



Cryptanalysis of Hill Cipher Modification: A Simplified Approach

Dasari Srivani¹

CSE(DATA SCIENCE)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

srivanikj507@gmail.com

Dheeravath Arundathi²

CSE(DATA SCIENCE)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

arundathistar3@mail.com

Netra Nagabhushan³

CSE(DATA SCIENCE)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

netran359@gmail.com

Ravula Lavanya⁴

CSE(DATA SCIENCE)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

lavanyareddy.gatla@gmail.com

Singireddy Sandyarani⁵

CSE(DATA SCIENCE)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

sandyareddy.809@gmail.com

Ravi Shankar Nanduri^{6,*}

Department of CSE (DS)

Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India.

ravishankar.nanduri@gmail.com

Abstract— Paragas et al. [1] proposed a modified Hill cipher that surrounds the classical key-matrix multiplication with a chain of bitwise XOR operations on the plaintext, a column-wise circular bit shift and a Radix-64 encoding stage. This paper asks whether these additions repair the known algebraic weakness of the Hill cipher, and shows that they do not. Every added operation is independent of the key and can be recomputed or inverted by an adversary, so the 4×4 key matrix remains the only secret and the relation between the data entering and leaving it remains linear. Exploiting this, we break the cipher with a single chosen ciphertext: its decryption discloses the inverse key matrix modulo 256, from which the key matrix itself follows at once. We conclude by proposing a substitution stage that would strengthen the cipher against attacks of this kind.

Index Terms— Hill cipher, chosen-ciphertext attack, modular matrix inverse, plaintext, ciphertext, Radix-64.

I. INTRODUCTION

The cipher introduced by Lester Hill [2, 3] was the first encryption scheme in the cryptographic literature to be built explicitly on linear algebra: a block of plaintext symbols is treated as a vector and enciphered by multiplication with an invertible key matrix under modular arithmetic. Because a whole group of symbols is transformed at once, a change to any one of them alters every symbol of the resulting ciphertext block; this made Hill's construction the first polygraphic cipher able to operate practically on blocks of more than three symbols. The same property gives the classical cipher strong diffusion of plaintext statistics and, for practical key sizes, a key space too large for exhaustive search. Its weakness lies elsewhere. Since encryption is a linear map, an adversary who holds enough plaintext-ciphertext pairs can solve for the key, and the cipher therefore falls to a known-plaintext attack [4]. A considerable body of work has tried to remove this weakness, most prominently the contributions of Levine [5–9]

and Makar [10]. Acharya et al. [11] gave a method for computing involutory key matrices, that is, matrices satisfying $KK \bmod n = I$, so that one matrix serves for both encryption and decryption.

The studies cited above follow a common strategy: they change how the key matrix is formed or applied so that no two plaintext blocks are enciphered under the same key. Sastry et al. took a different route. Their designs make the Hill cipher iterative, enlarge the key matrix to 8×8 , and in every iteration combine multiplication by the key with further transformations of the data, namely interlacing [12–14], interweaving [15–17], substitution [18–22], permutation [23, 24] and intertwining [25, 26]. The purpose of these transformations, taken together with the matrix multiplication, is to turn the linear dependence of ciphertext on plaintext into a nonlinear one, and so to make the cipher resistant to the algebraic attacks that succeed against the classical design.

This paper analyses the modified Hill cipher of Paragas et al. [1], referred to hereafter as the Target Cipher. Our question is whether its additional operations meaningfully strengthen the classical cipher. We argue that they do not: because none of them depends on the key, they leave the linear core of the cipher exposed, and a single chosen ciphertext is enough to recover the key.

The remainder of the paper is organized as follows. Section II describes the Target Cipher and traces its encryption procedure through a worked example. Section III sets out the attack model and its assumptions and then presents the attack. Section IV states our conclusions and suggests how the design could be strengthened.

II. DESCRIPTION OF THE TARGET CIPHER

The Target Cipher [1] keeps the core of the classical Hill cipher, multiplication of a plaintext block by a key matrix, and



surrounds it with additional processing before and after that step. Arithmetic is carried out modulo 256, whereas the plaintext alphabet is the 128-character ASCII set. Values above 127, which lie outside that alphabet, can therefore arise during encryption; we note this anomaly, but it has no effect on the attack presented here. The key is a 4×4 matrix, and the plaintext is accordingly processed in blocks of 16 characters arranged as 4×4 matrices so that they are conformable for multiplication with the key. The key matrix is derived from a 2×2 matrix as follows.

First, an invertible 2×2 matrix A is chosen manually:

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \begin{bmatrix} 56 & 11 \\ 5 & 25 \end{bmatrix} \quad (1)$$

The 4×4 key matrix K is then assembled from A in block form:

$$K = \begin{bmatrix} A & A^{-1} \\ A_T^{-1} & A_T \end{bmatrix} = \begin{bmatrix} 56 & 11 & 217 & 181 \\ 2 & 25 & 59 & 56 \\ 217 & 59 & 56 & 2 \\ 181 & 56 & 11 & 25 \end{bmatrix} \quad (2)$$

Although K is produced through a sequence of operations on A, these operations add nothing to the security of the cipher. An adversary need not recover A or retrace the construction, since obtaining K itself is all that is required to break the cipher. The construction of K therefore plays no part in the attack.

The inverse of K modulo 256, K^{-1} , is

$$K^{-1} = \begin{bmatrix} 174 & 69 & 45 & 41 \\ 75 & 55 & 37 & 248 \\ 77 & 139 & 78 & 201 \\ 135 & 216 & 135 & 99 \end{bmatrix} \quad (3)$$

As a running example, the plaintext block is taken to be $P = \text{"Imagination"}$

Replacing each character in (4) by its ASCII code gives the plaintext matrix

$$P = \begin{bmatrix} 73 & 105 & 105 & 105 \\ 109 & 110 & 111 & 115 \\ 97 & 97 & 110 & 32 \\ 103 & 116 & 32 & 109 \end{bmatrix} \quad (6)$$

Writing each element of P as an 8-bit binary string gives

$$P = \begin{bmatrix} 01001001 & \oplus & 01101001 & \oplus & 01101001 & \oplus & 01101001 \\ \oplus & & & & & & \\ 01101101 & \oplus & 01101110 & \oplus & 01101111 & \oplus & 01110011 \\ \oplus & & & & & & \\ 01100001 & \oplus & 01100001 & \oplus & 01101110 & \oplus & 00100000 \\ \oplus & & & & & & \\ 01100111 & \oplus & 01110100 & \oplus & 00100000 & \oplus & 01101101 \end{bmatrix} \quad (5)$$

Before multiplication by the key, the elements of P are combined through the chain of bitwise XOR operations given in (7). Within each row, every element is replaced by its XOR with the already updated element to its left, and the first element of each row is chained in the same way to the updated first element of the row above. No part of this step involves the key.

The resulting modified plaintext matrix is shown in (8), and its product with K modulo 256 in (9).

$$\begin{aligned} P_{11}^b &= P_{11}^b & P_{12}^b &= P_{11}^b \oplus P_{12}^b & P_{13}^b &= P_{12}^b \oplus P_{13}^b & P_{14}^b &= P_{13}^b \oplus P_{14}^b \\ P_{21}^b &= P_{11}^b \oplus P_{21}^b & P_{22}^b &= P_{21}^b \oplus P_{22}^b & P_{23}^b &= P_{22}^b \oplus P_{23}^b & P_{24}^b &= P_{23}^b \oplus P_{24}^b \\ P_{31}^b &= P_{21}^b \oplus P_{31}^b & P_{32}^b &= P_{31}^b \oplus P_{32}^b & P_{33}^b &= P_{32}^b \oplus P_{33}^b & P_{34}^b &= P_{33}^b \oplus P_{34}^b \\ P_{41}^b &= P_{31}^b \oplus P_{41}^b & P_{42}^b &= P_{41}^b \oplus P_{42}^b & P_{43}^b &= P_{42}^b \oplus P_{43}^b & P_{44}^b &= P_{43}^b \oplus P_{44}^b \end{aligned}$$

$$P = \begin{bmatrix} 73 & 32 & 73 & 32 \\ 36 & 74 & 37 & 86 \\ 69 & 36 & 74 & 106 \\ 34 & 86 & 118 & 27 \end{bmatrix} \quad (10)$$

$$C = KP \text{ mod } 256 = \begin{bmatrix} 11 & 128 & 183 & 163 \\ 72 & 246 & 232 & 92 \\ 23 & 0 & 130 & 165 \\ 252 & 130 & 159 & 97 \end{bmatrix} \quad (9)$$

Each element of C in (9) is then written as an 8-bit binary string:

$$C = \begin{bmatrix} 00001011 & 10000000 & 10110111 & 10100011 \\ 01001000 & 11110110 & 11101000 & 01011100 \\ 00010111 & 00000000 & 10001000 & 10100101 \\ 11111100 & 10000010 & 10011111 & 01100001 \end{bmatrix} \quad (12)$$

A left circular shift of 4 bits is applied column-wise, giving

$$C = \begin{bmatrix} 10110100 & 00001111 & 01111110 & 00110101 \\ 10000001 & 01100000 & 10001000 & 11001010 \\ 01111111 & 00001000 & 10001001 & 01010110 \\ 11001000 & 00101011 & 11111010 & 00010000 \end{bmatrix} \quad (13)$$

The elements of (11) are concatenated into a single bit string:

1011010010000001011111110010000001111011000000
00010000010101101111101000100010001001111101000
110101110010100101011000010000

This string is partitioned into substrings of 6 bits each:

$$101101 \ 001000 \ 000101 \ 111111 \ 110010 \ 000000 \quad (14)$$

$$111101 \ 100000 \ 000010 \ 000010 \ 101101 \ 111110$$

$$100010001000 \ 100111 \ 111010 \ 001101 \ 011100$$

$$101001 \ 010110 \ 000100 \ 000000$$

Four zero bits are appended so that the length of the string is a multiple of 6. Each 6-bit group is then converted to its decimal value, giving the Radix-64 indices

$$C = \begin{bmatrix} 45 & 50 & 2 & 34 & 13 & 4 \\ 8 & 0 & 2 & 8 & 28 & 0 \\ 5 & 61 & 45 & 39 & 41 & \\ 63 & 32 & 62 & 58 & 22 & \end{bmatrix} \quad (7)$$



Mapping these indices to their Radix-64 characters yields the final ciphertext

$$C = \text{tIF/yA9gCCt+iIn6NcpWEA} \quad (15)$$

Decryption applies the inverse of each of these steps in reverse order: Radix-64 decoding and removal of the padding bits, the inverse circular shift, multiplication by K^{-1} modulo 256 and, finally, reversal of the XOR chain.

III. THE CRYPTANALYTIC ATTACK

The aim of the attack is to recover the key matrix K together with its inverse K^{-1} modulo 256.

Cryptanalytic attacks are conventionally classified according to the information available to the adversary:

- Brute-force (ciphertext-only) attack.
- Known-plaintext attack.
- Chosen-plaintext attack.
- Chosen-ciphertext attack.

In a ciphertext-only setting the analyst possesses nothing but ciphertext. The brute-force approach is to decrypt it under every possible combination of key-matrix elements and to retain the key that yields the most coherent plaintext. In a known-plaintext attack the analyst also holds the plaintext corresponding to the intercepted ciphertext, and the task reduces to finding the combination of key elements that maps the one onto the other. In a chosen-plaintext attack the analyst selects plaintexts, crafted to expose weaknesses of the algorithm, and obtains their encryptions. A chosen-ciphertext attack is the mirror image: the analyst submits ciphertexts of their own choosing, again designed to exploit the shortcomings of the cipher, and obtains the corresponding plaintexts. In each case the key is then inferred from the resulting plaintext-ciphertext pairs.

The classical Hill cipher is vulnerable to the known-plaintext attack, and the additional operations of the Target Cipher were introduced to address this. They do not, however, protect the cipher when the analyst works in the reverse direction, starting from a ciphertext of their own choosing. This is the weakness exploited below.

The attack rests on two observations. First, the operations that surround the key multiplication, namely the XOR chain on the input side and the circular shift and Radix-64 encoding on the output side, are fixed and independent of the key; anyone can compute them and their inverses. Second, once these layers are set aside, decryption reduces to the linear map $X \mapsto K^{-1}X \pmod{256}$. An adversary who controls the block that enters this map can therefore choose it so that the map itself reveals K^{-1} .

We assume only that the adversary can submit a ciphertext to the legitimate holder of the key and obtain the corresponding plaintext; no knowledge of K is required. The attack proceeds as follows.

The adversary submits the ciphertext whose Radix-64 indices are given in (16) and requests the corresponding plaintext.

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (16)$$

Writing each index as a 6-bit binary string and concatenating the results gives

$$C = 000000\ 010000\ 000000\ 000000\ 000000\ 000000\ 000001\ 000000\ 000000\ 000000\ 000000\ 000000\ 000100\ 000000\ 000000\ 000000\ 000000\ 000000\ 010000$$

The final four zeros are the padding introduced during Radix-64 encoding. Discarding them and regrouping the remaining bits into 8-bit strings yields

$$C = \begin{bmatrix} 00000001 & 00000000 & 00000000 & 00000000 \\ 00000000 & 00000001 & 00000000 & 00000000 \\ 00000000 & 00000000 & 00000001 & 00000000 \\ 00000000 & 00000000 & 00000000 & 00000001 \end{bmatrix} \quad (17)$$

whose decimal form is the 4×4 identity matrix:

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (18)$$

Since the key stage of decryption multiplies its input by K^{-1} modulo 256, this ciphertext is mapped to $K^{-1}I = K^{-1}$. The only processing applied afterwards is the reversal of the XOR chain, which involves no secret; the adversary therefore reapplies the forward chain (7) to the returned plaintext and recovers K^{-1} exactly. The key matrix K is then obtained by inverting K^{-1} modulo 256, and the cipher is broken with one decryption query and negligible computation.

IV. CONCLUSIONS

Apart from multiplication by the key matrix, none of the operations introduced in the Target Cipher depends on secret information. The XOR chain applied before the key multiplication can be recomputed by anyone who knows the plaintext, which is a reasonable assumption for the attack models considered here. The circular shift and Radix-64 encoding applied afterwards can be recomputed or inverted just as easily. In effect, these layers are a public re-encoding of the input and output of the classical Hill cipher, and they leave its linear core exposed.

The Target Cipher is therefore open to cryptanalysis; as Section III shows, a single chosen ciphertext suffices to recover its key. We recommend adding a substitution stage either before or after the Radix-64 transformation. Such a stage would sever the direct relationship between the data entering and leaving the key-matrix multiplication, making the cipher considerably more robust against attacks of the kind presented here. For this remedy to be effective, the substitution should itself depend on the key: a fixed, public substitution could be inverted by the adversary in exactly the same way as the operations already present.



REFERENCES

- [1] J. R. Paragas, A. M. Sison and R. P. Medina, "Hill Cipher Modification: A Simplified Approach," 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 2019, pp. 821-825, doi: 10.1109/ICCSN.2019.8905360.
- [2] L.S.Hill, "Cryptography in an algebraic alphabet" American Mathematical Monthly, 1929, 36(6): 306-312.
- [3] Levine, Jack. "Some Elementary Cryptanalysis of Algebraic Cryptography." American Mathematical Monthly 68(5): 411-18.
- [4] 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
- [5] 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.
- [6] 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.
- [7] 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.
- [8] Boshra H. Makar, "Application of a Certain Class of Infinite Matrices to the Hill Cryptographic System", Cryptologia, January 1983, 7(1):63-78.
- [9] Jack Levine, Richard Chandler, "The Hill Cryptographic System with Unknown Cipher Alphabet, But Known Plaintext", Cryptologia, January 1989, 13(1):1-28.
- [10] Bhimbudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, "Novel Modified Hill Cipher Algorithm", Proceedings of ICETAETS, 2008, pp. 126-130.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] 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 (IJCSSE), 13(1):208-220.
- [18] 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.
- [19] 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.
- [20] 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
- [21] N.Ravi Shankar "A Novel Block Cipher with the Blending of the Hill Cipher and the Playfair Cipher", Journal of Xidian University, 16(1):207-217.
- [22] 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, 2(1): pp 35-43, January, 2011.
- [23] 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, vol.13, no.3, 2013, pp.50-63.
- [24] N. Ravi Shankar. "A Modified Hill Cipher Involving Key Dependent Permutation, Interlacing and Iteration", Communicated for publication.
- [25] 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, 1(2): 45-53, November, 2010.
- [26] N.Ravi Shankar, "A Large Block Cipher with the Blending of the Hill Cipher and the Playfair", Journal of Xidian University, 16(1):232-242.