

Proposed Triple Hill Cipher Algorithm for Increasing the Security Level of Encrypted Binary Data and its Implementation Using FPGA

Ashraf A.M. Khalaf *, Mona S. Abd El-karim *, Hesham F. A. Hamed*

**Department of Electronics & Communications Engineering, Faculty of Engineering, Minia University, Minia, Egypt
ashkhalaf@yahoo.com, engmona1889@gmail.com, hfah66@yahoo.com*

Abstract— Nowadays security becomes an important feature with the growth of electronic communication systems . In this paper ,we study the security problem and present a proposed triple hill cipher algorithm and its implementation on FPGA to encrypt any binary data such as images , audio , video ... etc. This proposed algorithm uses three stages of a modified hill cipher to make the algorithm more robust ,each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages to increase the security. The keys are taken from random number generator. The proposed algorithm is promising to give better security.

Keywords— hill cipher , 256 bit key ,cryptography.

I. INTRODUCTION

Nowadays security becomes an important feature with the growth of electronic communication systems. Cryptography is one of the methods used to protect data from unauthorized access and being stolen [1]. Cryptography is the science and study of secret writing. A cipher is a secret method of writing , whereby plaintext is transformed into cipher text .The process of transforming plaintext into cipher text is called encryption. The reverse process of transforming cipher text into plaintext is called decryption. Both encryption and decryption are controlled by a cryptographic key or keys [2][3].

There are two types of cryptosystem, which are symmetric cryptosystem and asymmetric cryptosystem. In Symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In Asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it [1][2].

In this paper we focus on hill cipher which is a type of symmetric cryptosystem.

The hill cipher was first described in 1929 by its inventor, the mathematician Lester S. Hill, in the journal of the american mathematical monthly (Eisenberg, 1998).[1][3][4]

The hill cipher is a classical symmetric cipher based on matrix transformation. It has several advantages including its resistance to frequency analysis and simplicity due to the fact that it uses matrix multiplication and inversion for encryption and decryption. However, it succumbs to the known plaintext attack [5] and as such there have been efforts to strengthen the cipher through the use of various techniques which have improved the security of the cipher quite significantly [6],[7],[8].

In this paper we present a proposed *triple hill cipher algorithm* which consists of three stages of hill cipher , each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages to increase the security. The keys are taken from random number generator each stage consists of eight rounds with different eight keys , in each round three operations are implemented ; key and plaintext matrix multiplication , stir operation and XOR operation . this will be discussed in details in section III .we expect to achieve an algorithm more robust to cryptanalysis as we will use three layers of security.

The reason for using three stages is that, we use the same concept of the common triple DES algorithm which is standardized by ANS X9.52 and is used to enhance the DES algorithm [12].

II. THE BASIC CONCEPT OF THE CLASSICAL HILL CIPHER

Hill Cipher was the first polygraphic cipher in which the key (K), plain text (P), and cipher text (C) are represented in the form of matrices. The basic method of encryption and decryption is represented by the following equations[9][10].

$$C = (K P) \bmod(26) \quad (1)$$

$$P = (K^{-1} C) \bmod(26) \quad (2)$$

where K^{-1} is the inverse of key matrix

Here modulo 26 arithmetic is used as the study was performed on the English alphabet, where each letter (Alphabet) is allotted a number generally starting from 0 in a continuous sequence one after the other as shown in figure 1 [3].

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1. Alphabet Numbering

As shown in figure 1, Alphabets are numbered as A = 0, B =1,..., Z=25, but this is not a fixed requirement of the cipher. The encryption of plain text takes n successive plain text letters and substitutes them for n cipher text letters. In case n = 3, the encryption can be expressed in terms of the matrix multiplication as follows[3]

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod(26) \quad (3)$$

III. THE PROPOSED TRIPLE HILL CIPHER ALGORITHM

As shown in Figure 2 the proposed Triple Hill Cipher algorithm consists of three stages ,where plaintext is encrypted three times using three different 256 bits keys.

Keying options :

Option 1: k1 ,k2 and k3 are different (not equal).

Option 2: k1 ,k2 are different and k3 equal to k1, this option is considered double encryption ,but it is stronger than simply hill cipher encrypting twice, e.g with k1 and k2 because it protects against meet in the middle attack[13],

Option 3: k1 ,k2 and k3 are the same, this option is considered the least secure one.

In our proposed algorithm we use the first **option 1**, the key of the first stage is taken from random number generator ,then 1st key is rotated one time to get the 2nd key and two times to get the 3rd key or we can take the three keys from different generators.

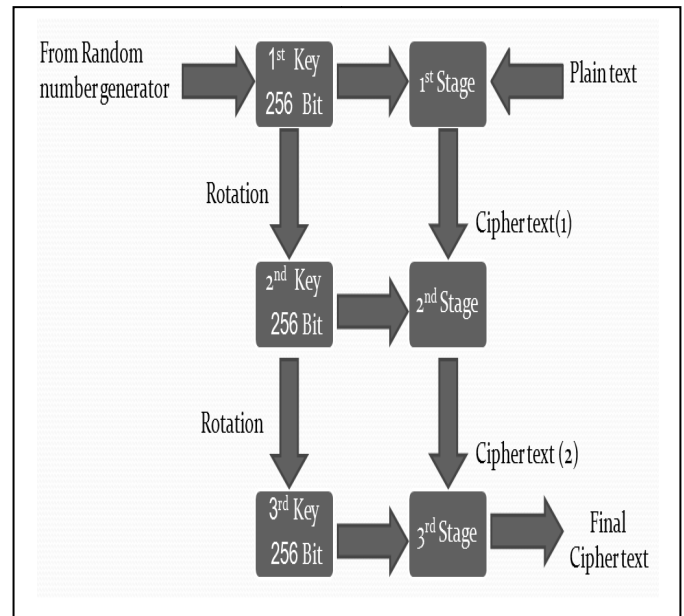


Figure 2. The Proposed Triple Hill Cipher Algorithm

A. Steps of the proposed algorithm

Each stage in this algorithm includes eight rounds as shown in Figure 3

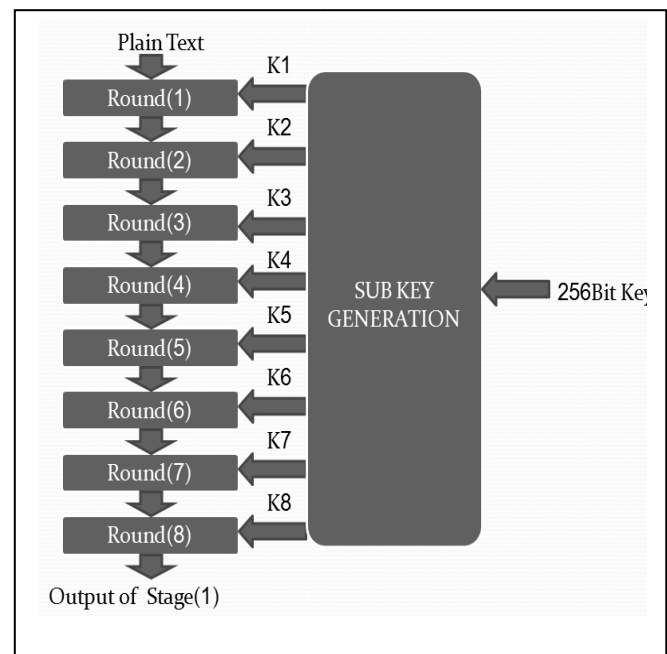


Figure 3. Single Stage Diagram

For the first stage ; plaintext is divided into blocks of lengths 128 bits ,each block is represented in 4 by 4 byte matrix .

Sub keys generation:

128 bits sub keys are generated from the 256 bits key as follow :

The 1st sub key k_2 is obtained by taking the bits from 255 to 224 , from 191 to 160 ,from 127 to 96 and from 63 to 31.

$$k_1 = \text{key}(255 \text{ downto } 224) \& \text{key}(191 \text{ downto } 160) \& \text{key}(127 \text{ downto } 96) \& \text{key}(63 \text{ downto } 32) \quad (4)$$

The 2nd sub key k_2 is obtained by taking the bits from 223 to 192 , from 159 to 128 ,from 95 to 64 and from 31 to 0 .

$$k_2 = \text{key}(223 \text{ downto } 192) \& \text{key}(159 \text{ downto } 128) \& \text{key}(95 \text{ downto } 64) \& \text{key}(31 \text{ downto } 0) \quad (5)$$

The 3rd sub key k_3 is obtained by taking the bits from 255 to 160 and from 31 to 0.

$$k_3 = \text{key}(255 \text{ downto } 160) \& \text{key}(31 \text{ downto } 0) \quad (6)$$

The 4th sub key k_4 is obtained by taking the bits from 127 to 32 and from 159 to 128.

$$k_4 = \text{key}(127 \text{ downto } 32) \& \text{key}(159 \text{ downto } 128) \quad (7)$$

The 5th sub key k_5 is obtained by taking the bits from 223 to 96.

$$k_5 = \text{key}(223 \text{ downto } 96) \quad (8)$$

The 6th sub key k_6 is obtained by taking the bits from 95 to 0 and from 255 to 224.

$$k_6 = \text{key}(95 \text{ downto } 0) \& \text{key}(255 \text{ downto } 224) \quad (9)$$

The 7th sub key k_7 is obtained by taking the bits from 31 to 0 and from 255 to 160.

$$k_7 = \text{key}(31 \text{ downto } 0) \& \text{key}(255 \text{ downto } 160) \quad (10)$$

The 8th sub key k_8 is obtained by taking the bits from 159 to 32.

$$k_8 = \text{key}(159 \text{ downto } 32) \quad (11)$$

Each of $k_1, k_2, k_3, k_4, k_5, k_6, k_7$ and k_8 is then represented in 4 by 4 byte matrices .

B. Operations in each round

Each round includes three operations as shown in Figure 4

Operation 1 represents matrix multiplication of plaintext (pt) and sub keys (k_i), where k_i represents $k_1, k_2, k_3, k_4, k_5, k_6, k_7$ and k_8 . Here we encrypt any binary data ,so we use modulo 2 field , when values in the matrices are multiplied, bitwise AND is used and when values are added bitwise XOR is used[10][11].

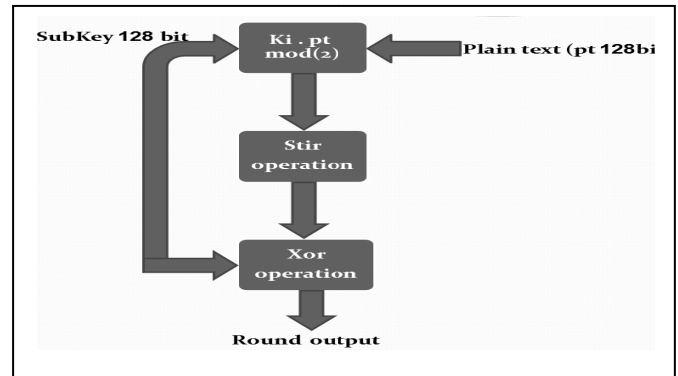


Figure 4. Single Round Diagram

Operation 2 represents the Stir operation

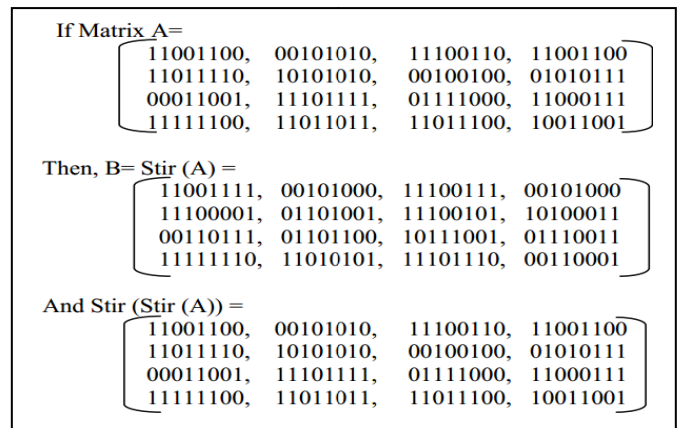


Figure 5. Stir operation

As shown in Figure 5 the stir operation is defined

by the following steps:

- The 1st and 2nd bits from each byte in a row of A are combined to form the first byte of B in that row.
- The 3rd and 4th bits from each byte in a row of A are combined to form next byte of B in that row.
- The 5th and 6th bits from each byte in a row of A are combined to form next byte of B in that row.
- The 7th and 8th bits from each byte in a row of A are combined to form the last byte of B in that row.
- This stir operation is reversible, i.e. $\text{Stir}(\text{Stir}(A))=A[9]$.

Operation 3 represents XOR operation

We perform XOR between sub keys k_i and the output of stir operation .it is performed as bit by bit XOR ,as example if we

XOR operation is reversible if $N = \text{XOR}(M, L)$
then $L = \text{XOR}(N, M)$ and $M = \text{XOR}(N, L)$.

Summary of The Proposed Triple Hill Cipher Algorithm

1. Read the message (plaintext) as a binary and divide it into blocks of lengths 128 bits ,then is represented in 4 by 4 byte matrices
2. 128 bits sub keys matrices ($k_i = 1:8$) are generated from 256 bits key
3. Find inverse of the sub keys matrices
4. If the matrices are non invertible change the key and go to step 2
- 5.

```

for m = 1:3
{
  for i = 1:8
  {
     $p_{m1} = (k_i.pt) \bmod(2)$ 
     $p_{m2} = stir(p_{m1})$ 
     $p_{m3} = XOR(k_i, p_{m2})$ 
     $pt = p_{m3}$ 
  }
}
c = pt

```

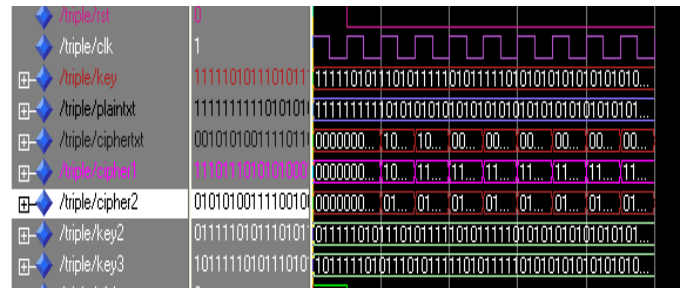
1. Prepare the inverse of the sub keys matrices k_i^{-1} .
- 2.

```

for m = 1:3
{
for i = 1:8
{
 $c_{m1} = XOR(k_i, c)$ 
 $c_{m2} = stir(c_{m1})$ 
 $c_{m3} = (k_i^{-1} \cdot c_{m2}) \bmod(2)$ 
 $c = c_{m3}$ 
}
}
pt = c

```

The proposed algorithm is coded using VHDL language and simulation results taken from Modelsim6.0C software as shown in figure 6 which shows data in binary form and figure 7 in Hex-decimal form .



wave - default					
/triples/clk	0				
/triples/cik	1				
/triples/key	FAEBE8EAAAAA9	FAEBE8EAAAAAG0FFAAAAAAEAAAAAEABFF0G0AAAAAAAAAAAAAFFC0CAEA...			
/triples/plainbit	FFD555555555400F	FFD555555555400FFD554BCCD555555			
/triples/cipherbit	2A7B283283479AE	2A7B2832834F9AE42A24282907F320			
/triples/cipher1	EBA888C254A232C	EEA888C254A262EEBA88882AFAD780			
/triples/cipher2	54F2446101DF3154	54F2446101DF31548500444 75FA3170			
/triples/cypher	7D75F5F5555555307	7D75F5F5555555507D5555555555555F831555555555555F8165F05F05555			
/triples/k ey3	BEBFAFAAAAAAAA9	BEBFAFAAAAAA983F3FAAAAAABAAAAABAAFFC1BAAAAAAAABFF032BAAE			

```

1111110101110101111101011111010101010101010101010
10011000001111111101010101010101010101010111101010
101010101010101010101011101010101111111110000011000
10101010101010101010101010101010101010101010101010
11111111110000001100101011101010101110101010101010
110010

```

```
11111111110101010101010101010101010101010101010101010101
0000000000111111111010101010110101010100011001100
11010101010101010101010101
```

```

11101110101010001000100011000010010101001010001001
10001011101000101010101010100010001000100000101010
1111101011011111001010110000

```

```

01010100111100100100010001100001000000011101111100
11000101010100010101000101000001000100010000010111
0100111110100011000101010000

```

Cipher text 3 which also is the Final Cipher text of the proposed algorithm :

00101010011110110010100000110010100000110100011110
01101011101010001010100010101000101000001000101001
0000011111110011001000110000

As shown from the simulation results ,plain text is encrypted three times ,which proves that our proposed algorithm increases the difficulty in cryptanalysis .

B. Implementation results

FPGA implementation of the proposed algorithm was accomplished on Space-Grade Virtex-4QV XQR4VSX55-10CF1140 using Xilinx ISE Design Suite 13.2 as synthesis tool . The top level RTL schematic of the proposed algorithm as shown in figures 8 and 9 is given to establish the fact that the HDL codes are synthesizable.

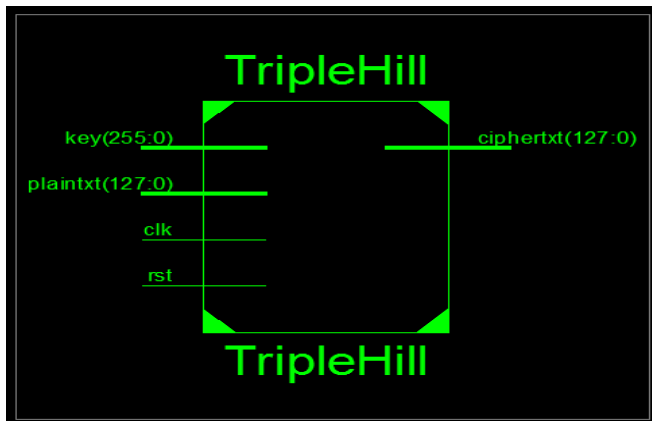


Figure 8. Top Level RTL schematic of the proposed algorithm

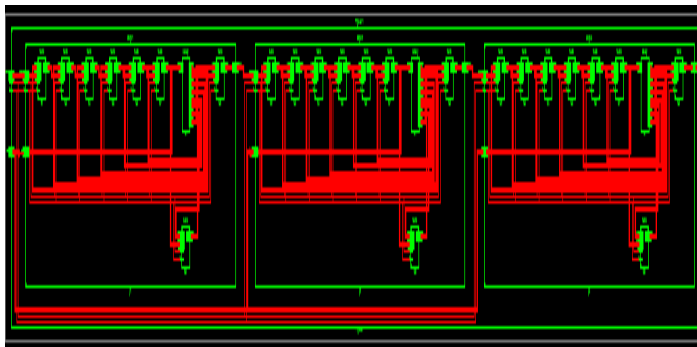


Figure 9. Top Level RTL schematic of the proposed algorithm (cont.).

Design summary for the proposed algorithm is specified in Figure 10 to set up details .

Device Utilization Summary			
Logic Utilization	Used	Available	Utilization
Number of Slice Flip Flops	3,072	49,152	6%
Number of 4 input LUTs	9,222	49,152	18%
Number of occupied Slices	4,636	24,576	18%
Number of Slices containing only related logic	4,636	4,636	100%
Number of Slices containing unrelated logic	0	4,636	0%
Total Number of 4 input LUTs	9,222	49,152	18%
Number of bonded IOBs	514	640	80%
Number of BUFG/BUFGCTRLs	1	32	3%
Number used as BUFs	1		
Average Fanout of Non-Clock Nets	3.77		

Figure 10. Design summary of the proposed algorithm

Power analysis summary of the proposed algorithm design is specified in figures 11,12 and 13 .

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Device	Virtex4	On-Chip	Power (W)	Used	Available	Utilization (%)			Supply	Summary	Total	Dynamic	Quiescent
Family	Virtex4	Clocks	0.112	1	---	---			Source	Voltage	Current (A)	Current (A)	Current (A)
Part	xq4vsc55	Logic	0.068	9222	49152	19			Vccint	1.200	0.682	0.239	0.444
Package	cf1140	Signals	0.105	9616	---	---			Vccaux	2.500	0.084	0.003	0.091
Grade	QR-Grade	DCMs	0.000	0	8	0			Vcco25	2.500	0.049	0.047	0.001
Process	Typical	IOs	0.128	514	640	80							
Speed Grade	-10	Leakage	0.763										
		Total	1.174										
Environment													
Ambient Temp (C)	50.0												
Use custom TjA?	No	Thermal Properties		Effective TjA	Max Ambient	Junction Temp							
Custom TjA (C/W)	NA			(C/W)	(C)	(C)							
Airflow (LFM)	250			6.2	117.7	57.3							
Characterization													
PRODUCTION	v1.0.02-02-08												

Figure 11. Power analysis summary of the design with Clock frequency 25 MHZ

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Device	Virtex4	On-Chip	Power (W)	Used	Available	Utilization (%)			Supply	Summary	Total	Dynamic	Quiescent
Family	Virtex4	Clocks	0.132	1	---	---			Source	Voltage	Current (A)	Current (A)	Current (A)
Part	xq4vsc55	Logic	0.135	9222	49152	19			Vccint	1.200	0.859	0.401	0.458
Package	cf1140	Signals	0.209	9616	---	---			Vccaux	2.500	0.096	0.005	0.091
Grade	QR-Grade	DCMs	0.000	0	8	0			Vcco25	2.500	0.096	0.095	0.001
Process	Typical	IOs	0.255	514	640	80							
Speed Grade	-10	Leakage	0.780										
		Total	1.512										
Environment													
Ambient Temp (C)	50.0												
Use custom TjA?	No	Thermal Properties		Effective TjA	Max Ambient	Junction Temp							
Custom TjA (C/W)	NA			(C/W)	(C)	(C)							
Airflow (LFM)	250			6.2	115.6	59.4							
Characterization													
PRODUCTION	v1.0.02-02-08												

Figure 12. Power analysis summary of the design with Clock frequency 50 MHZ

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Device	Virtex4	On-Chip	Power (W)	Used	Available	Utilization (%)			Supply	Summary	Total	Dynamic	Quiescent
Family	Virtex4	Clocks	0.172	1	---	---			Source	Voltage	Current (A)	Current (A)	Current (A)
Part	xq4vsc55	Logic	0.271	9222	49152	19			Vccint	1.200	1.215	0.726	0.488
Package	cf1140	Signals	0.419	9616	---	---			Vccaux	2.500	0.101	0.010	0.091
Grade	QR-Grade	DCMs	0.000	0	8	0			Vcco25	2.500	0.191	0.190	0.001
Process	Typical	IOs	0.510	514	640	80							
Speed Grade	-10	Leakage	0.817										
		Total	2.183										
Environment													
Ambient Temp (C)	50.0												
Use custom TjA?	No	Thermal Properties		Effective TjA	Max Ambient	Junction Temp							
Custom TjA (C/W)	NA			(C/W)	(C)	(C)							
Airflow (LFM)	250			6.2	111.4	63.6							
Characterization													
PRODUCTION	v1.0.02-02-08												

Figure 13. Power analysis summary of the design with Clock frequency 100MHZ

V. CONCLUSION

In the cryptanalysis of the classical hill cipher ,the known plaintext attack is performed using the method $k = p^{-1} c$ where p is an invertible matrix , so if an attacker has m distinct plaintext and cipher text ,can retrieve the key using the previous method .In the proposed triple Hill Cipher algorithm the known plain text attack becomes more difficult as the plain text is encrypted using eight rounds with eight different keys three times ,we can say that , we used 24 different keys which makes the task of the known plain text attack more difficult, there is no doubt that increasing the number of stages for example four stages instead of three increases the level of security but the overall performance of the algorithm become more slower.

REFERENCES

- [1] A.F.A. Abidin, O.Y. Chuan and M.R.K. Ariffin "A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes" Journal of Computer Science 7 (5): 785-789, 2011.
- [2] William Stallings ,''Cryptography and Network Security Principles and Practices'', Fourth Edition, Prentice Hall, November 16, 2005.
- [3] Jasdeep Singh Bhalla, '' A Database Encryption Technique to Enhance Security Using Hill Cipher Algorithm'', International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 4, April 2013.
- [4] M. Nordin A. Rahman, A. F. A. Abidin, Mohd Kamir Yusof, N. S. M. Usop, '' Cryptography: A New Approach of Classical Hill Cipher'', International Journal of Security and Its Applications, Vol. 7, No. 2, March, 2013.
- [5] D.R. Stinson, "Cryptography Theory and Practice", Third Edition, Chapman and Hall/CRC, Pp.13-37, 2006.
- [6] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text," International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, Pp. 27 -30, Oct. 2009.
- [7] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", International Journal of Computational Science, Vol. 2, No. 6, 815-826, Dec. 2008.
- [8] Bhimbudendra Acharya, Girija Sankar Rath, and Sarat Kumar Patra, "Novel Modified Hill Cipher Algorithm," Proceedings of ICTAETS, Pp. 126-130, 2008.
- [9] Gandharba Swain, and Saroj Kumar Lenka, ''A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography'', International Journal of Security and Its Applications, Vol. 6, No. 2, April, 2012.
- [10] Ahmed Desoky, Anju Panicker Madhusoodhanan, '' Bitwise Hill Crypto System'', DOI: [10.1109/ISSPIT.2011.6151539](https://doi.org/10.1109/ISSPIT.2011.6151539)
- [11] Ali Muhammad Ali Rushdi and Fares Ahmad Muhammad Ghaleb, ''On Self-Inverse Binary Matrices Over the Binary Galois Field'', Journal of Mathematics and Statistics 9 (3): 238-248, 2013.
- [12] D. Coppersmith, D. B. Johnson and S. M. Matyas, ''A proposed mode for triple-DES encryption'', IBM J. RES, DEVELOP. VOL. 40 NO. 2 MARCH 1996.
- [13] D. McIlroy Editor, ''On the Security of Multiple Encryption'', Communications July 1981 of Volume 24 the ACM Number 7.