Cryptanalysis of Bitwise Hill Cryptosystem–A Chosen Plaintext Attack

Rampaka Manojkumar[1], M Satish Kumar [2], Prudhvi Raju Ganasala[3], Sandi Sridhar Reddy[4], Macha Pooja[5] and Ravi Shankar Nanduri[6]*

[1,2,3,4,5,6] Nalla Narasimha Reddy Education Society's Group of Institutions. Hyderabad, India
ravishankar.nanduri@gmail.com

Abstract. This paper cryptanalyzes a block cipher proposed by Ahmed Desoky et al, which essentially is a variant of the classical Hill Cipher. The researchers have modified the cipher wherein, plaintext is taken in the form of rectangular matrices of size 3X8 in the illustration of the cipher. The claim of the authors is that, since the plaintext is in the form of rectangular matrix, there can be no modular arithmetic inverse for the plaintext. Thus, the cipher overcomes the weakness of the classical Hill Cipher, the known plaintext attack vulnerability. The cipher does show resistance against the known plaintext vulnerability exhibited by the classical Hill Cipher. However, the cryptosystem proposed by the researchers' exhibits weaknesses in the face of the chosen plaintext attack, which is employed in this paper. The cipher is broken with the help of 8 chosen plaintexts.

Keywords: Encryption, Decryption, Modular Arithmetic Inverse, Plaintext, Ciphertext.

1 Introduction

The study of cryptology comprises two streams, cryptography and cryptanalysis. The science of cryptography broadly depends on mathematics and number theory, concentrates on converting the plaintext into an unintelligible stream of bytes, also called the ciphertext. The cryptanalysis is about exploiting the weaknesses in the encryption algorithms and breaks the ciphers. Both these sub-branches of the cryptology complement each other and help bring out robust and secure cryptosystems which offers stiff resistance to attacks. The cryptographic algorithms are also classified based on unit of encryption. Depending on whether each character is encrypted independently or a group of characters together are encrypted as a single unit, the former class is called stream ciphers, while the latter go by the name block ciphers. The encryption algorithms are also classified into two groups depending on the key used in the processes of encryption and decryption. If same key is for encryption and decryption, such algorithm is called symmetric key cipher/private key cryptographic algorithms. However, if different keys, one for encryption and another for decryption are used, they are termed as public key/asymmetric key cryptographic algorithms. Here, it

© The Author(s) 2026
P. Bagchi et al. (eds.), *Proceedings of the International Conference on Information Systems Design And Intelligent Applications (ICISDA 2026)*, Advances in Intelligent Systems Research 215,
https://doi.org/10.2991/978-94-6239-821-4_6

should be noted that it should be computationally infeasible to deduce decryption key from encryption key.

The literature of symmetric key block ciphers started with the first cipher proposed by Lester Hill [2, 3]. This is the first polyalphabetic cipher reported in the literature of the cryptography. This also is the first cipher that has demonstrated that algebraic principles can be used in the design of encryption algorithms. However, this cipher suffers from a fatal vulnerability, the known plaintext attack [4]. Several stream ciphers [5-8] were proposed during Second World War for secure communication. However, all these ciphers were proposed in the pre-computerization period thus are trivial according to today's computational power. The first non-trivial block cipher, in the post computerization period, is proposed by IBM Corporation, known as Data Encryption Standard (DES) [9]. Developed by IBM Corporation, under the close supervision by the US government, this cipher was always viewed with suspicion. Many block ciphers, outside the influence of the US government were proposed by many researchers [10-13], originating mainly from European countries.

Coming back to the literature of the classical Hill Cipher, a number of researchers have attempted to strengthen the cipher by adding additional operations or by making modifications to the cipher. Some of these researchers have attempted to make modifications to the key matrix, in such a way that each block of the plaintext is encrypted with a different key. Thus, cryptanalyst has to obtain each key matrix separately. Jack Levine [14-18] used drazin inverses, also known as auto key inverses, to encrypt data. Application of RD class of matrices is proposed by Boshra H. Makar [19]. In this, infinite invertible matrices can be derived from a single matrix. Each block of plaintext is encrypted with a different key. Jack Levine and Richard Chandler [20] through their work proposed the concept of involutory matrices, where the key matrix itself is its inverse and it satisfies the relation $KK \equiv I \pmod{n}$. Bhibudendra Acharya et al [21] have given a method of computing the involutory matrix.

All these works concentrated on making modifications to the key matrix and derive a separate key for encrypting each block of plaintext. Sastry et al have taken a different approach and made the cipher iterative. They have also added additional operations in each of such iterations to make the cipher complex and make the relationship between the plaintext and the ciphertext complex and non-linear. In their papers, they have proposed interlacing [22, 23], interweaving [24-27], permutation [28-30], intertwining [31-33]. They have also added Playfair cipher into this encryption scheme [34-39] and introduced substitution in addition to the key matrix multiplication. In all these ciphers, the emphasis is on making the cipher an iterated one, and adds multiple additional operations in each of the iterations.

This paper concentrates on carrying out a chosen plaintext attack on the cipher "Bitwise Hill Cryptosystem" proposed by Ahmed Desoky et al [1], which hereinafter, will be referred to as the Target Cipher.

The paper is organized as follows: Section 2 describes the functioning of the Target Cipher, Section 3 demonstrates the cryptanalytic attack devised in this paper. Finally Sction 4 draws conclusions.

2 Description of the Target Cipher

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts. True Type 1 or Open Type fonts are required. Please embed all fonts, in particular symbol fonts, as well, for math, etc.

The Bitwise Hill Cryptosystem proposed by Ahmed Desoky et al [1], is essentially a modification of the classical Hill Cipher. The scheme proposed by the researchers is described below.

a. The plaintext is taken as a group of n characters. These n characters are then converted into their equivalent EBCDIC codes and are further mutated into their 8 bit binary equivalent. By transforming n characters into n strings of 8 bits for each character, 8n elements are formed. These 8n elements are then divided into 8 parts in a columnwise manner, each part is called a plane. In their paper, the authors have taken 24 characters as a block. Thus, they form an 8X24 matrix wherein, the first character's binary equivalent will form the first column of this matrix, second one's binary equivalent will be placed in the second column and so on. Each group of 24 bits, of each row, is then converted into a matrix of size 3X8, arranged in a columnar manner. The first three bits fill the first column of the 3X8 matrix. Next three bits will be placed in the second column and so on. Thus, 8 numbers of 3X8 matrices, one for each row, are formed. The authors probably want to keep the number of planes and the number of blocks (three in this case) confidential.
b. 8 random matrices of size 8X8 size, with elements from {0, 1} are formed. The matrices are formed in such a way that each of them will have a modular arithmetic inverse (modulo 2). These are 8 key matrices K_i | i=1 to 8.
c. Each of the 3X8 matrices, formed as described above, are then multiplied with K_i | i=1 to 8, modulo 2. The resultant matrix, of size 3X8, is the ciphertext.
d. Now, blocks are combined together into planes and merging planes together to get the final ciphertext of size of 24 characters.

In the process of decryption, the 24 character ciphertext is converted into their binary equivalent binary form, as an 8X24 matrix and then each row of this 8X24 matrix is again arranged in the form of a 3X8 binary matrix. Each of these 3X8 matrices are then multiplied (modulo 2) with the modular arithmetic inverses of k_i, k_i^{-1}| i= 1 to 8, to get the original plaintext.

3 The Cryptanalytic Attack

As outlined in the introduction, cryptanalysis is the study of exploiting the weaknesses in the encryption algorithms. This is a process that helps researchers in proposing ciphers that are robust and resistant to rigorous cryptanalytic attacks, which is the ultimate goal of the study.

The elementary cryptanalytic techniques that are reported in the literature [40] are

a. Ciphertext only / Brute force attack.
b. Known plaintext attack.
c. Chosen plaintext/ciphertext attack.

d. Adaptive chosen plaintext/ciphertext attack.

In the case of the brute force attack, the cryptanalyst has the knowledge of encryption algorithm and the ciphertext only. The cryptanalyst will then start decrypting the ciphertext with every possible key in the key space. Whichever plaintext, after decryption, constitute a coherent one is taken as the plaintext and the corresponding key is considered as the decryption key. Here, the cryptanalyst has to check for all possible combinations in the key space. The size of such a key space is 2^n. The brute force attack, by its fundamental characteristics, is meant to be difficult.

In the case of the known plaintext attack, the cryptanalyst has the knowledge of the plaintext, ciphertext and the algorithm used in the cipher. Here, the cryptanalyst has to exploit the weaknesses in the algorithm, intelligently utilize the knowledge of the plaintext and the corresponding ciphertext to ascertain the key and thus break the cipher. In these types of attacks, the adversary has the knowledge of all the aspects of the algorithm, except the key. If the adversary can still obtain the key, then the cipher is considered as a weak cipher and cannot be used for secure communications.

The chosen plaintext/ciphertext attack is a little more leniency given to the cryptanalyst in finding the vulnerabilities of the encryption algorithm. The attacker is given the freedom to choose the plaintext and seek the corresponding ciphertext. Alternatively, a ciphertext is chosen and its respective plaintext is sought. In this process, the attacker will exploit the weaknesses in the cipher to break it.

The last case is the adaptive chosen plaintext/ciphertext attack, wherein the cryptanalyst will chooses a plaintext/ciphertext and seeks its corresponding ciphertext/plaintext. Once the data is received, attacker will study the pair and then make some modifications to the previously chosen text and the corresponding text is sought. This way, the adversary will seek any number of plaintext/ciphertext pairs. If the cryptanalyst is able to reveal the key, from all such texts, the cipher is again considered as weak and should not be used in confidential communications. In the case of Data Encryption Standard (DES), which has a key and plaintext space of 56 bits each, 2^{47} chosen plaintext-ciphertext pairs were sought to break the cipher in differential cryptanalytic attack.

Other than these four basic attacks, many advanced cryptanalytic attacks were reported in the literature like Linear Cryptanalysis [41], Differential Cryptanalysis [42], Slide attacks [43], impossible differentials [44], boomerang attacks [45] … etc.

The Target Cipher is essentially a variant of the classical Hill Cipher. However, it does not suffer from the fatal weakness which the original cipher suffers from, i.e., the known plaintext attack. In the case of the known plaintext attack, if the adversary can compute the modular arithmetic of the plaintext, it gives away the key matrix. However, the Target Cipher's plaintext size is 3X8 matrix, which is a non-square matrix and thus doesn't have a modular arithmetic inverse. However, it suffers from another kind of vulnerability.

Here, every block of plaintext, comprising 24 binary bits, arranged in the form of a matrix of size 3X8, in a columnwise manner. This 3X8 matrix is then multiplied with a key matrix of size 8X8, containing 0s and 1s. The matrices are multiplied (modulo 2). This multiplication of the 8^{th} block of plaintext is multiplied with an 8X8 key matrix K_8 is illustrated below:

$$P_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (1)$$

$$K_8 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (2)$$

The corresponding ciphertext $C_8 = K_8P_8 \bmod 2$, is

$$C_8 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \quad (3)$$

A closer examination of this multiplication is needed. If a plaintext is taken in the form shown below,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4)$$

The multiplication of this plaintext matrix with the key matrix will completely reveal the first row of the key matrix. If the element K_{11} is 0 (zero) then the first element of the resultant product matrix will also be 0. If the first element of the key matrix is a 1, then the first element of the resultant product matrix will be a 1. Same principle applies to all the elements of the first row of the key matrix. Similarly, if the plaintext of the form

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

When multiplied with the key matrix will give away the second row of the key matrix.

Thus, the element 1 at each position in the first row of the plaintext will reveal the corresponding row of the key matrix. As a result, 8 chosen plaintexts will give away all 8 rows of the key matrix.

The complete attack is now outlined below: Firstly a chosen plaintext containing two characters (any two characters) are supplied to the encipherer and its corresponding ciphertext is sought. This step is needed to find out the size of the block. Block ciphers have a property, where the size of the plaintext is fixed. The cipher cannot operate if the size of the plaintext block is lesser than the designed size. Thus, if a smaller sized block is supplied, the cipher will pad the given plaintext to fill up to the block size. Thus, when two characters are given, the cipher pads up the two characters with additional characters to make the designed block size (22 in this case). Thus, by examining the ciphertext, corresponding to the plaintext supplied, the attacker will be able to deduce the block size. Along with this, the adversary will also know the number of key matrices, and size of each of the key matrix. The cryptanalyst also knows that the plaintext matrix will be of size 3X8.

The second block of plaintext is {255, 0, 0,…, 0}. Here, the first character is 255 and the remaining characters are 0s (EBCDIC). Those 24 characters are first converted into their binary equivalent and then arranged in the form of an 8X24 matrix. Here, the first column is the first character and the second column is the second character and so on. Thus, such a matrix assumes the form

$$\begin{bmatrix} 1 & 0 & 0 & \\ 1 & 0 & 0 & \\ 1 & 0 & 0 & \\ 1 & 0 & 0 & \\ 1 & 0 & 0 & \ldots 24 \text{ columns} \\ 1 & 0 & 0 & \\ 1 & 0 & 0 & \\ 1 & 0 & 0 & \end{bmatrix} \tag{6}$$

The first row of this matrix, given in (6) is again converted into another matrix of size 3X8, in a columnwise manner. Thus, the first three bits form the first column. Next three bits will be placed in the second column and the pattern continues. Thus, the first row, converted into 3X8 matrix, is the first plaintext block P_1, is then multiplied with the first key matrix K_1 of size 8X8, for which a modular arithmetic inverse exists. Thus,

$C_1 = K_1P_1 \bmod 2.$

$$\text{Here, } P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{7}$$

When K_1 is multiplied with P_1, as explained above, the resulting matrix contains the elements of K_1 in the first row and the elements in the remaining two rows are 0s. The second row of (6), when rearranged into a 3X8 sized matrix form, constitutes P_2. This P_2 is also of the form given in (7). The second block of ciphertext is obtained by multiplying K_2 and P_2.

$$C_2 = K_2P_2 \bmod 2. \tag{8}$$

Here also, the first row of C_2 is same as the first row of K_2 and the elements in the remaining two rows of C_2 will be zeroes. When all the rows of (6), converted into plaintext matrices of size 3X8, multiplied with the respective key matrix K_i, give away the first rows of the all the key matrices.

In the next step, the cryptanalyst chooses a plaintext of form {0, 0, 0, 255, 0, 0, …}.

When this plaintext is converted into its binary form in a columnar fashion, will be of the form

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \ldots 24 \text{ columns} \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & \end{bmatrix} \tag{9}$$

Each row of this matrix, when converted into a matrix of size 3X8, in a columnwise fashion, each of those matrices will be of the form

$$P_i = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad i=1 \text{ to } 8 \tag{10}$$

Each of these P_i, when multiplied with the corresponding K_i, i=1 to 8, will give the ciphertext C_i, i=1 to 8. The first row of each of the C_i will be same as the second row of the K_i, i=1 to 8. The elements of second and third rows of C_i will be zeros. Thus, the second chosen plaintext reveals the second row of the key matrices K_i.

Third chosen plaintext of the form{0,0,0,0,0,0,255,0,0,…}, when converted into their binary equivalent and arranged in the form of a 3X8 matrix, will appear as

$$P_i = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad i=1 \text{ to } 8 \tag{11}$$

This will reveal the third row of all the K_i. Thus, with 8 chosen plaintexts, all the elements of the K_i will be revealed and the cipher is broken. It can be noted that the size of the plaintext block, size of the key matrix, number of blocks or any other factor will not affect the cryptanalytic attack. The cipher is conclusively broken.

4 Conclusions

The major vulnerability of the classical Hill Cipher is the known plaintext. If the plaintext [P] is taken in the form of a matrix of size nXn, which is then multiplied with the key matrix [K], also of size nXn, the ciphertext C is obtained as

C = KP mod x, where x is the number of characters in the domain of the alphabet. If P is known and if P can be inverted (modulo x), then such P^{-1}, when multiplied by C, will give away the key matrix K.

C = KP mod x.

CP^{-1} mod x = KPP^{-1} mod x = K.

In the Target Cipher, authors assumed that P is taken in the form of a rectangular matrix, for which no modular arithmetic inverse exists. Thus, the known plaintext vulnerability vanishes and the cipher becomes strong. However, there are other ways in which a cipher can be broken as illustrated in this paper.

Any non-trivial cipher has to be an iterated one, with multiple operations applied on the plaintext in each of the iteration to make the cipher robust and to be resistant to rigorous cryptanalytic attacks. In the Target Cipher, that part is lacking. A single key matrix multiplication can never be a good encryption technique.

Many variants of the classical Hill Cipher have been broken by various researchers, which have only a single matrix multiplication. However, multiple operations in each iteration as specified in Fiestel Structure offer better performance. All the modern block ciphers follow this pattern.

References

1. A. Desoky and A. P. Madhusoodhanan, "Bitwise hill crypto system," 2011 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Bilbao, Spain, 2011, pp. 080-085, doi: 10.1109/ISSPIT.2011.6151539.
2. Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, TheAmerican Mathematical Monthly 1931, 38(3):135-154.
3. L.S.Hill, "Cryptography in an algebraic alphabet" American Mathematical Monthly, 1929, 36(6): 306-312.
4. Levine, Jack. "Some Elementary Cryptanalysis of Algebraic Cryptography." American Mathematical Monthly 68(5): 411-18.
5. Rivest, R. L. (1992). The RC4 encryption algorithm. RSA Data Security, Inc.
6. Boesgaard, M., Vesterager, M., Pedersen, T., Christiansen, J., & Scavenius, O. (2003). Rabbit: A New High-Performance Stream Cipher. In T. Johansson (Ed.), Fast Software Encryption (FSE 2003). Lecture Notes in Computer Science, vol 2887, pp. 307-329. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-39887-5_23
7. P. Rogaway and D. Coppersmith, "A Software-Optimized Encryption Algorithm (SEAL)," in Journal of Cryptology, vol. 11, no. 4, pp. 273–287, 1998, DOI: 10.1007/s001459900048.
8. Halevi, S., Coppersmith, D., & Jutla, C. (2002). Scream: A Software-Efficient Stream Cipher. In Daemen, J., & Rijmen, V. (Eds.), *Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science* (Vol. 2365). Springer, Berlin, Heidelberg.
9. National Institute of Standards and Technology. (1999). Data encryption standard (DES) (FIPS PUB 46-3). U.S. Department of Commerce. doi.org
10. X. Lai and J. L. Massey, "IDEA: A proposal for a new block encryption standard," Advances in Cryptology — EUROCRYPT '90, vol. 473, pp. 389–404, 1991.
11. Anderson, R. J., Biham, E., & Knudsen, L. R. (1998). "Serpent: A New Block Cipher Proposal." In Fast Software Encryption, FSE '98 (Lecture Notes in Computer Science, Vol. 1372).
12. Barreto, P. S. L. M., & Rijmen, V. (2000). The Anubis block cipher. Submission to the NESSIE project.
13. Nakahara, J., Rijmen, V., Preneel, B., & Vandewalle, J. (2004). The MESH block ciphers. In K.-J. Chae & M. Yung (Eds.), Information Security Applications (Lecture Notes in Computer Science, Vol. 2908, pp. 493–508). Springer. https://doi.org/10.1007/978-3-540-24591-9_3
14. Jack Levine and Robert E. Hartwig, "Applications of the Drazin Inverse to the Hill Cryptographic System Part-I", Cryptologia, April 1980, 4(2):71-85. 232
15. Jack Levine and Robert E. Hartwig, "Applications of the Drazin Inverse to the Hill Cryptographic System Part-II", Cryptologia, July 1980, 4(3): 150-168.
16. Jack Levine and Robert E. Hartwig, "Applications of the Drazin Inverse to the Hill Cryptographic System Part-III", Cryptologia, April 1981, 5(2):67-77.
17. Jack Levine and Robert E. Hartwig, "Applications of the Drazin Inverse to the Hill Cryptographic System Part-IV", Cryptologia, October 1981, 5(4):213-228.
18. Brawley, J. V., & Levine, J. (1972). Equivalence classes of linear mappings with applications to algebraic cryptography, I. Duke Mathematical Journal, 39(1), 121-132.
19. Boshra H. Makar, "Application of a Certain Class of Infinite Matrices to the Hill Cryptographic System", Cryptologia, January 1983, 7(1):63-78.
20. Jack Levine, Richard Chandler, "The Hill Cryptographic System with Unknown Cipher Alphabet, But Known Plaintext", Cryptologia, January 1989, 13(1):1-28.

21. Bhibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, “Novel Modified Hill Cipher Algorithm”, Proceedings of ICETAETS, 2008, pp. 126-130.
22. V.U.K. Sastry, N.Ravi Shankar, “Modified Hill Cipher with Interlacing and Iteration”, Journal of Computer Science, Science Publications, 2007, 3(11):854-859.
23. V.U.K. Sastry, N.Ravi Shankar, “Modified Hill Cipher for a large block of plaintext with Interlacing and Iteration”, Journal of Computer Science, Science Publications, 2008, 4(1):15-20.
24. Vadlamudi Naveen Kumar, N. Ravi Shankar, "Cryptanalysis of A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm: A Chosen Ciphertext Attack", Progress in Computing, Analytics and Networking (Proceedings of ICCAN 2019), Advances in Intelligent Systems and Computing, Springer, Volume: 1119, pp: 475-482.
25. K. Vishwa Nageshwar, N. Ravi Shankar,"Cryptanalysis of Modification in Hill Cipher for Cryptographic Application" (Advances in Machine Learning and Computational Intelligence 2020),Algorithms for Intelligent Systems Springer, Volume:16171, pp: 659-666.
26. V.U.K.Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Modified Hill Cipher involving Interweaving and Iteration”, International Journal of Network Security (scopus), 11(2): 51-56, September 2010.
27. V.U.K.Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Large Block Cipher involving Interweaving and Iteration”, proceedings of the International Conference on Advances and Emerging Trends in Computing Technologies (ICAET10)” June 21-24, 2010, Chennai pp: 328-333.
28. Joshi Padma N, N. Ravishankar, M. B. Raju, N.Ch. Ravi, "SURGICAL STRIKING SQL INJECTION ATTACKS USING LSTM", / Indian Journal of Computer Science and Engineering (IJCSE), 13(1): 208-220.
29. V.U.K.Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Modified Playfair Cipher Involving Interweaving and Iteration”, International Journal of Computer Theory and Engineering, 1(5): 594-598, December, 2009.
30. V.U.K.Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Modified Playfair Cipher for a Large Block of Plaintext”, International Journal of Computer Theory and Engineering, 1(5): 590-594, December, 2009.
31. Joshi Padma N, N. Ravishankar, M. B. Raju, "Defensive Walls for Detecting and Preventing SQL Injection and XSS attacks in Dynamic Content Delivery Network Web Applications" Design Engineering (scopus), 2021(7):10019- 10039, 2021.
32. V.U.K. Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Blending of A Generalized Playfair Cipher and A Modified Hill Cipher”, International Journal of Networks and Mobile Technologies, January, 2011, 2(1): 35-43.
33. Padma, NJ, Raju, MB, Ravishankar, N, Ravi, NC, Encountering SQL Injection in Web Applications, PROCEEDINGS OF THE 2ND INTERNATIONAL CONFERENCE ON COMPUTING METHODOLOGIES AND COMMUNICATION (ICCMC 2018), Page257-261
34. Padma, NJ, Raju, MB, Ravishankar, N, Ravi, NC, Contemplating Security of Http From Sql Injection and Cross Script, 2017 IEEE INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND COMPUTING RESEARCH (ICCIC), Page948-952
35. V.U.K. Sastry, N.Ravi Shankar, S.Durga Bhavani, “A Generalized Playfair Cipher involving Intertwining, interweaving and Iteration”, International Journal of Networks and Mobile Technology, November 2010, 1(2): 45-53.

36. Sastry, V. U. K., Shankar, N. Ravi and Bhavani, S. Durga. "A Large Block Cipher Involving Key Dependent Permutation, Interlacing and Iteration" Cybernetics and Information Technologies (ESCI), 2013 13(3): 50-63.
37. Sastry, V. U. K., & Janaki, V. (2007). A block Cipher using linear Congruences. Journal of Computer Science, 3(7), 556-561.
38. Sastry, V. U. K., & Janaki, V. (2007). Modified Hill Cipher with key dependent permutation and circular Rotation. Journal of Computer Science, 3(9), 736-739.
39. Sastry, V. U. K., & Janaki, V. (2008). A modified hill cipher with multiple keys. International Journal of Computational Science, 2(6), 815-826.
40. Stallings, William. Cryptography and Network Security: Principles and Practice. 7th ed. New York: Pearson, 2017.
41. Matsui, M. (1994). Linear cryptanalysis method for DES cipher. In T. Helleseth (Ed.), Advances in Cryptology — EUROCRYPT '93 (pp. 386–397). Springer-Verlag.
42. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3-72.
43. A. Biryukov, D. Wagner (1999). "Slide Attacks". In: Fast Software Encryption (FSE '99). Lecture Notes in Computer Science, vol 1636. Springer, Berlin, Heidelberg.
44. Boura, C., Naya-Plasencia, M., BOURA, C. and NAYA-PLASENCIA, M. (2024). Impossible Differential Cryptanalysis. In Symmetric Cryptography 2 (eds C. Boura and M. Naya-Plasencia).https://doi.org/10.1002/9781394256327.
45. David Wagner. 1999. The Boomerang Attack. In Proceedings of the 6th International Workshop on Fast Software Encryption (FSE '99). Springer-Verlag, Berlin, Heidelberg, 156–170.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

