 \\ 14 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) mod\ (31)$$

$$= \begin{bmatrix} 567 \\ 14 \\ 562 \\ 815 \\ 807 \end{bmatrix} mod(31) = \begin{bmatrix} 9 \\ 14 \\ 4 \\ 9 \\ 1 \end{bmatrix}.$$

(iv) Now, receiver converts the numerical values into corresponding alphabets of Table 1 and finds the original message '**INDIA'** backs.

**REFERENCES**


**1.** Chefranov A.G. (2007), "Secure Hill cipher Modification SHC-M, Proceedings of the First Internationl Conference on Security of Information and Networks, Trafford Publishing, Canada" 34-37.

**2.** Dahab, R., Hankerson, D., Hu, F., Long, M., Lopez, J. and Alfred, M. (2006), "Software multiplication using Gaussian normal bases" *IEEE Trans. Computation*, 55, 974-984.

**3.** Gao, S. (1993), "Normal bases over finite fields, Ph.D. thesis, University of Waterloo, Canada".

**4.** Hill, L.S. (1929), "Cryptography in an Algebraic Alphabet" *American Mathematical Monthly*, 36, 306-312.

**5.** Hill, L. S. (1931), "Concerning Certain Linear Transformation Apparatus of cryptography" *American Mathematical Monthly*, 38, 135-154.

**6.** Koblitz, N. (1994), "A Course in Number Theory and Cryptography, Second Edition, Springer".

**7.** Lidl, R. and Niederreiter, H. (1986), "Introduction to finite fields and their applications, Cambridge University Press, First Edition".

**8.** Lidl, R. and Niederreiter, H. (1997), "Finite Fields, Cambridge University Press, Second Edition".

**9.** Mullen, G. L. and Panario, D. (2013), "Handbook of Finite Fields, CRC Press".

**10.** Saeednia, S. (2000), "How to make the Hill Cipher secure", *Cryptologia*, 24, 353-360.

**11.** Schneier, B. (1996) "Applied Cryptography John Wiley & Sons, New York, Second Edition".

**12.** Sharma, P. L. and Sharma, S. (2015), "Hill cipher cryptosystem using irreducible polynomials over finite fields" *Himachal Pradesh University Journal (HPUJ)*, 3, 44-52.

**13.** Sharma, P. L. and Rehan, M. (2013), "On Security of Hill cipher using finite fields" *International Journal of Computer Applications*, 71, 30-33.

**14.** Sharma, P. L. and Rehan, M. (2014), "Modified Hill cipher using vandermonde matrix and finite field" *International Journal of Technology*, 4, 252-256.

**15.** Stallings, W. (2006), "Cryptography and Network Security, Fourth Edition, Pearson".

**16.** Stinson, D. R. (2006), "Cryptography: Theory and Practice, Third Edition, Chapman & Hall/ CRC".

**17.** Toorani, M. and Falahati, A. (2011), "A secure cryptosystem based on affine transformation" *Journal of Security and Communication Networks*, 2, 207-215.

**18.** Wan, Z. X. (2003), "Lectures on finite fields and Galois rings, Singapore: World Scientific".

**19.** Wang, C. C. (1989), "An algorithm to design finite field multipliers using a self-dual normal basis" *IEEE Trans. Computation*, 38, 1457-1460.

**20.** Yeh, Y. S., Wu, T.C., Chang, C.C. and Yang, W. C. (1991), "A new cryptosystem using matrix transformation, 25th IEEE International Carnahan Conference on Security Technology" 131-138.