Augmented Hill Cipher

AbdAllah A. ElHabshy

(Corresponding author: AbdAllah A. ElHabshy)

Mathematics Department, Al-Azhar University, Faculty of Science, 11884, Nasr City, Cairo, Egypt

(Email: AbdAllah@Azhar.edu.eg)

(Received Mar. 19, 2018; Revised and Accepted Aug. 18, 2018; First Online Jan. 22, 2019)

Abstract

Securing data over an open network is one of the most critical problems in network security. To secure data, an encryption algorithm should be used. Hill cipher is one of most famous encryption algorithms. Although the Hill cipher is not strong enough and vulnerable to many types of attacks, it is still playing a significant role in educational systems; The original Hill cipher is vulnerable to known plaintext attack. In the last decade, Hill cipher got much attention. Researchers proposed many enhances to the Hill cipher; New modifications of the Hill cipher are proposed to enhance the security of Hill cipher. In this paper we shall show that "A Modified Hill Cipher Based on Circulant Matrices" is vulnerable to both known plaintext attack and chosen plaintext attack. Moreover, we will introduce a new mode of operation which can be used with any block cipher. Then we will propose a new enhanced encryption algorithm. After that, we shall provide a security analysis and efficiency evaluation for our new encryption algorithm.

Keywords: Cryptanalysis; Data Encryption; Hill Cipher; Mode of Operations; Semi Cipher Block Chaining

1 Introduction

Hill cipher was developed by Lester Hill in 1929 [8]. It is a polyalphabetic substitution cipher based on linear algebra. Unfortunately, Hill cipher is vulnerable to known plaintext attack. In time, many versions of Hill cipher are proposed to overcome its security flaws. The idea of Hill cipher is to take m successive plaintext letters and substitutes for them m ciphertext letters [24]. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, ..., z = 25). For $m =$ 3, the system can be described as **C**=**PK** *mod* 26, where **C** and **P** are 3×3 matrices representing the ciphertext and plaintext respectively, and **K** is an invertible 3×3 matrix representing the encryption key. Operations are performed in mod 26. The biggest strength of Hill cipher is that it completely hides the $(m-1)$ letters frequency information. But unfortunately, it is vulnerable to known plaintext attack. Nevertheless, Hill cipher serves a significant educational role in teaching cryptographic principles, due to its simplicity [17]. Moreover, Hill cipher is used to enhance the security in many systems [4, 9, 19, 23].

The rest of this paper is organized as follows. Section 2 presents the related works. Section 3 illustrates the cryptanalysis of Reddy *et al.* cryptosystem. Section 4 proposes a new mode of operations in bock cipher, namely, Semi-Cipher Block Chaining; Semi-CBC, in short, which inspires the shape of our new cipher. Section 5 proposes our new enhanced Hill Cipher; namely, Augmented Hill Cipher (AHC). Section 6 shows the security analysis of AHC. Section 7 investigates the performance evaluation of AHC. Finally, Section 8 presents the conclusion.

2 Related Work

Hill cipher has been getting much attention since last decade. There are many research papers which proposed an enhanced Hill Cipher [1, 2, 10–13, 16, 22].

Affine-Hill Cipher is a variant of Hill Cipher, which adds a nonlinear affine transformation to Hill Cipher [25]; **C**= (**PK**+**V**) *mod* n, where **V** is $m \times m$ constant matrix. If $m = 8$ and $n = 2^{16}$, then the key space of Affine-Hill cipher is corresponding to 2046-bit key. This can be proven as follows: If $n = p^k$ where p is a prime, then the number of invertible $m \times m$ matrices over $\mathbb{Z}_n$ is $p^{(k-1)m^2} \prod_{i=0}^{m-1} \left(p^m - p^i\right)$ [18]. In the case of $m =$ 8 and $n = 2^{16}$, the number of invertible matrices (which can be used as a secret key, **K**) over $n = 2^{16}$ is $2^{(16-1)8^2} \prod_{i=0}^{7} \left(2^8 - 2^i\right) = 5.21186 \times 10^{307}$. Since $\log_2 \left(5.21186 \times 10^{307}\right) = 1022.21$, (which corresponds to a 1022-bit key). Also, the number of matrices which can be used as a secret key **V** is $m^2 \times \log_2 n = 64 \times 16 = 1024$ bit. Consequently, the key space of Affine-Hill Cipher is corresponds to 1022+1024 = 2046-bit key.

According to [15], A symmetric cryptosystem provides k-bit security if the brute force attack takes on average 2^{k-1} operations to break this cryptosystem. So, Affine-Hill cipher provides 2046-bit security.

As a side note, Affine-Hill cipher is vulnerable to chosen plaintext attack; if $\mathbf{P_1}$=**0**, then $\mathbf{C_1}$=**V**. And, if $\mathbf{P_2}$=**I**, then $\mathbf{C_2}$= (**K**+$\mathbf{C_1}$) mod n; *i.e.* **K**= ($\mathbf{C_2}$−$\mathbf{C_1}$) mod n.

Moreover, once **V** is known, then we return to original Hill cipher, which is vulnerable to known plaintext attack, which means that Affine-Hill cipher is vulnerable to known plaintext attack; the known plaintext attack on Affine-Hill cipher can be demonstrated as follows: If the adversary knows the two ciphertexts **C**, $\mathbf{C}'$and the two corresponding plaintexts **P,** $\mathbf{P}'$such that $(\mathbf{P}-\mathbf{P}')$ mod n is invertible matrix, then $(\mathbf{C}-\mathbf{C}') = (\mathbf{P}-\mathbf{P}')\mathbf{K}$ mod n; *i.e.*$\mathbf{K} = (\mathbf{P}-\mathbf{P}')^{-1}(\mathbf{C}-\mathbf{C}')$ mod n. Now **V** can be computed such that **V**= (**C**−**PK**) *mod* n.

In 2012, Reddy *et al.* [20] presented a variant of Hill Cipher; this cipher is based on circulant matrices. A circulant matrix is a special kind of matrices in which every row of the matrix is a right cyclic shift of the row above it [7]. Moreover, a prime circulant matrix is $m \times m$ circulant matrix in which any two elements in the same row are coprimes.

If G is a non-singular 2×2 matrix such that

$$\mathrm{G} = \begin{bmatrix} \mathrm{a}_{11} & \mathrm{a}_{12} \\ \mathrm{a}_{21} & \mathrm{a}_{22} \end{bmatrix}$$

then $\mathrm{G_c}$ is 4×4 matrix G_c, where

$$\mathrm{G_c}= \begin{bmatrix} \mathrm{a}_{11} & \mathrm{a}_{12} & \mathrm{a}_{21} & \mathrm{a}_{22} \\ \mathrm{a}_{22} & \mathrm{a}_{11} & \mathrm{a}_{12} & \mathrm{a}_{21} \\ \mathrm{a}_{21} & \mathrm{a}_{22} & \mathrm{a}_{11} & \mathrm{a}_{12} \\ \mathrm{a}_{12} & \mathrm{a}_{21} & \mathrm{a}_{22} & \mathrm{a}_{11} \end{bmatrix}$$

At the beginning, parties agree upon a non-singular matrix A over $GF(p)$ as a secret key where p is a prime, and a non-singular $m \times m$ matrix G over $GF(p)$ as a public key, such that the determinant of the coefficient matrix $\mathrm{G_c}$ is zero; *i.e.*$|\mathrm{G_c}| = 0$. Then parties could compute the secret key $\mathrm{K} = \mathrm{AGA}^{-1}$ mod p. Then the encryption and decryption processes can be described as follows:

Encryption process: $\mathrm{C} = \mathrm{KP}+\mathrm{A}^{\mathrm{T}}$ mod p, where C is $m \times m$ ciphertext matrix, P is $m \times m$ plaintext and A^{T} is the transpose of the secret matrix A.

Decryption process: P $=\mathrm{K}^{-1}\left(\mathrm{C}-\mathrm{A}^{\mathrm{T}}\right)$ mod p, where $\mathrm{K}^{-1} = \mathrm{AG}^{-1}\mathrm{A}^{-1}$ mod p.

To find the key space of Reddy *et al.* schema, we should find the number of invertible matrices which can be used as a secret key **A**. This because the key space depends only on the invertible secret matrix A. The number of $m \times m$ invertible matrices over $GF(p)$is $\prod_{i=0}^{m-1}\left(p^m - p^i\right)$ [18]. If $m = 8$ and $\lceil \log_2 p \rceil = 16$ (where $\lceil\rceil$ is ceiling operation, ceiling(x) = $\lceil \mathrm{x} \rceil$ is the least integer greater than or equal to x), then the key space of Reddy *et al.* is $\prod_{i=0}^{7}\left(p^8 - p^i\right) \cong \prod_{i=0}^{7}\left(\left(2^{16}\right)^8 - \left(2^{16}\right)^i\right) = 1.79767 \times 10^{308}$ which is approximately corresponding to 1024-bit key, since $\log_2\left(1.79767 \times 10^{308}\right) = 1023.99998$, *i.e.*Reddy *et al.* cryptosystem approximately provides 1024-bit security.

3 Cryptanalysis of "A Modified Hill Cipher Based on Circulant Matrices"

In this section we will show that Reddy *et al.* cryptosystem "A Modified Hill Cipher Based on Circulant Matrices" is vulnerable to both known plaintext and chosen plaintext attacks.

3.1 Known Plaintext Attack

Let $\mathrm{C}_1$and C_2 are two $m \times m$ known ciphertext matrices of the two $m \times m$ plaintext matrices P_1 and P_2 respectively. Then $\mathrm{C}_1 = \left(\mathrm{KP}_1+\mathrm{A}^{\mathrm{T}}\right)$ mod p and $\mathrm{C}_2 = \left(\mathrm{KP}_2+\mathrm{A}^{\mathrm{T}}\right)$ mod p thus $(\mathrm{C}_1 - \mathrm{C}_2)$ mod p $= \left(\mathrm{KP}_1+\mathrm{A}^{\mathrm{T}} - \mathrm{KP}_2 - \mathrm{A}^{\mathrm{T}}\right)$ mod p= $(\mathrm{K}(\mathrm{P}_1 - \mathrm{P}_2))$ mod p. Suppose $(\mathrm{C}_1 - \mathrm{C}_2)$ mod p=C' and $(\mathrm{P}_1 - \mathrm{P}_2)$mod p=P' thus $\mathrm{C}' = \mathrm{KP}'$mod p; *i.e.*$\mathrm{K} = \mathrm{C}'\mathrm{P}'^{-1}$ mod p. Thus, the secret key K is now known. Furthermore, since $\mathrm{C}_1 = \left(\mathrm{KP}_1+\mathrm{A}^{\mathrm{T}}\right)$ mod p, *i.e.*$\mathrm{A}^{\mathrm{T}} = (\mathrm{C}_1 - \mathrm{KP}_1)$ mod p. Consequently, we can get A^{T} and A. #

3.2 Chosen Plaintext Attack

Reddy *et al.* cryptosystem is also vulnerable to chosen plaintext attack. If the adversary can chose the plaintext matrix P as the $m \times m$ zero matrix;P $=\mathbf{0}$; *i.e.*every element in P is zero. Thus $\mathrm{C} = \left(\mathrm{KP}+\mathrm{A}^{\mathrm{T}}\right)$ mod p= $\left(\mathrm{K}\mathbf{0}+\mathrm{A}^{\mathrm{T}}\right)$ mod p=A^{T}mod p=A^{T}. Thus, now A^{T} is known, as well A. Furthermore, since G is public, the secret key $\mathrm{K} = \left(\mathrm{AGA}^{-1}\right)$ mod p can be computed#.

4 Semi Cipher Block Chaining (Semi-CBC) Mode

In this section we will introduce a new mode of operation which inspires the structure of our new cryptosystem. A mode of operation is a technique that used to magnify the impact of a block cipher. This technique determines if a block ciphertext could (could not) be effected by the previous plaintext(s).

Our new chaining mode (Semi Cipher Block Chaining Mode; Semi-CBC mode, in short) can be used with any block cipher. In encryption process of Semi-CBC mode, the output of encryption algorithm is XORed with a previous half-encrypted block to produce the ciphertext except the first block which is XORed with Initialization Key (IK), as illustrated in Figure 1.

While, in the decryption process of Semi-CBC mode, the output of decryption algorithm is XORed with a previous half-decrypted block to produce the plaintext, excluding the first block which is XORed with Initialization Key (IK), as illustrated in Figure 2.

The Initialization Key (IK) is a secret key. At communication's beginning, parties should agree upon an IK which could be the session key or an arbitrary secret key.

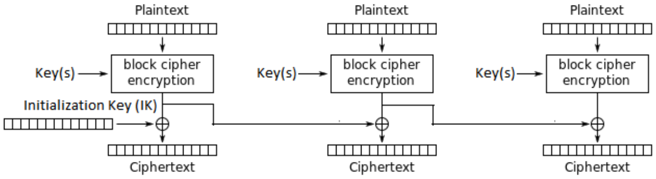

Figure 1: Semi-CBC encryption

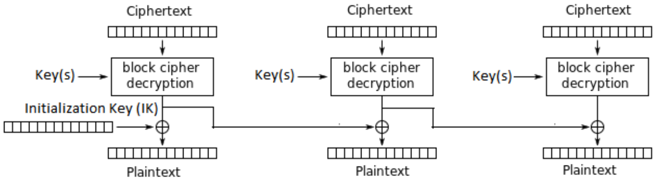

Figure 2: Semi-CBC decryption

Similar approaches are Electronic Code Book (ECB) Mode, Cipher Block Chaining (CBC) Mode, Cipher Feedback (CFB) Mode, Output Feedback(OFB) Mode, and Counter (CTR) Mode [24]. In this section we introduced a new mode of operation (Simi-CBC). Inspired by Simi-CBC we will propose the following cryptosystem, namely, Augmented Hill Cipher (AHC).

5 Augmented Hill Cipher

In this section, we shall present a new enhanced modified Hill Cipher. At the beginning of each session, parities agree upon three different random secret keys K_0, K_1 and K_2. Each one of the secret keys K_0, K_1, and K_2 is an invertible $m \times m$ matrix over $\mathbb{Z}_n$ where n is an integer. The integers m and n are security parameters.

5.1 Encryption Process

At the beginning, the plaintext should be divided into $P_0, P_1, P_2, P_3, \ldots, P_N$, where P_i is $m \times m$ matrix over an integer n and $i = 0, 1, 2, 3, \ldots,$ N. Each one of P_i is considered as a block of plaintext with length L, where L $=m^2 \times \lceil \log_2 n \rceil$ bits. If the length of plaintext is not multiple of L, consequently extra random bits (padding) should be added at the end of the plaintext; *i.e.*pad the last block (plaintext matrix) if necessary. This padding is the number of added bits written between two special delimiters, followed by these random bits. The plaintext matrices are initially filled column by column with the plaintext; *i.e.*the first $\lceil \log_2 n \rceil$ bits are filled into the cell at column1-raw1, the second $\lceil \log_2 n \rceil$ bits are filled into the cell at column1-raw2, and so forth. Afterwards, the $m \times m$ matrices of ciphertext $C_0, C_1, C_2, C_3, \ldots, C_N$ can be computed as follows:

$$C'_i = \left(K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}\right) \bmod n, \quad i = 0, 1, 2, \cdots, N$$

$$C_i = \begin{cases} C'_i \oplus K_2 & \text{if } i = 0 \\ C'_i \oplus C'_{i-1} & \text{if } i = 1, 2, \ldots, N \end{cases}$$

Figure 3 illustrates the encryption process of Augmented Hill Cipher.

The encryption algorithm of Augmented Hill Cipher can be described as follows:

Algorithm 1 AHC Encryption Algorithm

```
Input: $K_0, K_1, K_2, P_0, P_1, P_2, P_3, \ldots, P_N$
Output: $C_0, C_1, C_2, C_3, \ldots, C_N$
Begin
$C'_0 = (K_0 P_0 + K_1) \bmod n$
$C_0 = C'_0 \oplus K_2$
$i = 0$
while $i <= N$ do
    $C'_i = \left(K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}\right) \bmod n$
    $C_i = C'_i \oplus C'_{i-1}$
    $i = i + 1$
end while
End
```

5.2 Decryption Process

The corresponding plaintext P_i of the ciphertext C_i (where $i = 0, 1, 2, \ldots, N$) can be computed as follows:

$$C'_i = \begin{cases} C_i \oplus K_2 & \text{if } i = 0 \\ C_i \oplus C'_{i-1} & \text{if } i = 1, 2, \ldots, N \end{cases}$$

$$P_i = \left[K^{-1}_{i \bmod 3} * \left(C'_i - K_{(i+1) \bmod 3}\right)\right] \bmod n, \quad i = 0, 1, 2, \ldots N$$

Figure 4 illustrates the decryption process in Augmented Hill Cipher

Therefore, the decryption algorithm of Augmented Hill Cipher can be described as follows.

Algorithm 2 AHC Decryption Algorithm

```
Input: $K_0, K_1, K_2, C_1, C_2, C_3, \ldots, C_N$
Output: $P_0, P_1, P_2, P_3, \ldots, P_N$
Begin
$C'_0 = C_0 \oplus K_2$
$P_0 = [K_0^{-1} * (C'_0 - K_1)] \bmod n$
$i = 0$
while $i <= N$ do
    $C'_i = C_i \oplus C'_{i-1}$
    $P_i = [K^{-1}_{i \bmod 3} * (C'_i - K_{(i+1) \bmod 3})] \bmod n$
    $i = i + 1$
end while
End
```

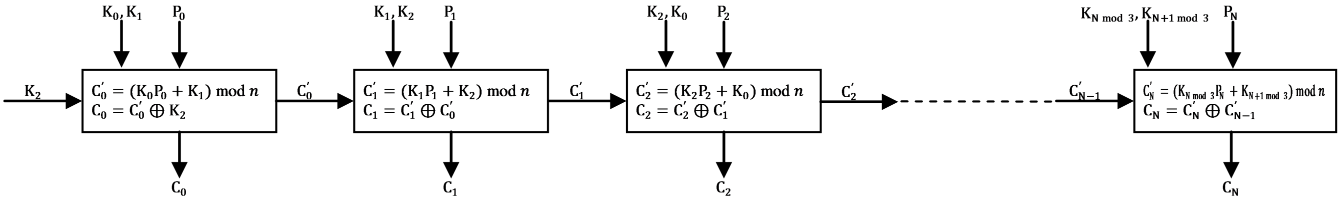
K_0, K_1
P_0
K_1, K_2
P_1
K_2, K_0
P_2
$K_{N \bmod 3}, K_{N+1 \bmod 3}$
P_N
K_2
$C_0' = (K_0P_0 + K_1) \bmod n$
$C_0 = C_0' \oplus K_2$
C_0'
$C_1' = (K_1P_1 + K_2) \bmod n$
$C_1 = C_1' \oplus C_0'$
C_1'
$C_2' = (K_2P_2 + K_0) \bmod n$
$C_2 = C_2' \oplus C_1'$
C_2'
C_{N-1}'
$C_N' = (K_{N \bmod 3}P_N + K_{N+1 \bmod 3}) \bmod n$
$C_N = C_N' \oplus C_{N-1}'$
C_0
C_1
C_2
C_N

Figure 3: The encryption process of augmented hill cipher

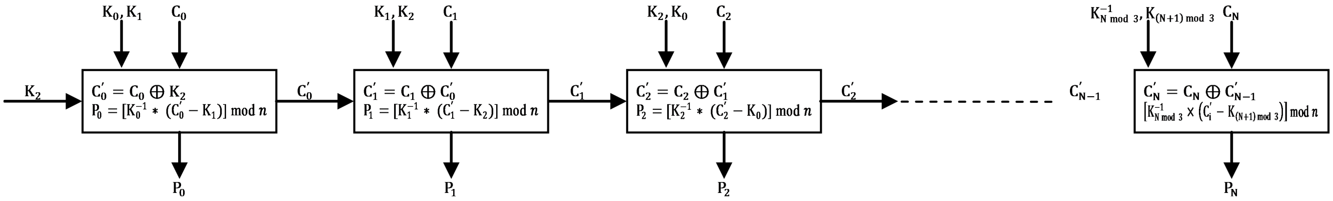
K_0, K_1
C_0
K_1, K_2
C_1
K_2, K_0
C_2
$K_{N \bmod 3}^{-1}, K_{(N+1) \bmod 3}$
C_N
K_2
$C_0' = C_0 \oplus K_2$
$P_0 = [K_0^{-1} * (C_0' - K_1)] \bmod n$
C_0'
$C_1' = C_1 \oplus C_0'$
$P_1 = [K_1^{-1} * (C_1' - K_2)] \bmod n$
C_1'
$C_2' = C_2 \oplus C_1'$
$P_2 = [K_2^{-1} * (C_2' - K_0)] \bmod n$
C_2'
C_{N-1}'
$C_N' = C_N \oplus C_{N-1}'$
$[K_{N \bmod 3}^{-1} \times (C_i' - K_{(N+1) \bmod 3})] \bmod n$
P_0
P_1
P_2
P_N

Figure 4: The decryption process of augmented hill cipher

5.3 Security Parameters and Keyspace

As mentioned before in this section, m and n are security parameters, which mean the security of AHC depends on the values of m and n. The values of m and n are chosen according to the desired security for the system. This means, if we choose m and n with large values, then the system not only gain strength (i.e. be more secure system), but also loses its efficiency (i.e. inefficient encryption and decryption processes). In other words, the larger values we chose for m and n, the more secure and slow system we get. To obtain secure and efficient system, we should compromise in order to choose the optimal values of m and n (i.e. the values of m and n depend upon efficiency–security tradeoff). A smart agent (an optimizer) can be used to automatically choose the optimal values of m and n according to the level of security needed as well as the available device resources. ACH intended to be used in mobile phones and other small devices with limited resources such as wearable technology, e.g. Wireless Body Area Network (WBAN) devices [5,14,21]. So, as instance of AHC, we can choose $m = 8$ and $n = 2^{16}$. In this case, each plaintext (or ciphertext) contains $8^2 \times \lceil \log_2 2^{16} \rceil = 64 \times 16 = 1024$ bits, where $\lceil\rceil$ is ceiling operation, ceiling(x) = $\lceil x \rceil$ is the least integer greater than or equal to x. So, there are $2^{1024} = 1.79769 \times 10^{308}$ different plaintext/ciphertext pairs. So, in this case, AHC provides 3066-bit security.

As mentioned in Section 2, the number of invertible $m \times m$ matrices over $n = p^k$ is $p^{(k-1)m^2} \prod_{i=0}^{m-1} (p^m - p^i)$ [18]. In the case of $m = 8$ and $n = 2^{16}$, the number of invertible matrices over $n = 2^{16}$ is $2^{(16-1)8^2} \prod_{i=0}^{7} (2^8 - 2^i) = 5.21186 \times 10^{307}$, which corresponds to a 1022-bit key. Then in this case, keyspace of each matrix key $(\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2)$ is equivalent to the keyspace of a system use key of length 1022 bits. Since ACH uses three different keys, then the keyspace of AHC is equivalent to the keyspace of a system use key of length $3 * 1022 = 3066$ bits, *i.e.*the keyspace of this version of AHC is $2^{3066} = 9.0775 \times 10^{922}$ key.

6 Security Analysis

AHC guarantees the most desirable attributes of symmetric ciphers; namely, Avalanche Effect (any small changes in plaintext cause a great change in ciphertext) and Completeness (each bit of the ciphertext depends on many bits of the plaintext). These two attributes make AHC very strong cipher; resists all types of attacks. Additionally, AHC has built-in flexibility of key length (depending on the values given to m and n). So, there is a degree of 'future proofing' against progressing of computer ability to perform exhaustive key searches. Moreover, the advantage of using both $+$ and $\oplus$ operations together in AHC is that they do not commute [24], which hardness the cryptanalysis of AHC.

There are many types of attacks on any cryptosystem such as Ciphertext Only Attack (COA), Known Plaintext Attack (KPA), Chosen Plaintext Attack (CPA), Dictionary Attack, Brute Force Attack (BFA), and Fault Analysis Attacks (FAA). In this section we shall discuss the security of our cryptosystem, and prove that it is immune to all kind of these attacks.

In this section we assume that, $m = 8$ and $n = 2^{16}$, this means 2^{1024} different pairs of plaintext/ciphertext, and a keyspace equals to $2^{3066} = 9.0775 \times 10^{922}$ key.

6.1 Ciphertext Only Attack (COA)

In this type of attack, an adversary has access to a collection of ciphertexts. The adversary does not know the corresponding plaintexts. The cryptosystem is vulnerable to COA if the adversary can determine the corresponding plaintext of any ciphertext.

So, in this case, an adversary should search for a plaintext (which is corresponding to a specific ciphertext) in $m^2 \times \log_2 n = 2^{1024} = 1.79769 \times 10^{308}$ different values ($m \times m$ matrices). Doing this is practically impossible with the fastest computer on the earth. According to [26], the fastest computer has speed equals to 122.3 PFLOPS $\cong 10^2.087$ PFLOPS= $10^{17.087}$ FLOPS (FLOPS or flops ;an acronym for FLoating-point Operations Per Second). The FLOPS is used to measure the computer performance.

To prove this, let us consider a computer with a speed of EFLOPS $= 10^3$ PFLOPS $= 10^{18}$ FLOPS (there is no announcement of creating such computer). In other words, let us consider the fastest computer on the earth can do 10^{18} FLOPS. In a billion year, there are 3.15576×10^{16} seconds[1]. Then, this computer can perform $10^{18}_{\text{FLOPS}} \times 3.15576 \times 10^{16} = 3.15576 \times 10^{34}$ operations per billion years. Let us consider that, the operation means to decrypt the ciphertext and compare it with all the possible plaintexts to get the correct secret keys. Then this computer needs time $= \frac{1.79769 \times 10^{308}}{3.15576 \times 10^{34}} = 5.69653 \times 10^{273}$ billion years to do this attack; a much greater time than the universe age. According to last announcement in 2013, the age of the universe = 13.8 billion year [3]. For generic purposes, let us consider a computer with speed = 10^u FLOPS, then the computer can perform $10^u_{\text{FLOPS}} \times 3.15576 \times 10^{16} = 3.15576 \times 10^{16+u}$ operations per billion years. So, to break AHC, this computer needs time $BT = \frac{2^{(m^2 \times \log_2 n)}}{3.15576 \times 10^{16+u}}$ billion years. Thus, BT should be much greater than 1; $i.e. BT \gg 1$. So, if u gets bigger (the computer speed is upgraded), then the security parameters m and n should be enlarged in order to maintain the security of AHC.

6.2 Known Plaintext Attack (KPA)

In this type of attack an adversary knows the corresponding plaintexts for some ciphertexts, *i.e.*the adversary knows some pairs of (plaintext, ciphertext). In this case the attacker tries to figure out the key using plaintext-ciphertext pairs and the nature of cryptosystem.

In our cryptosystem we hide any relationship between the plaintext and its corresponding ciphertext. Let us consider that the adversary has ($\mathrm{P_{i-1}}$, $\mathrm{P_i}$ and $\mathrm{C_{i-1}}$, $\mathrm{C_i}$). Since $\mathrm{C_i{=}C'_i \oplus C'_{i-1}}$ and $\mathrm{C'_i} = \left(\mathrm{K_{i \bmod 3}\, P_i + K_{(i+1) \bmod 3}}\right)$ mod n then $\mathrm{C_i} = \left(\left(\mathrm{K_{i \bmod 3}\, P_i + K_{(i+1) \bmod 3}}\right) \bmod n\right) \oplus \left(\left(\mathrm{K_{(i-1) \bmod 3}\, P_{i-1} + K_{i \bmod 3}}\right) \bmod n\right)$. Although the adversary has $\mathrm{P_{i-1}}$, and $\mathrm{P_i}$ he/she has no clue of the secret keys $\mathrm{K_0}$, $\mathrm{K_1}$and $\mathrm{K_2}$.

6.3 Chosen Plaintext Attack (CPA)

In this type of attack the adversary chooses the plaintext to be encrypted. In other words, the adversary has the power to choose the plaintext-ciphertext pairs. Sometimes, this attack could help the adversary to gain the secret key(s).

In Augmented Hill Cipher, consider that the adversary chooses a small plaintext such that $\mathrm{P} = \mathrm{P_0} = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix. Then the ciphertext should be $\mathrm{C} = \mathrm{C_0} = \mathrm{K_1 \oplus K_2}$. So, the adversary still has no clue about $\mathrm{K_1}$ or $\mathrm{K_2}$. Also, if the adversary chooses a plaintext such that $\mathrm{P} = \mathrm{P_0} = \mathbf{I}$, where $\mathbf{I}$ is the identity matrix. Then the ciphertext should be $\mathrm{C} = \mathrm{C_0} = (\mathrm{K_0 + K_1}) \bmod n \oplus \mathrm{K_2}$. In other words, the adversary still does not have any information about $\mathrm{K_0}, \mathrm{K_1}$ or $\mathrm{K_2}$. Even if he/she XOR the first ciphertext with the second one to gain a new furmula, *i.e.* $[\mathrm{K_1 \oplus K_2}] \oplus [(\mathrm{K_0 + K_1}) \bmod n \oplus \mathrm{K_2}] = \mathrm{K_1 \oplus K_2 \oplus} (\mathrm{K_0 + K_1}) \bmod n \oplus \mathrm{K_2} = \mathrm{K_1} \oplus (\mathrm{K_0 + K_1}) \bmod n$. Clearly, the adversary has no idea about the secret keys $\mathrm{K_0}$, $\mathrm{K_1}$ or $\mathrm{K_2}$. So, our cryptosystem resists the chosen plaintext attack.

6.4 Dictionary Attack (DA)

In this type of attack, the adversary builds a dictionary of plaintext-ciphertext pairs which have been obtained over a period of time. In our new cipher, to build such dictionary, the adversary needs to know each possible plaintext (with any length) and its corresponding ciphertext. In our new cipher, if only one bit is changed in a plaintext, the corresponding ciphertext will change too. Also, the keys are changed in each session, *i.e.*in AHC, the keys are session keys which means they change in each session. So, it is impossible for adversary to build such dictionary.

6.5 Brute Force Attack (BFA)

In this type of attacks, the adversary tries all possible keys until she\he finds the correct keys $\mathrm{K_0}$,$\mathrm{K_1}$ and $\mathrm{K_2}$. As we dissected before in this section, if we let $m = 16$, and $n = 2^{16}$, and the number of possible keys is $2^{3066} = 9.0775 \times 10^{922}$ key. As we prove in COA attack, it is impossible for an adversary to try all these possible keys.

6.6 Fault Analysis Attacks (FAA)

In this type of attack, the adversary tries to take advantage of any error in designing the cryptosystem, in order to crack the system. As we discussed in this section, ACH is immune to COA, KPA, CPA, DA, and BFA attacks. Moreover, ACH is similar to a block cipher with Semi-CBC mode which has been presented is Section 4. This means that the value of each block of ciphertext depends on all the previous plaintexts. In other words, our new cipher is well thoughtful and all possible attacks are considered when we design this cryptosystem. So AHC is immune to fault analysis attacks.

7 Performance Evaluation

In this section we present a complexity analysis for AHC. Then we present a brief comparative study among AHC

[1] $60_{\text{Seconds}} \times 60_{\text{Minutes}} \times 24_{\text{Hours}} \times 365.25_{\text{Days}} \times 1000_{\text{Years}} \times 1000_{\text{Thousand Years}} \times 1000_{\text{Billion Years}} = 3.15576 \times 10^{16}$ *seconds*

Table 1: Comparison among AHC and some other existing algorithms

Algorithm	Attacks		Key Space	
	Chosen Plaintext attack	Known Plaintext attack	provides k-bit security	Remark; $m = 8$
Original Hill Cipher	Yes	Yes	1022-bit key	$n = 2^{16}$
Affine-Hill Cipher	Yes	Yes	2046-bit key	$n = 2^{16}$
Reddy *et al.* Cipher	Yes	Yes	1024-bit Key	$n = p$ sit $\lceil \log_2 p \ \rceil = 16$
Augmented Hill Cipher	No	No	3066-bit key	$n = 2^{16}$

and some variants of Hill cipher. Thereafter, we will show the advantages of AHC.

7.1 Complexity Analysis

Time Complexity: According to [6], the time complexity of matrix multiplication is $O(m^{2.373})$, where m is the degree of the matrix. Also, the time complexity of adding two matrices is $O\left(m^2\right)$, Moreover, the time complexity of XOR two matrices is $O\left(m^2\right)$. Thus, the total time complexity of AHC is $O\left(m^{2.373}\right) + \left(2 \times O\left(m^2\right)\right) \cong O\left(m^{2.373}\right)$; *i.e.*the complexity of AHC is $O\left(m^{2.373}\right)$ which is equals to the complexity of the original Hill Cipher.

Space Complexity: Since each matrix needs a space of $m^2 \times \lceil \log_2 n \ \rceil$ bits to be stored in the system, thus AHC needs space of $6 \times m^2 \times \lceil \log_2 n \ \rceil$ bits. This because AHC needs to store three keys $\mathrm{K}_0, \mathrm{K}_1$,K_2 and two matrices to hold plaintext and ciphertext, in addition to a matrix to hold $\mathrm{C}'_{\mathrm{i}-1}$; the previous half encrypted plaintext. In the instance of AHC described in Section 5.3, in which $m = \ 8$ and $n = 2^{16}$, each matrix needs 1024bits = 128 byte to be stored; *i.e.*AHC needs memory space equals to $6 \times m^2 \times \lceil \log_2 n \ \rceil = 6 \times 1024\ bits = 6 \ \times 128\ byte = 768\ byte$ less than 1 KB.

7.2 Comparative Study

Table 1 presents a brief comparison between AHC and other algorithms such as Hill Cipher, Affine-Hill Cipher, and Reddy *et al.* Cipher. As shown in Table 1, the key space of Hill Cipher is corresponding to 1022-bit key if $m = 8$ and $n = 2^{16}$, this is because the secret matrix of Hill Cipher should be invertible matrix; i.e., in this case, Hill Cipher provides 1022-bit secuiry.

The complexity of all these cryptosystems is $O\left(m^{2.373}\right)$ [6], which is equal to the complexity of matrix multiplication.

7.3 Advantages of AHC

AHC is a promising encryption algorithm, which provides many advantages. These advantages can be described as follows.

7.3.1 Security Advantages

- The keyspace is very large; 2^{3066} key, which prevents any type of the brute force attack.
- Ensures the Avalanche Effect (any small changes in plaintext causes a great change in ciphertext) and Completeness (each bit of the ciphertext depends on many bits of the plaintext).
- Evolves with computer speed.
- Multiple encryption with AHC (with the same or different keys) can be implemented in order to achieve a higher level of security. Using Multiple encyption with AHC will increase the effects of desirable features such as conffution and diffusion.

7.3.2 Performance Advantages

- Very fast encryption and decryption algorithms; time complexity $= \mathrm{O}(\mathrm{m}^{2.373})$.
- Each matrix is considered as a block of 1024 bits = 1 Kib, which makes it easy to divide the plaintext and to estimate the number of matrices $(\mathrm{N}+1)$ that form the plaintext.

8 Conclusions

In this paper we have shown that Reddy *et al.* Cipher is vulnerable to both chosen plaintext and known plaintext attack. Then we presented a new mode of operations of block ciphers, which inspires the schema of our new cryptosystem. After that, we proposed a new variant of Hill Cipher, namely Augmented Hill Cipher (AHC). To support AHC we presented a security analysis and performance evaluation of AHC. We have shown that AHC resists all kinds of attacks. Also, we have proven that, AHC has much greater key space than original Hill Cipher, which is corresponding to 3066-bit key although the complexity of AHC is almost the same with other variant of Hill Cipher.

Acknowledgments

I would like to thank Porf. Kamal ElDahshan for his kind help and support during this research.

References

[1] M. N. AbdElRahman *et al.*, "Cryptography: A new approach of classical hill cipher," *International Journal of Security and Its Applications*, vol. 7, no. 2, pp. 179–190, 2013.

[2] A. S. Al-Khalid and A. O. Al-Khfagi, "Cryptanalysis of a hill cipher using genetic algorithm," in *World Symposium on Computer Networks and Information Security (WSCNIS'15)*, pp. 1–4, 2015.

[3] C. L. Bennett *et al.*, "Nine-year wilkinson microwave anisotropy probe (WMAP) observations: Final maps and results," *in Cosmology and Nongalactic Astrophysics Cornell University: NY , United States*, pp. 1–177, 2013.

[4] P. Praveenkumar *et al.*, "Fusion of confusion and diffusion: A novel image encryption approach," *Telecommunication Systems*, vol. 65, no. 1, pp. 65–78, 2017.

[5] S. Farooq, D. Prashar, and K. Jyoti, "Hybrid encryption algorithm in wireless body area networks (WBAN)," in *Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing*, pp. 401–410, vol. 624, 2018.

[6] F. L. Gall, "Powers of tensors and fast matrix multiplication," in *The 39th International Symposium on Symbolic and Algebraic Computation (ISSAC'14)*, pp. 296–303, 2014.

[7] R. M. Gray, "Toeplitz and circulant matrices: A review," *Foundations and Trends® in Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.

[8] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929.

[9] R. Jothi and A. Ojha, "On multi-secret sharing using hill cipher and random grids," in *International Conference on Advances in Computer Engineering and Applications*, pp. 683–687, 2015.

[10] L. Keliher and A. Z. Delaney, "Cryptanalysis of the toorani-falahati hill ciphers," in *IEEE Symposium on Computers and Communications (ISCC'13)*, pp. 436–440, 2013.

[11] L. Keliher and S. Thibodeau, "Slide attacks against iterated hill ciphers," in *Security in Computing and Communications: International Symposium*, pp. 179–190, 2013.

[12] A. A. M. Khalaf, M. S. A. El-karim, and H. F. A. Hamed, "Proposed triple hill cipher algorithm for increasing the security level of encrypted binary data and its implementation using fpga," in *17th International Conference on Advanced Communication Technology (ICACT'15)*, pp. 454–459, 2015.

[13] S. Khazaei and S. Ahmadi, "Ciphertext-only attack on d x d hill in o(d13^d)," *Information Processing Letters*, vol. 118, pp. 25–29, 2017.

[14] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Networks*, vol. 70, no. 1, pp. 23–43, 2018.

[15] A. K. Lenstra, "Unbelievable security: Matching AES security using public key systems," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 67–86, 2001.

[16] R. Mahendran and K. Mani, "Generation of key matrix for hill cipher encryption using classical cipher," in *World Congress on Computing and Communication Technologies (WCCCT'17)*, pp. 51–54, 2017.

[17] A. McAndrew, "Using the hill cipher to teach cryptographic principles," *International Journal of Mathematical Education in Science and Technology*, vol. 39, no. 7, pp. 967–979, 2008.

[18] J. Overbey, W. Traves, and J. Wojdylo, "On the keyspace of the hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

[19] K. H. S. Ranjan *et al.*, "A survey on key(s) and keyless image encryption techniques," *Cybernetics and Information Technologies*, vol. 17, no. 4, pp. 134–164, 2017.

[20] K. A. Reddy *et al.*, "A modified hill cipher based on circulant matrices," *Procedia Technology*, vol. 4, pp. 114–118, 2012.

[21] M. Salayma *et al.*, "Wireless body area network (wban): A survey on reliability, fault tolerance, and technologies coexistence'," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–38, 2017.

[22] V. U. K. Sastry and K. Shirisha, "A block cipher involving a key bunch matrix and an additional key matrix, supplemented with XOR operation and supported by key-based permutation and substitution," *International Journal of Advanced Computer Science and Applications (IJACSA'13)*, vol. 4, no. 1, pp. 131–138, 2013.

[23] Y. Sazaki and R. S. Putra, "Implementation of affine transform method and advanced hill cipher for securing digital images," in *10th International Conference on Telecommunication Systems Services and Applications (TSSA'16)*, pp. 1–5, 2016.

[24] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 2017.

[25] D. R. Stinson, *Cryptography: Theory and Practice*, Chapman & Hall/CRC, 2005.

[26] TOP500.org, *The list; June 2018*, 2018. (`https://www.top500.org/lists/2018/06/`)

Biography

Dr. AbdAllah Adel AlHabshy is a lecturer of computer science at Mathematics department, faculty of science, AlAzhar University, Egypt. He is an experienced scientist researcher and educator with over twelve years of IT experience. His fields of research are Cryptography, Network Security, Mobile Security, Database Security, and Internet of things.