Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 1071-1082
ISSN: 2008-6822 (electronic)
http://www.ijnaa.semnan.ac.ir

A New Approach of Classical Hill Cipher in Public Key Cryptography

Rajaa K. Hasoun[a], Sameerah Faris Khlebus[a,*], Huda Kadhim Tayyeh[a]

[a] *College of Business Informatics, University of Information Technology and Communication, Iraq*

(Communicated by Madjid Eshaghi Gordji)

Abstract

Secure message transformation promote the creation of various cryptography systems to enable receivers to interpret the transformed information. In the present age of information technology, the secure transfer of information is the main study of most agencies. In this study, a particular symmetric cryptography system, Hill Cipher method, is enhanced with the help of encryption and decryption algorithms of the asymmetric RSA cryptography system to avoid certain problems. Previous results show that the original Hill algorithms are still insufficient because of their weakness to known plaintext attack, and a modification of the Hill Cipher cryptography system is therefore presented to increase its invulnerability. The enhancement focuses on implementing the RSA algorithms over the Hill cipher to increase its security efficiency. The suggested method relies on the security of the RSA and Hill Cipher cryptosystems to find the private decryption keys, and thus is much more secure and powerful than both methods applied separately. Also secure and dynamic generation of the hill cipher matrix instead of using static matrix are proposed. This new approach is composed of a public key cryptosystem that has a shared secret key (between participants only), public key (announced to all), and two private keys (for each person). Therefore, this new modification can increase the invulnerability of the Hill Cipher against future attacks during transmission of information between agencies in this age of information technology.

Keywords: Asymmetric cryptosystem, Hill Cipher, Invertible Key Matrix, Involutory matrix, RSA cryptosystem, Symmetric cryptosystem

[*] Corresponding author

Email addresses: dr.rajaa@uoitc.edu.iq (Rajaa K. Hasoun), sameerah.alradhi@uoitc.edu.iq (Sameerah Faris Khlebus), haljobori@uoitc.edu.iq (Huda Kadhim Tayyeh)

Received: March 2021 *Revised:* May 2021

1. Introduction

Cryptography performs a considerable function in the science of secret writing, and can be defined as the art of keeping information by switching and applying technology. The utilization of cryptography can guarantee that the message contents are completely transferred confidentially and remains exactly the same [4]. Encryption alters the database to non-recordable text [7]. Figure (1) shows two kinds of cryptography: secret key cryptography (symmetric) (when the same key is utilized in the encryption and the decryption such as in DES, Triple DES, AES, and RC5) and public key cryptography (asymmetric) (when two various keys are utilized, that is one key is utilized in the encryption and another is utilized in the decryption such as in RSA, Elliptic Curve) [1].

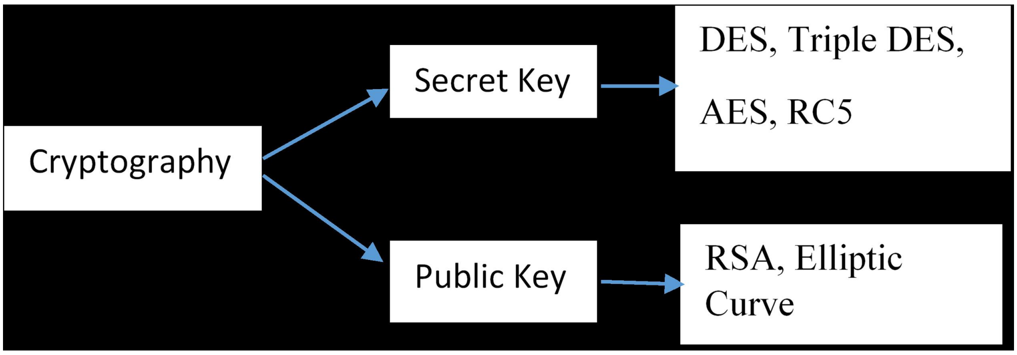


Figure 1: Classification of Cryptography

Designed by L.S. Hill in 1929 [11], the Hill cipher is a popular polygram and symmetric traditional cipher dependent on the conversion of the matrix but suffers from the known plain text attack [10]. Although the vulnerability of coding analysis has made it practically unusable, this cipher plays a fundamental educational role in coding and linear algebra. Hill cipher is a block cipher with various functions such as masking the letter hesitations in plain text, clarity due to utility of multiplication and reflection matrix for encoding and decoding, high speed, and high productivity [6].

In Hill Cipher, ciphertext is generated from the plain text by using linear conversion. Encryption continues by encoding the resulting ciphertext row vector to the main plain text alphabets. The parameter value of m in the genuine Hill cipher was 26, but its value can be selected. Matrix K is assumed to be shared securely among the participants. All operations are performed over a micrometer range. For proper decoding, the main matrix K must be reversible or equivalent and must obtain the gcd (det K (mod m), m) [7, 10]. However, many square matrices are not reversible above m. The risk of co-factors with laboratories can be decreased by taking the initial number as a coefficient. This option also increases the key area of the cipher system [8]. Currently, RSA is one of the most well-known and widely utilized public key systems. Developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978, RSA is the first famous algorithm to be appropriate for signature and encryption, and one of the first great advances in public key cryptography. RSA is a public key ciphering system that uses the concept of number theory. Therefore, its security depends on the complexity of the pre-treatment of large numbers, which is a known mathematical problem without a known effective solution. This makes RSA one of the most widely utilized methods for asymmetric master encryption in encryption standards and digital signature. In general, the RSA algorithm consists of three stages, which are the main generation, coding, and decoding [2]. Figure (2) shows the generation step of RSA. while Figures (3) and (4) show examples of generation, encryption, and decryption.

The Hill cipher has the following basic problems:

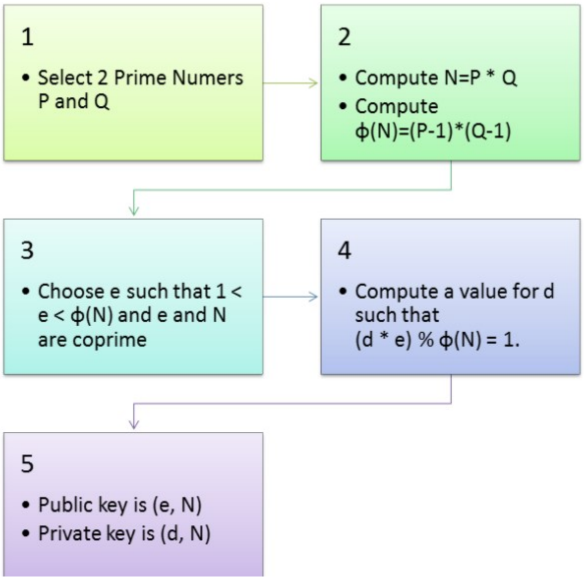
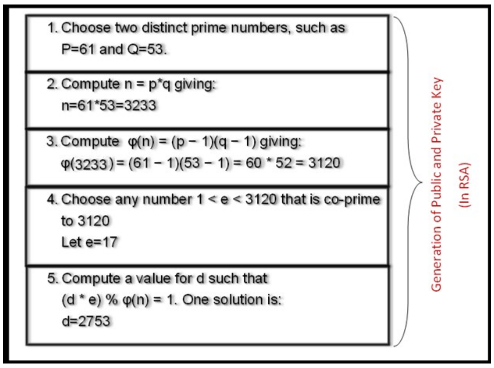

1
• Select 2 Prime Numers P and Q
2
• Compute N=P * Q
• Compute ϕ(N)=(P-1)*(Q-1)
3
• Choose e such that 1 < e < ϕ(N) and e and N are coprime
4
• Compute a value for d such that (d * e) % ϕ(N) = 1.
5
• Public key is (e, N)
• Private key is (d, N)

Figure 2: Generation Step of RSA


1. Choose two distinct prime numbers, such as P=61 and Q=53.

2. Compute n = p*q giving: n=61*53=3233

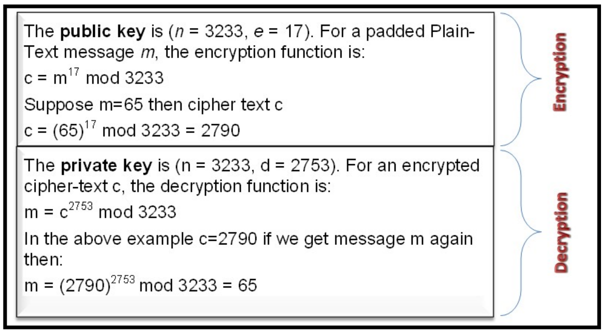
3. Compute φ(n) = (p − 1)(q − 1) giving: φ(3233) = (61 − 1)(53 − 1) = 60 * 52 = 3120

4. Choose any number 1 < e < 3120 that is co-prime to 3120
Let e=17

5. Compute a value for d such that (d * e) % φ(n) = 1. One solution is: d=2753

Generation of Public and Private Key
(In RSA)

Figure 3: Generation of key in RSA


The **public key** is (*n* = 3233, *e* = 17). For a padded Plain-Text message *m*, the encryption function is:

c = m^{17} mod 3233

Suppose m=65 then cipher text c

c = (65)^{17} mod 3233 = 2790

The **private key** is (n = 3233, d = 2753). For an encrypted cipher-text c, the decryption function is:

m = c^{2753} mod 3233

In the above example c=2790 if we get message m again then:

m = (2790)^{2753} mod 3233 = 65

Encryption
Decryption

Figure 4: Encryption and decryption of RSA

1. The key space is the set of all possible keys, and its size is the number of possible keys. Thus, the Hill cipher key space is small.
2. Hill cipher is vulnerable to a known plaintext attack because of its linearity. While matrix multiplication alone does not result in a secure cipher, it is still a useful step when combined with other non-linear operations by providing diffusion.

   In this study, these two problems are solved using RSA and proposed generation of involutory key matrix.

we here propose a new approach for classical hill cipher. In particular, the merits of the proposed system are as follows:

1. Avoiding the linearity feature of the original hill cipher method using RSA.
2. Secure and dynamic generation of the hill cipher matrix instead of using static matrix (smallkey space) in the original hill cipher method. In the proposed modification $K_{ij} \in Z_m$ in which Z_m is ring of integers modulo m where $m \geq 1$, particular let $m = 256$.

2. Related Works

A new modified Hill cipher [3] is suggested to provide enhanced security performance of the conventional hill cipher scheme dependent on the non-square NxM matrix approach. The NxM Hill cipher matrix defuses N plaintext information letters into M cipher text messages. Therefore, the varying M redundant cipher text creates greater confusion than the conventional Hill cipher. Moreover, the modified technique always provides non-singular matrix while finding its inverse, which avoids the complication of singular matrixes in the conventional Hill cipher scheme.

A new mode of operation [5] is also introduced and can be utilized with any block cipher. Then a new enhanced encryption algorithm is proposed. Subsequently, a security analysis and efficiency evaluation are carried out for the new encryption algorithm.

The previously proposed traditional hill cipher procedures are combined with the additional transposition, substitution, and left-right shifting functions [9]. In this method, transposition and substitution of plaintext are performed on $n \times n$ matrix, respectively. After this second procedure of right and left shifting is applied on the encryption, all functions are applied in reverse order to perform the decryption.

In section 4 a comparison will be made between the proposed method and the previous work in [3, 5, 9] in term of some types of attack.

3. Proposed Version of Hill Cipher Utilizing RSA Cryptosystem

The suggested version relies on the enhancement of Hill Cipher cryptography system that can strengthen its invulnerability against known plaintext attack. This modification includes the application of RSA algorithms over the Hill cipher to raise the latter's security and competence. With this suggested version, the plaintext block P is encrypted in the Hill Cipher's encryption algorithm as $C = K \times P(mod\ m)$, where C appears as the ciphertext block and K is the key in the form of involutory key matrix for encryption that should be interchanged secretly among the sender and the receiver. K is called involutory matrix if $K = K^{-1}$. Then, the last outcome ciphertext block C is encrypted again utilizing the RSA encryption algorithm as $C_R = C_e(modN)$, where N is the output of the two large prime numbers p and q and $1 < e, d < \phi(N), gcd(e, \phi(N)) = 1\ and\ ed \equiv 1(mod\ \phi(N))$. In addition, the public key of the RSA is announced to be the pair (e, N) and the private key that is kept secret is the pair (d, N). Indeed, only d should be preserved secret. For the decryption of the ciphertext block C_R, two decryption algorithms with their identical secret keys are utilized to obtain the plaintext block P. Therefore, the ciphertext block C_R is decrypted utilizing the RSA's private (specific) key (d, N) and the decryption algorithm as $C \equiv (C_R)^d(modN)$. The final plaintext block P is then obtained by utilizing the inverse key matrix K^{-1} of K (Hill Cipher key matrix, and $K = K^{-1}$ which is involutory) as $P = C \times K^{-1}(mod\ m)$. Anyone other than the participants who attempts to obtain Fthe original plaintext P from C_R has to find the shared Hill Cipher's secret key matrix K and the RSA private key (d, N). Therefore, the proposed Hill Cipher utilizing the RSA cryptosystem, a public key encryption system, has better security than the traditional version. The reason is that its security relies on the secrecy of the invertible key matrix K and its rank n and on factoring a large integer N, composed of the output of two large prime numbers p and q, to find the private key d. This is a difficult step, as explained in the RSA encryption system. The following shows the generation of involutory key matrix, key generation, encryption algorithm, and the decryption algorithm of the proposed version of the Hill Cipher in the public key cryptography.

Generation of Involutory Key Matrix

The proposed version of the Hill Cipher in public key cryptography utilizes an involutory key matrix for the first encryption technique. K is called involutory matrix if$K = K^{-1}$. The following section shows how to generate the involutory key matrix [11]. Both the sender and the receiver are assumed to agree on the involutory matrix, which will be used to generate the involutory key matrix.

1. Let $K = \begin{bmatrix} k12 & \cdots & k1n \\ \vdots & \ddots & \vdots \\ kn1 & \cdots & \text{knn} \end{bmatrix}$ be an $n \times n$ random involutory key matrix partitioned to $K = \begin{bmatrix} K11 & K12 \\ K21 & K22 \end{bmatrix}$, where n is even and $K_{11}, K_{12}, K_{21}, K_{22}$ are matrices of order $\frac{n}{2} \times \frac{n}{2}$.
2. Then $K_{12}.K_{21} = (I - K_{11}^2) = (I + K_{11})(I - K_{11})$, if K_{12} is one of the factors of $(I - K_{11}^2)$ *and* K_{21} is the other factor.
3. Solve the second matrix equation results $K_{11} + K_{22} = 0$, then form the matrix.

Complete Algorithm

1. Choose any $\frac{n}{2} \times \frac{n}{2}$ matrix, $K22$.
2. Let $K11 = K22\ (mod\ m)$ where $K_{ij} \in Z_m$ in which Z_m is ring of integers modulo m where $m \geq 1$, and I particular let $m = 256$.
3. Either $K12 = s(I + K11)\ or\ s(IK11)$ where s is a scalar constant.
4. Then $K21 = \frac{1}{\kappa}(I + K11) or \frac{1}{\kappa}(IK11)$.
5. Form the involutory key matrix K completely.

Key Generation Process

1. Select an involutory key matrix K, where $K_{ij} \in Z_{256}$ in whichZ_{256} is a ring of integers modulo 256 and K should be interchanged secretly between the sender and the receiver.
2. Choose two distinct prime numbers p and q. For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.
3. Compute $N = pq$, such that N is utilized as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
4. Compute Euler's phi-function $\phi(N) = (p - 1)(q - 1)$.
5. Choose an integer e such that $1 < e < \phi(n)$ and $gcd(e, \phi(N)) = 1$.
6. Determine d such that d is the multiplicative modular inverse of e modulo $\phi(N)$; that is, $d \equiv e - 1\ (mod\ \phi(N))\ or\ ed \equiv 1\ (mod\ \phi(N))$.
7. Publish the pair (e, N) as the public key, and keep d as the private key.

Therefore, this new approach of the Hill Cipher in the public key cryptography has a secret exchanged key matrix K, a public key (e, N) that should be available to all, and a private key d that must be maintained secret by each person.

Encryption Process

The encryption algorithm of this proposed Hill Cipher in the public key cryptography varies from the ordinary algorithms of the symmetric and asymmetric cryptosystems. In this approach, encrypting a plaintext uses two algorithms. The first is the Hill cipher's encryption algorithm applied on the plaintext block P. The second is the RSA encryption algorithm utilized over the outcome of the first algorithm. The steps to encrypt a plaintext block P with only the involutory key matrix K where $k_{ij} \in Z_{256}$ and the public key (e, N) are as follows:

1. Let the plaintext block $P = \begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix}$ such that for all i, $\quad p_i \in \{0, 1, 2, \ldots, 255\}$.
2. Compute Hills ciphertext block $C_H = \begin{bmatrix} C_{h_1} \\ \vdots \\ C_{h_n} \end{bmatrix}$ *as* $C_H = K \times P \ (mod\ 256)$ *or* $E(P) =$ $$C_H = \begin{bmatrix} C_{h_1} \\ \vdots \\ C_{h_n} \end{bmatrix} \equiv \begin{bmatrix} k_{12} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \cdots & k_{nn} \end{bmatrix} \begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix} \ (mod\ 256).$$
3. Compute RSA's ciphertext block as $E(C_H) = C_R = \begin{bmatrix} C_{r_1} \\ \vdots \\ C_{r_n} \end{bmatrix} \equiv (C_H)^e \quad (mod\ N) \equiv$ $$\begin{bmatrix} C_{h_1} \\ \vdots \\ C_{h_n} \end{bmatrix}^e \quad (mod\ N).$$

Now the encoded plaintext block (final ciphertext block) can be sent as $C_R = \begin{bmatrix} C_{r_1} \\ \vdots \\ C_{r_n} \end{bmatrix}$. Upon reaching the intended destination, C_R must be decrypted by the receiver.

4. Decryption Process

In decrypting the ciphertext C_R, the secret shared involutory key matrix $K = K^{-1}$ and private key d are necessary. The process follows from the subsequent algorithm that can be applied on every single ciphertext block:

1. By utilizing the private key d, compute $D(C_R) = \begin{bmatrix} C_{h_1} \\ \vdots \\ C_{h_n} \end{bmatrix} = C_H\ as\ \ D(C_R) = (C_R)^d \equiv \begin{bmatrix} C_{r_1} \\ \vdots \\ C_{r_n} \end{bmatrix}^d \quad (mod\ \ N)$.
2. By utilizing the shared involutory key matrix $K = K^{-1}$, compute $D(C_H) = P \equiv CH \times K(mod\ m)$ or, $D(C_H) = P = \begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix} \equiv \begin{bmatrix} C_{h_1} \\ \vdots \\ C_{h_n} \end{bmatrix} \begin{bmatrix} k_{12} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{n1} & \cdots & k_{nn} \end{bmatrix} \quad (mod\ 256)$.

Illustration of the Method

Suppose that a person "A" wants to encrypt and send a plaintext matrix $M = \begin{bmatrix} 1 & 55 & 235 & 40 \\ 46 & 200 & 155 & 198 \\ 137 & 4 & 66 & 80 \\ 201 & 251 & 111 & 70 \end{bmatrix}$ to a person "B". Assume that the secret exchanged involutory key matrix $K = \begin{bmatrix} 216 & 146 & 41 & 110 \\ 55 & 6 & 201 & 251 \\ 217 & 146 & 40 & 110 \\ 55 & 7 & 201 & 250 \end{bmatrix}$. B's public key is $(e, N = p \star q) = (17, 899 = 29 \star 31)$ and the corresponding private key $d = 593$.

Encryption Process

Step1. The 4×4-plaintext matrix is divided into 4 plaintext blocks:

$$P1 = \begin{bmatrix} 1 \\ 46 \\ 137 \\ 201 \end{bmatrix}, P2 = \begin{bmatrix} 55 \\ 200 \\ 4 \\ 251 \end{bmatrix}, P3 = \begin{bmatrix} 235 \\ 155 \\ 66 \\ 111 \end{bmatrix},\ and\ P4 = \begin{bmatrix} 40 \\ 198 \\ 80 \\ 70 \end{bmatrix}$$

.

Remark 4.1. *For the encryption, the algorithms should be applied over every single plaintext block. However, in this example, only one plaintext block, P1, is considered to show the process and the rest follows in a similar fashion.*

Step2. The plaintext block $P1 = \begin{bmatrix} 1 \\ 46 \\ 137 \\ 201 \end{bmatrix}$ is encrypted utilizing the mentioned algorithms of the new approach, as follows:

$$E(P1) = C_{H1} \equiv K \times P(mod\ 256) \equiv \begin{bmatrix} 216 & 146 & 41 & 110 \\ 55 & 6 & 201 & 251 \\ 217 & 146 & 40 & 110 \\ 55 & 7 & 201 & 250 \end{bmatrix} \begin{bmatrix} 1 \\ 46 \\ 137 \\ 201 \end{bmatrix} (mod\ 256)$$

$$\equiv \begin{bmatrix} 34659 \\ 78319 \\ 34523 \\ 78164 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 99 \\ 239 \\ 219 \\ 84 \end{bmatrix}.$$

$$E(C_{H1}) = C_{R1} \equiv (C_{H1})^e (modN) \equiv \begin{bmatrix} 99 \\ 239 \\ 219 \\ 84 \end{bmatrix}^{17} (mod\ 899) \equiv \begin{bmatrix} 708 \\ 198 \\ 500 \\ 694 \end{bmatrix}.$$

Now the encoded plaintext block (final ciphertext block) can be sent as $C_{R1} = \begin{bmatrix} 708 \\ 198 \\ 500 \\ 694 \end{bmatrix}$.

Remark 4.2. *For the decryption, the algorithms should be applied over every single ciphertext block* C_{Ri}.

However, in this example, we encrypt C_{R1} to show the process and the rest follows in a similar fashion.

Therefore, once $C_{R1} = \begin{bmatrix} 708 \\ 198 \\ 500 \\ 694 \end{bmatrix}$ reaches the intended receiver, the receiver utilizes the mentioned decryption algorithms of the new approach, as follows:

By utilizing the private key $d = 593$,

$$D(C_{R1}) = (C_{R1})^d (mod\ 899) \equiv \begin{bmatrix} 708 \\ 198 \\ 500 \\ 694 \end{bmatrix}^{593} (mod\ 899) = \begin{bmatrix} 99 \\ 239 \\ 219 \\ 84 \end{bmatrix} = C_{H1}.$$

By utilizing the shared involutory key matrix $K = K^{-1}$,

$$D(C_H) = P \equiv C_H \times K(mod\ 256),\ then\ D(C_{H1}) \equiv \begin{bmatrix} 216 & 146 & 41 & 110 \\ 55 & 6 & 201 & 251 \\ 217 & 146 & 40 & 110 \\ 55 & 7 & 201 & 250 \end{bmatrix} \begin{bmatrix} 99 \\ 239 \\ 219 \\ 84 \end{bmatrix} (mod\ 256)$$

$$\equiv \begin{bmatrix} 74497 \\ 71982 \\ 74377 \\ 72137 \end{bmatrix} (mod\ 256) \equiv \begin{bmatrix} 1 \\ 46 \\ 137 \\ 201 \end{bmatrix} = P1.$$

5. Security Analysis and Experimental Results

The modified Hill Cipher algorithm provides an enhanced security performance. One of the measures that can be used to evaluate the proposed method is the confusion metric (which is the metric used to clarify the correlation. In this technique, the size of the matrix is extended as much as possible. However, in conventional Hill cipher technique, the confusion is dependent on the fixed matrix size. Table (1) clearly shows the difference between the two versions.

Table 1: Confusion Comparison of Original and Modified Hill Cipher versions

Hill Cipher Version	***Confusion for*** $N = 2, M = 2$	***Confusion for*** $N = 2, M = 4$	***Confusion for*** $N = 2, M = 8$	***Confusion for*** $N = 2, M = 16$
Original Version	***2***	***2***	***2***	***2***
Modified Version	***2***	***4***	***8***	***16***

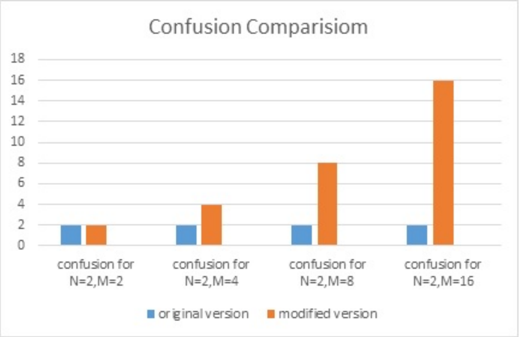


Figure 5: Confusion comparison of original and modified hill cipher versions

The performance of the algorithms is evaluated using the propers of statistical tests for encrypted and plain files using (Frequency(Freq.), block–frequency (Blk_Freq.), cumulative–sums (Cum–Sum), Run, longest-run (Long_Run.), Serial and linear-complexity (Len_Comp.)
Table (2) shows the results.

Table 2: Statistical Test

Sample size	*Freq.*	*Blk_Freq.*	*CumSum*	*Run*	*Long_Run*	*Serial*	*Len_Comp*
500	*0.7980*	*1.0000*	*0.8040*	*0.8000*	*1.0000*	*0.8061*	*1.0000*
200	*0.9952*	*1.0000*	*1.0000*	*0.8450*	*1.0000*	*0.0700*	*1.0000*
100	*0.9700*	*1.0000*	*1.0000*	*0.8000*	*1.0000*	*0.0000*	*1.0000*

The results in Table (2) explain that the proposed approach passed a proximity all the tests. The passing values of the proposed version shows good randomness, which causes greater security against known plaintext attack. In addition, Table (3) and figure (6) shows the time calculation where the proposed modified Hill Cipher has good encryption time.

Table 3: Encryption Processing Time

Size of Message in char	*Encryption & Decryption Processing Time (msec)*	
	Classical hill cipher	*Proposed method*
2518	*401*	*400*
5523	*450*	*440*
7836	*1310*	*1300*

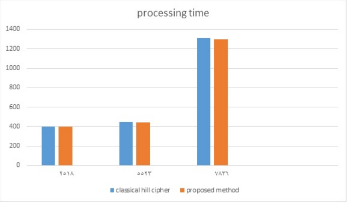


Figure 6: Encryption& Decryption time (comparison)

Calculation of Encryption & Decryption Throughput

Calculation of Encryption & Decryption Throughput = Σ Input File Size/Σ Encryption & Decryption Execution time

Σ Input File Size = 2518+5523+7836=15877 bytes.

Encryption & Decryption Throughput for classical hill cipher:

Σ Encryption & Decryption Execution Time $[classical\ hill\ cipher] = 401 + 450 + 1310 = 2161$

Encryption & Decryption Throughput $[classical\ hill\ cipher] = 15877/2161 = 7.348\ bytes/msec.$

Encryption & Decryption Throughput for proposed method:

Σ Encryption & Decryption Execution Time $[proposed\ method] = 400 + 440 + 1300 = 2140$

Encryption & Decryption Throughput $[proposed\ method] = 15877/2140 = 7.419\ bytes/msec.$

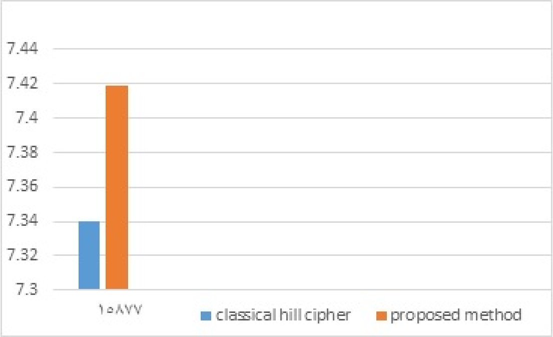


Figure 7: Throughput of classical and proposed method Encryption & Decryption Algorithms

It is clear that from figure (7), the proposed algorithm provides better throughput for file sizes of any type when compared with the actual algorithm. Now will make a comparison between the proposed method and the literature in [3, 5, 9].

Table 4: Dispersion energy parameters of the aqueous extract.

Algorithms	*Chosen plaintext attack*	*Known plaintext attack*	*Man in the middle*
Original hill cipher	*Yes*	*Yes*	*Yes*
Non square matrix [3]	*Yes*	*Yes*	*Yes*
Augmented hill cipher [5]	*No*	*No*	*Yes*
TSLRS [9]	*Yes*	*Yes*	*Yes*
Proposed method	*No*	*No*	*No*

Secure and dynamic generation of the hill cipher matrix instead of using static matrix make the proposed method more secure than chosen plain text attack and known plain text attack while using RSA make it more secure against man in the middle attack.

6. Conclusion

In this study, a new version of Hill Cipher in public key cryptography is proposed. This enhanced version is based on developing the symmetric encryption system utilizing the RSA algorithm. This approach converges on the application of the RSA algorithms over the Hill Cipher to increase the latter's security and efficiency. However, this new approach contains an involutory key matrix K that can be utilized for both encryption and decryption steps, a public key (e, N) that is utilized for encryption, and a private key (d, N) that is utilized for decryption. Basically, in this modified version, a plaintext block P is encrypted utilizing two encryption algorithms, $E(P) = C_H = K \times P\ (mod\ 256)\ and\ as\ E(C_H) = C_R \equiv (C_H)^e (mod\ N)$. The encoded plaintext is then sent as C_R and decrypted utilizing two decryption algorithms$D(C_{R1}) = C_H = (C_{R1})^d (mod\ N)$ and $D(C_H) = P \equiv C_H \times K(mod\ 256)$, respectively. Therefore, this modified version does not require any additional operation to determine the inverse matrix key, which saves more computing time. Moreover, the most interesting result of this modified Hill Cipher is a better security than the traditional version. The security of this modified version is based on the security of the RSA cryptosystem (the prime factorization problem) and of the Hill Cipher cryptosystem (the secrecy of the key matrix K and its rank n). Therefore, the modified version of Hill Cipher has better security than the modern cryptosystem RSA. This new modification can make the Hill Cipher safer against any known plaintext attacks during the transmission of information between agencies in this age of information technology.

References

[1] O.G. Abood, et al., *A survey on cryptography algorithms* international journal of scientific and research publications, 7 (2018).

[2] S. Al-Kaabi, et al., *Methods toward enhancing RSA algorithm*, International Journal of Network Security & Its Applications (IJNSA) 3 (2019).

[3] M. Attique, et al., *Security enhancement of Hill cipher by using non-square matrix approach*, 4^{th} International conference on Knowledge and Innovation in engineering, science and technology, (2018) 21-23.

[4] H. Chien-Lung et al., *A supervising authenticated encryption scheme for multilevel security*, IJICIC (2011).

[5] A. ElHabshy, *Augmented Hill cipher*, International Journal of Network Security. 5 (2019) 812-818.

[6] I.A. Ismail, et al., *How to repair the Hill cipher*. Journal of Zhejiang University-Science A, 12 (2006) 2022-2030.

[7] A. Joseph Amalraj, et al., *A Survey Paper on Cryptography Techniques*, IJCSMC, 8 (2016) 55 59.

[8] J. Overbey, et al., *On the keyspace of the Hill cipher*. Cryptologia Journal, 1 (2005) 59-72.

[9] F. Qazi, et al., *Modification in Hill cipher for cryptographic application*, 3 CTecnologa. Glosas de innovacinaplicadas a la pyme, Special Issue, (2019) 240-257.

[10] D.R. Stinson, *Cryptography Theory and Practice* 3^{rd} *edition*, Chapman & Hall/CRC, (2006) 13-37.

[11] M. Toorani, et al., *A secure variant of the Hill cipher*. Proceedings of the 14th IEEE Symposium on Computers and Communications, (2009) 313-316.