International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 6461~6471
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp6461-6471

A new hybrid text encryption approach over mobile ad hoc network

Mohammed Amin Almaiah[1], Ziad Dawahdeh[2], Omar Almomani[3], Adeeb Alsaaidah[4], Ahmad Al-khasawneh[5], Saleh Khawatreh[6]
[1]Faculty of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia
[2]School of Computer and Communication Engineering, UniMAP University, Malaysia
[3,4]Computer Network and Information Systems Department,
The World Islamic Sciences and Education University, Jordan
[5]Department of Computer Information System, The Hashemite University of Jordan, Jordan
[6]Department of Computer Engineering, Al Ahliyya Amman University, Jordan

Article Info

Article history:

Received Feb 7, 2020
Revised May 28, 2020
Accepted Jun 6, 2020

Keywords:

ASCII code
Encryption
Decryption
Elliptic curve cryptosystem
Hill cipher
Mobile networks security
Self-invertible key matrix

ABSTRACT

Data exchange has been rapidly increased recently by increasing the use of mobile networks. Sharing information (text, image, audio and video) over unsecured mobile network channels is liable for attacking and stealing. Encryption techniques are the most suitable methods to protect information from hackers. Hill cipher algorithm is one of symmetric techniques, it has a simple structure and fast computations, but weak security because sender and receiver need to use and share the same private key within a non-secure channel. Therefore, a novel hybrid encryption approach between elliptic curve cryptosystem and hill cipher (ECCHC) is proposed in this paper to convert Hill Cipher from symmetric technique (private key) to asymmetric one (public key) and increase its security and efficiency and resist the hackers. Thus, no need to share the secret key between sender and receiver and both can generate it from the private and public keys. Therefore, the proposed approach presents a new contribution by its ability to encrypt every character in the 128 ASCII table by using its ASCII value direct without needing to assign a numerical value for each character. The main advantages of the proposed method are represented in the computation simplicity, security efficiency and faster computation.

Corresponding Author:

Mohammed Amin Almaiah,
Faculty of Computer Sciences and Information Technology,
King Faisal University,
31982 Al-Ahsa, Saudi Arabia.
Email: malmaiah@kfu.edu.sa

1. INTRODUCTION

On mobile ad hoc network, information passes from one device to another through numerous systems before it reaches its destination. Some information is very sensitive such as electronic payment, therefore it should run and exchanged over the network in a robust manner and safely [1]. Also, because the mobile ad hoc network makes the nodes moving over the network and it has also become widely used nowadays, so the security requirements for this type of network is also increasing. Therefore, the security for mobile ad hoc network could be offered by means cryptography algorithms. Cryptography over mobile ad hoc network is considered one of the most used ways to protect the sensitive information and prevent unauthorized people from altering that information.

Cryptography is the science of using mathematics to encrypt and decrypt of data. Cryptography enables sender to transmit sensitive information (e.g., text, image, audio, and video) across insecure networks

(like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis [2].

Cryptographic algorithm is a function used for both encryption and decryption processes. In the encryption process, the plaintext (original data) is converted into ciphertext (unreadable) before sending it via the internet to the recipient. In the decryption process, when the data reaches to the intended recipient, it will be returned the ciphertext back to the original data. Since the cryptographic function is mainly dependent on a key value necessary for both encryption and decryption [3]. The cryptographic algorithms can be classified into two main categories which are symmetric key cryptographic algorithms and asymmetric key cryptographic algorithms [4].

In symmetric key cryptographic algorithms, keys used for encryption and decryption processes are the same, as shown in Figure 1. This requires that sender and receiver agree on the key prior to any information exchange, which is called secret key [3, 4]. Symmetric algorithm may contain stream ciphers and block ciphers. Stream ciphers encrypts single bit of plain text at a time, whereas block ciphers encrypt a number of bits of plain text as a single unit. Hill cipher algorithm is an example of symmetric key cryptographic. Although, the Hill cipher algorithm offers several benefits like simple structure, high speed and high throughput, but the level of security is weak, because the sender and receiver share the same key (private key) via unsecured channels [5, 6]. This could lead to easily discover the encryption and decryption keys.

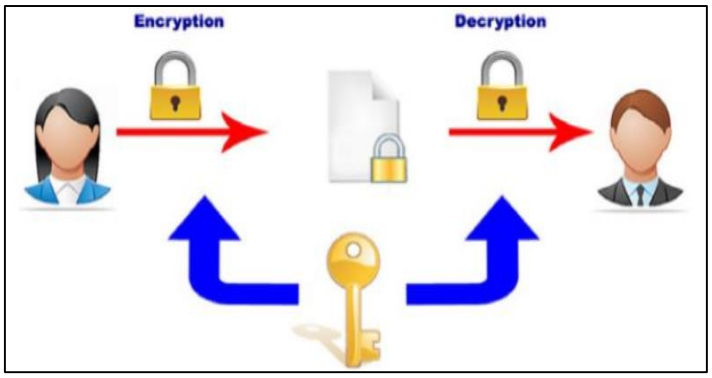

Figure 1. Symmetric key cryptographic

While in asymmetric key cryptographic algorithms, the opposite, where the key used for decryption process is different from the one used for encryption process. It is extremely difficult to determine one key by analyzing the other. This allows for the free distribution of one key (i.e., public), while the key used for decryption is kept private (private key) [3, 4]. Elliptic curve cryptography (ECC) is an example of asymmetric key cryptographic. Figure 2 illustrates asymmetric key cryptography processes.

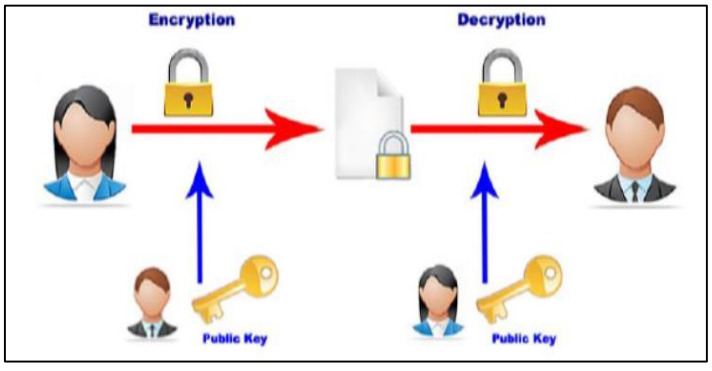

Figure 2. Asymmetric key cryptographic

Elliptic curve cryptography (ECC) is one of the effective asymmetric key cryptographic algorithms which depends on that sender uses a key differ than the receiver's private key and each party generates the public and secret key separately after agreeing on elliptic curve domain parameters [1, 2]. ECC provides a smaller key size with reducing storage and transmission requirements as compared to other algorithms like RSA [6, 7]. This means that that an elliptic curve algorithm could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key: for example, a 256-bit elliptic curve public key should provide comparable security to a 3072-bit RSA public key.

In fact, several researchers have indicated that the problem associated with the cryptographic algorithms is the security that can be provided. This means that the strength of any cryptographic algorithm depends on the strength of the keys used. In other words, the problem of low-level security of any algorithm arises from the weak encryption and decryption keys that have been used and because of the rapid growth in factorization algorithms; weak encryption and decryption keys were easily factored and discovered. To overcome this problem and to provide a good level security, the used keys should be powerful enough [3].

In this work a new encryption and decryption method based on combining the elliptic curve cryptosystem (ECC) with hill cipher (HC) algorithm, which is called (ECCHC). This new approach starts with agree of both sender and receiver to share the domain parameters through elliptic curve function. Then it generates the private and public keys by using the ECC algorithm. Then both sender and receiver have the ability to produce the secret key using the self-invertible key matrix, thus no need to share it through the internet or unsecured communication channel. Also, the same key can be used for encryption and decryption (the matrix is self-invertible if ($k = k^{-1}$), and no need to find the inverse key matrix. The aim of using the proposed self-invertible key matrix in this study is:

- To overcome the problem in Hill cipher algorithm, which is that the inverse of the key matrix does not always exist. So, if the key matrix is not invertible, the decryption process cannot be done, and the receiver cannot get the original data.
- To overcome the problem of distributing the secret key and to make the proposed algorithm more secure and difficult or even impossible to be broken and
- To overcome the problem of delaying the decryption process. Majority of cryptography approaches use the alphabets (a, b, c, …, z), so it needs to assign each character to numerical value through mapping table. While, in our proposed approach, all characters from the 128 ASCII table can be included in the plaintext message and then decrypted directly by its ASCII value without needing to assign it with numerical value from mapping table, which reduces the computational process needs during the decryption process. Thus, the decryption process will be faster.

This paper is organized as follows. An introduction to elliptic curve function over a prime field is introduced in Section 2. Section 3 describes the original Hill Cipher algorithm. Section 4 explains the proposed hybrid encryption approach. An example of the proposed approach is given and analyzed in Section 5. Finally, Section 6 shows the conclusion and the advantages of the proposed approach.

2. LITERATURE REVIEW

Several researchers have tried to improve the security of Hill Cipher. Ismail [8] proposed a new Hill cipher (HillMRIV) that adjusting the encryption key and using a different key for each plaintext block instead of using one key matrix for all blocks and increasing the security of Hill algorithm. Bibhudendra [9] solved the decryption problem if the inverse key matrix does not exist by proposing a novel advanced Hill algorithm (AdvHill) that uses an involutory key matrix for encryption and decryption and eliminates the computations needed by the recipient to find the inverse key matrix. Hamissa [10] enhanced Hill cipher algorithm security by using chaotic functions and presenting a new encoder-decoder technique (ChaoEncoDeco). Nordin [11] proposed a new Hill algorithm (Hill++) that computed a random matrix key based on the previous blocks as an extra key for encryption and resisted all zeroes plaintext blocks.

Agrawal and Gera [12] produced a new method for encryption by using Hill cipher algorithm first to produce the ciphertext numerical values, then convert it to points on the ECC by using scalar multiplication. This method increased the security but also increased the time of computations because scalar multiplication consumed a long time. Sharma and Chirgaiya [13] proposed a method to solve the problem of decryption in the Hill cipher if the key matrix is not invertible, they suggested using setting offset value one if the determinant of a matrix is zero and offset value -1 if the determinant is negative. Mahmoud and Chefranov [14] proposed modification for the Hill cipher (HCM-PRE) that resists known plaintext-ciphertext attack by using pseudo-random eigenvalues and changing key matrix dynamically. Ramesh [15] introduced an algorithm consists of four stages to eliminate the repetition of the substrings and enhance the security, and double columnar transposition is done for the plaintext twice, each time before applying Hill cipher

encryption. Dawahdeh [16] proposed a new image encryption technique that combined elliptic curve cryptosystem with hill cipher and applied the new technique on grayscale images and got a good results compared with other similar techniques.

3. ELLIPTIC CURVE FUNCTION

Elliptic curve cryptography (ECC) is a suitable encryption technique to be used in mobile devices because it can provide high security with smaller key size and fewer computations with little memory and fewer power consumptions. This section describes the primary operations related to elliptic curve function.
Definition 2.1. An elliptic curve E over a prime field F_p is defined by

$$E: y^2 \equiv x^3 + ax + b \ (mod\ p)$$

where $a, b \in F_p$, $p \neq 2, 3$, and satisfy the condition $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$. The set of all points (x, y) that satisfy the elliptic curve E with the point O at the infinity represent the elliptic curve group $E(F_p)$ [1, 17].

3.1. ELLIPTIC CURVE OPERATIONS

3.1.1. Point addition

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, where $P \neq Q$, are two points lie on an elliptic curve E. Adding the two points P and Q giving a third point R that should lie on the same curve E. Depending on the coordinates of the points P and Q, there are two cases for this addition [12, 18].
If $P \neq Q \neq O$ with $x_1 \neq x_2$, the sum of the points P and Q is defined by

$$R = P + Q = (x_3, y_3)$$

where
$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)}$
$x_3 \equiv (\lambda^2 - x_1 - x_2) \ (mod\ p)$
$y_3 \equiv (\lambda x_1 - \lambda x_3 - y_1) \ (mod\ p)$

If $x_1 = x_2$ but $y_1 \neq y_2$ then $P + Q = O$.

3.1.2. Point doubling

Point doubling means adding the point $P = (x_1, y_1)$ that lies on the elliptic curve E to itself. The point R that results from doubling is also lies on the elliptic curve E [19, 20].

$$R = 2P = P + P = (x_3, y_3)$$

where
$\lambda = \frac{3\,{x_1}^2 + a}{2\,y_1}$
$x_3 \equiv (\lambda^2 - 2x_1) \ (mod\ p)$
$:y_3 \equiv (\lambda x_1 - \lambda x_3 - y_1) \ (mod\ p)$

3.1.3. Scalar multiplication

The scalar multiplication of an integer k by the point $Q = (x_1, y_1)$ that lies on the curve E can be defined by repeating the addition of the point Q to itself k times. The results point R also lies on the elliptic curve E.

$$R = kQ = \underbrace{Q + Q + \cdots + Q}_{k-times}$$

For example, computing $15Q$ can be done using point addition and point doubling as follows [19]:

$$15Q = 2(2(2Q + Q) + Q) + Q$$

4. HILL CIPHER ALGORITHM

Hill cipher is a symmetric block cipher technique invented by the mathematician Lester Hill in 1929 [21]. Both sender and receiver should share and use the same key matrix for ciphering and deciphering. The main concept of this technique based on assign each letter by a numerical value, for example, a=0, b=1, …, z=25. Then divide the plaintext (message) into blocks consist of the same size m depending on the key matrix size $m \times m$. For example, if the block size is two ($P_{2\times1}$), then the key matrix ($K_{2\times2}$) should be of size 2×2 , and the encryption process will produce ciphertext with two numerical values ($C_{2\times1}$) as follows [12]:

If $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ and $K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ then

$$C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \bmod 26 = \begin{bmatrix} (k_{11}p_1 + k_{12}p_2) \bmod 26 \\ (k_{21}p_1 + k_{22}p_2) \bmod 26 \end{bmatrix}$$

To decrypt the ciphertext, the recipient needs to compute the key matrix inverse (K^{-1}) where $K.K^{-1} = I$, I is the identity matrix, then use the following equation to produce the plaintext (original message) [9, 21].

$$P = K^{-1}.C \bmod 26$$

5. THE PROPOSED CRYPTOSYSTEM

The new approach of Elliptic Curve Cryptosystem and Hill Cipher (ECCHC) has been introduced in this section. This modification increases the security and makes the system more efficient than the original technique, also speeds up the decryption computations because no need to compute the key matrix inverse. Suppose User A (the sender) wants to send a message M to User B (the receiver) using ECCHC over an insecure channel. Firstly, they should agree on the elliptic curve function E and share the domain parameters $\{a, b, p, G\}$, where a, b are the coefficients of the elliptic function, p is a large prime number, and G is the generator point. Then each party needs to choose his private key randomly from the interval $[1, p-1]$; n_A for User A and n_B for User B. The public key for each user can be generated as follows

$$P_A = n_A . G$$

$$P_B = n_B . G$$

Each user multiplies his private key by the public key of the other user to get the initial key $K_I = (x, y)$

$$K_I = n_A . P_B = n_B . P_A = n_A . n_B . G = (x, y)$$

Then computes

$$K_1 = x . G = (k_{11}, k_{12})$$

$$K_2 = y . G = (k_{21}, k_{22})$$

Next step is generating the secret key matrix by sender and receiver. The inverse of the key matrix does not always exist. So, if the key matrix is not invertible, the recipient cannot decrypt the ciphertext. To solve this problem, the self-invertible key matrix will be generated, and the same key will be used for encryption and decryption (the matrix K is self-invertible if $K = K^{-1}$), and no need to find the inverse key matrix. Assume the message $\boldsymbol{M}$ divided into blocks of size four characters (add space to complete the last block, if necessary). So, each party produces the 4×4 self-invertible key matrix $\boldsymbol{K_m}$ by using the proposed method in [16, 22]:

Let $K_m = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}$ be self-invertible matrix partitioned as $K_m = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$.

The proposed approach assumes that $K_{11}=\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$, then the values of the other partitions of the secret matrix key K_m is obtained by solving $K_{12}=I-K_{11}$, $K_{21}=I+K_{11}$, and $K_{11}+K_{22}=0$, where I is the identity matrix.

The main concept of Hill cipher depends on assigning a numerical value for each character in the plaintext [23]. The decimal ASCII code table from 32 to 126 will be used for this issue (space=32, !=33, …, 0=48, 1=49, …, A=65, B=66, …, a=97, b=98, …, ~=126), and mod 95 will be used in this case for modulo. This modification considered as a new contribution in this approach because all other methods encrypt only (a=0, b=1, …, z=25), whereas all characters from the 128 ASCII table can be included in the plaintext message of the proposed approach [24, 25].

Now, separate the plaintext message M into blocks of size four characters (add space to complete the last block, if necessary) and replace each character by its decimal ASCII value and take modulo 95 for each value, then arrange each block into four rows column vector $(P_1, P_2, P_3, ...)$ and multiply the self-invertible key matrix K_m by each vector and take modulo 95 to get the ciphertext vectors $(C_1, C_2, C_3, ...)$. After that, add 32 to each value in the ciphertext vectors because we work only on characters that start from the value 32 in the ASCII table. Then replace each numerical value in the ciphered vectors with its corresponding character from the ASCII table and rearrange the characters in a new message C that represents the ciphered message. The following calculations are repeated for each block:

Let $P_1=\begin{bmatrix} p_{11} \\ p_{21} \\ p_{31} \\ p_{41} \end{bmatrix}$ then

$$C_1=K_m.P_1=\begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}\begin{bmatrix} p_{11} \\ p_{21} \\ p_{31} \\ p_{41} \end{bmatrix}=\begin{bmatrix} ((k_{11}p_{11}+k_{12}p_{21}+k_{13}p_{31}+k_{14}p_{41}) \bmod 95)+32 \\ ((k_{21}p_{11}+k_{22}p_{21}+k_{23}p_{31}+k_{24}p_{41}) \bmod 95)+32 \\ ((k_{31}p_{11}+k_{32}p_{21}+k_{33}p_{31}+k_{34}p_{41}) \bmod 95)+32 \\ ((k_{41}p_{11}+k_{42}p_{21}+k_{43}p_{31}+k_{44}p_{41}) \bmod 95)+32 \end{bmatrix}=\begin{bmatrix} c_{11} \\ c_{21} \\ c_{31} \\ c_{41} \end{bmatrix}$$

Decryption processes start when the recipient receives the ciphertext C by separating the ciphertext into blocks of size four characters then replacing each character by its decimal ASCII value and subtracting 32 from each value and arrange each block into four rows column vector. Then multiplies the self-invertible key matrix K_m by each vector $(C_1, C_2, C_3, ...)$ and takes modulo 95 to get the plaintext vectors $(P_1, P_2, P_3, ...)$. Finally, adds 95 to each value less than 32 and replaces each numerical value with its corresponding character from the ASCII table to get the original plaintext message M.

5.1. The proposed approach (ECCHC)

Step 1: Key Generation

User A (The sender)

1. Choose the private key $n_A \in [1, p-1]$
2. Compute the public key $P_A = n_A.G$
3. Compute the initial key $K_I = n_A.P_B = (x, y)$
4. Compute $K_1 = x.G = (k_{11}, k_{12})$ and $K_2 = y.G = (k_{21}, k_{22})$
5. Generate the self-invertible key matrix K_m

User B (The receiver)

1. Choose the private key $n_B \in [1, p-1]$
2. Compute the public key $P_B = n_B.G$
3. Compute the initial key $K_I = n_B.P_A = (x, y)$
4. Compute $K_1 = x.G = (k_{11}, k_{12})$ and $K_2 = y.G = (k_{21}, k_{22})$
5. Generate the self-invertible key matrix K_m

Step 2: Encryption (User A)

1. Separate the plaintext message M into blocks of size four characters.
2. Replace each character by its decimal ASCII value and take modulo 95 for each value.

3. Arrange each block into four rows column vector (4×1).
4. Multiply the self-invertible key matrix K_m by each vector $(P_1, P_2, P_3, ...)$ and take modulo 95 for each value $C_1 = (K_m . P_1) \bmod 95$
5. Add 32 to each value in the ciphertext vectors $(C_1, C_2, C_3, ...)$.
6. Replace each numerical value with its corresponding character from the ASCII table.
7. The resulting text forms the ciphertext message C.

Step 3: Decryption (User B)

1. Separate the ciphertext message C into blocks of size four characters.
2. Replace each character by its decimal ASCII value.
3. Subtract 32 from each value in the ciphertext blocks.
4. Arrange each block into four rows column vector.
5. Multiply the self-invertible key matrix K_m by each vector $(C_1, C_2, C_3, ...)$ and take modulo 95 for each value $P_1 = (K_m . C_1) \bmod 95$
6. Add 95 to each value in step5 less than 32.
7. Replace each numerical value in the vectors $(P_1, P_2, P_3, ...)$ by its ASCII table corresponding character.
8. The resulting text forms the decrypted message M.

6. EXPERIMENTAL RESULTS AND ANALYSIS

Assume that User A wants to send the message M to User B and they agreed to use the elliptic curve function

$$E: y^2 \equiv x^3 + x + 3 \ (mod\ 31)$$

where $A = 1, B = 3, p = 31$; which satisfies the condition $4A^3 + 27B^2$ = $4(1)^3$+$27(3)^2$ = 4+243 = 247 *mod* 31 = 30 $\neq$ 0. The elliptic curve $E_{31}(1,3)$ points are shown in Table 1 [16, 18].

Table 1. The points of the elliptic curve $E: y^2 \equiv x^3 + x + 3 \ (mod\ 31)$

(1, 6)	(6, 15)	(15, 13)	(21, 4)	(26, 11)
(1, 25)	(6, 16)	(15, 18)	(21, 27)	(26, 20)
(3, 8)	(9, 11)	(17, 2)	(22, 3)	(27, 11)
(3, 23)	(9, 20)	(17, 29)	(22, 28)	(27, 20)
(4, 3)	(12, 10)	(18, 5)	(23, 14)	(28, 2)
(4, 28)	(12, 21)	(18, 26)	(23, 17)	(28, 29)
(5, 3)	(14, 8)	(20, 5)	(24, 5)	(30, 1)
(5, 28)	(14, 23)	(20, 26)	(24, 26)	(30, 30)

Since the order of the elliptic curve $E_{31}(1,3)$ is 41, which is a prime number, any point from Table 1 can be chosen to represent the base point or generator point G. So, if we choose $G = (1,6)$, the domain parameters for E are $\{A, B, p, G\} = \{1, 3, 31, (1,6)\}$. If User A wants to send the plaintext message M ="Hi, our meeting at 10 Am" to User B. Both sender and receiver should apply the proposed approach (ECCHC) on the message M as follows:

6.1. The proposed approach (ECCHC)

Step 1: Key Generation

User A

1. Choose the private key $n_A = 13 \in [1, 30]$
2. Compute the public key $P_A = n_A . G = 13(1,6) = (3,23)$
3. Compute the initial key $K_I = n_A . P_B = 13(24,5) = (20,5) = (x, y)$
4. Compute $K_1 = x \,.\, G = 20(1,6) = (4,28) = (k_{11}, k_{12})$ and $K_2 = y \,.\, G = 5(1,6) = (15,18) = (k_{21}, k_{22})$
5. Assume that $K_{11} = \begin{bmatrix} 4 & 28 \\ 15 & 18 \end{bmatrix}$, then the self-invertible key matrix $K_m = \begin{bmatrix} 4 & 28 & 92 & 67 \\ 15 & 18 & 80 & 78 \\ 5 & 28 & 91 & 67 \\ 15 & 19 & 80 & 77 \end{bmatrix}$

User B

1. Choose the private key $n_B = 17 \in [1, 30]$
2. Compute the public key $P_B = n_B.G = 17(1, 6) = (24, 5)$
3. Compute the initial key $K_I = n_B.P_A = 17(3, 23) = (20, 5) = (x, y)$
4. Compute $K_1 = x\,.\,G = 20(1, 6) = (4, 28) = (k_{11}, k_{12})$ and $K_2 = y\,.\,G = 5(1, 6) = (15, 18) = (k_{21}, k_{22})$
5. Assume that $K_{11} = \begin{bmatrix} 4 & 28 \\ 15 & 18 \end{bmatrix}$, then the self-invertible key matrix $K_m = \begin{bmatrix} 4 & 28 & 92 & 67 \\ 15 & 18 & 80 & 78 \\ 5 & 28 & 91 & 67 \\ 15 & 19 & 80 & 77 \end{bmatrix}$

Step 2: Encryption (User A)

1. $M =$ (Hi,)(our)(meet)(ing)(at 1)(0 Am)
2. The ASCII values for M

$M = (72\ 105\ 44\ 32)(111\ 117\ 114\ 32)(109\ 101\ 101\ 116)(105\ 110\ 103\ 32)$ $(97\ 116\ 32\ 49)(48\ 32\ 65\ 109)$

and after taking modulo 95, it will be

$M = (72\ 10\ 44\ 32)(16\ 22\ 19\ 32)(14\ 6\ 6\ 21)(10\ 15\ 8\ 32)(2\ 21\ 32\ 49)(48\ 32\ 65\ 14)$

3. $P_1 = \begin{bmatrix} 72 \\ 10 \\ 44 \\ 32 \end{bmatrix}$, $P_2 = \begin{bmatrix} 16 \\ 22 \\ 19 \\ 32 \end{bmatrix}$, $P_3 = \begin{bmatrix} 14 \\ 6 \\ 6 \\ 21 \end{bmatrix}$, $P_4 = \begin{bmatrix} 10 \\ 15 \\ 8 \\ 32 \end{bmatrix}$, $P_5 = \begin{bmatrix} 2 \\ 21 \\ 32 \\ 49 \end{bmatrix}$, and $P_6 = \begin{bmatrix} 48 \\ 32 \\ 65 \\ 14 \end{bmatrix}$
4. The multiplication of K_m by the first vector P_1 will be done, and the same process will be repeated for the other vectors.

$$C_1 = K_m.P_1 = \begin{bmatrix} 4 & 28 & 92 & 67 \\ 15 & 18 & 80 & 78 \\ 5 & 28 & 91 & 67 \\ 15 & 19 & 80 & 77 \end{bmatrix} \begin{bmatrix} 72 \\ 10 \\ 44 \\ 32 \end{bmatrix} \bmod 95 = \begin{bmatrix} 15 \\ 56 \\ 43 \\ 34 \end{bmatrix}$$

5. Add 32 to each value in C_1

$$C_1 = \begin{bmatrix} 47 \\ 88 \\ 75 \\ 66 \end{bmatrix}$$

6. From the ASCII table $C_1 =$ /XKB

After repeating steps 4, 5, and 6 for the vectors $P_2, P_3, P_4, P_5,$ and P_6, the ciphertext message that will be sent to user B is $C =$ /XKB,1)r}]&N/I18nMP1:s)&

Step 3: Decryption (User B)

1. $C =$ (/XKB) (,1)r) (}]&N) (/I18) (nMP1) (:s)&)
2. The ASCII values for C

$C = (47\ 88\ 75\ 66)(44\ 124\ 41\ 114)(125\ 93\ 38\ 78)(47\ 73\ 49\ 56)(110\ 77\ 80\ 49)$ $(58\ 115\ 41\ 38)$

3. Subtract 32 from each value in the ciphertext vectors

$$C = (15\ 56\ 43\ 34)(12\ 92\ 9\ 82)(93\ 61\ 6\ 46)(15\ 41\ 17\ 24)(78\ 45\ 48\ 17)(26\ 83\ 9\ 6)$$

4. $C_1 = \begin{bmatrix} 15 \\ 56 \\ 43 \\ 34 \end{bmatrix}$, $C_2 = \begin{bmatrix} 12 \\ 92 \\ 9 \\ 82 \end{bmatrix}$, $C_3 = \begin{bmatrix} 93 \\ 61 \\ 6 \\ 46 \end{bmatrix}$, $C_4 = \begin{bmatrix} 15 \\ 41 \\ 17 \\ 24 \end{bmatrix}$, $C_5 = \begin{bmatrix} 78 \\ 45 \\ 48 \\ 17 \end{bmatrix}$, and $C_6 = \begin{bmatrix} 26 \\ 83 \\ 9 \\ 6 \end{bmatrix}$

5. The multiplication of K_m by the first vector C_1 will be done, and the same process will be repeated for the other vectors.

$$P_1 = K_m . C_1 = \begin{bmatrix} 4 & 28 & 92 & 67 \\ 15 & 18 & 80 & 78 \\ 5 & 28 & 91 & 67 \\ 15 & 19 & 80 & 77 \end{bmatrix} \begin{bmatrix} 15 \\ 56 \\ 43 \\ 34 \end{bmatrix} \bmod 95 = \begin{bmatrix} 72 \\ 10 \\ 44 \\ 32 \end{bmatrix}$$

6. Add 95 to each value in step5 less than 32

$$P_1 = \begin{bmatrix} 72 \\ 105 \\ 44 \\ 32 \end{bmatrix}$$

7. From the ASCII table $P_1 =$ Hi,

After repeating steps 5, 6, and 7 for the vectors C_2, C_3, C_4, C_5, and C_6, the decrypted message that will be resulted is $M =$ Hi, our meeting at 10 Am.

7. CONCLUSION

Information security is one of the most important issues in the recent times. Elliptic curve cryptography (ECC) is one of the most efficient public key cryptosystems that is secured against adversaries because it is hard for them to find the secret key and solve the elliptic curve discrete logarithm problem. It's strengthened security also comes from the small key size that is used in it with the same level of safety compared to the other cryptosystems like RSA.

A new approach cryptosystem (ECCHC) has been proposed in this paper combining ECC with standard Hill cipher algorithm to enhance and increase the security of the original Hill cipher. It generates a new encryption/decryption key by using ECC approach which produces a strong secret key that resistant against intruders and provides better security because no need to share the key through the internet. Self-invertible key matrix is used for encryption and decryption. So, no need to find the inverse key matrix in the decryption process. The ability to encrypt every character in the 128 ASCII table directly without mapping table is a new contribution in this approach because other methods used only the alphabets (a, b, c, …, z) and need mapping table. Otherwise, the proposed approach can be used efficiently in real-time multimedia and wireless applications and suitable for small devices and embedded systems because it has a simple structure and faster computations and can be applied on text, image, audio, and video.

REFERENCES

[1] H. Darrel, et al., "Guide to elliptic curve cryptography," *Springer-Verlag Professional Computing Series*, pp. 1-311, 2004.

[2] M. U. Bokhari and Q. M. Shallal, "A Review on Symmetric Key Encryption Techniques in Cryptography," *International Journal of Computer Applications*, vol. 147, no. 10, pp. 43-48, 2016.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[4] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*, pp. 417-426, 1985.

[5] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.
[6] B. K. Alese, et al., "Comparative analysis of public-key encryption schemes," *International Journal of Engineering and Technology*, vol. 2, no. 9, pp. 1552-1568, 2012.
[7] K. Rajadurga and S. R. Kumar, "GF (2m) based low complexity multiplier for elliptic curve cryptography systems," *Networking and Communication Engineering*, vol. 6, no. 4, pp. 150-155, 2014.
[8] I. A. Ismail, et al., "How to repair the Hill cipher," *Journal of Zhejiang University SCIENCE A*, vol. 7, no. 12, pp. 2022-2030, 2006.
[9] B. Acharya, et al., "Image encryption using advanced hill cipher algorithm," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 663-667, 2009.
[10] G. Hamissa, et al., "Securing JPEG architecture based on enhanced chaotic hill cipher algorithm," in *2011 International Conference on Computer Engineering & Systems (ICCES)*, pp. 260-266, 2011.
[11] M. N. A. Rahman, 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.
[12] K. Agrawal and A. Gera, "Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem," *International journal of computer applications*, vol. 106, no. 1, pp. 18-24, 2014.
[13] N. Sharma and S. Chirgaiya, "A Novel Approach to Hill Cipher," *International Journal of Computer Applications*, vol. 108, no. 11, pp. 34-37, 2014.
[14] A. Mahmoud and A. Chefranov, "Hill cipher modification based on pseudo-random eigenvalues," *Applied Mathematics and Information Sciences*, vol. 8, no. 2, pp. 505-516, 2014.
[15] A. Ramesh, "Enhancing the Security of Hill Cipher using Columnar Transposition," in *International Journal of Engineering Research and Technology*, vol. 4, no. 07, pp. 741-744, 2015.
[16] Z. E. Dawahdeh, et al., "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349-355, 2018.
[17] J. Hoffstein, et al., "Elliptic Curves and Cryptography," in *An Introduction to Mathematical Cryptography*, pp. 299-371, 2014.
[18] Z. E. Dawahdeh, et al., "A New Modification for Menezes-Vanstone Elliptic Curve Cryptosystem," *Journal of Theoretical and Applied Information Technology*, vol. 85, no. 3, pp. 290-297, 2016.
[19] B. Nayak, "Signcryption schemes based on elliptic curve cryptography," Master Thesis, National Institute of Technology Rourkela, India, 2014.
[20] M. N. Udin, et al., "Application of message embedding technique in ElGamal elliptic curve cryptosystem," in *2012 International Conference on Statistics in Science, Business, and Engineering (ICSSBE)*, pp. 1-6, 2012.
[21] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306-312, 1929.
[22] B. Acharya, et al., "Novel methods of generating self-invertible matrix for hill cipher algorithm," *International Journal of Security*, vol. 1, no. 1, pp. 14-21, 2007.
[23] P. G. Mante, et al., "A Symmetrical Encryption Technique for Text Encryption Using Randomized Matrix Based Key Generation," in *Advances in Data Science and Management*, pp. 137-148, 2020.
[24] M. A. Naji, et al., "Cryptanalysis cipher text using new modeling: Text encryption using elliptic curve cryptography," in *AIP Conference Proceedings*, vol. 2203, no. 1, 2020.
[25] R. Anandkumar and R. Kalpana, "A Survey on Chaos Based Encryption Technique," in *Enabling Technologies and Architectures for Next-Generation Networking Capabilities*, pp. 147-165, 2019.

BIOGRAPHIES OF AUTHORS

Mohammed Amin Almaiah received his PhD in Computer Science from University Malaysia Terengganu from Malaysia. MSc in Computer Information System from Middle East University (MEU) in 2011 from Jordan. He is now working as Assistant Professor in the Department of CIS at King Faisal Saudi Arabia. He has published over 15 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, the Journal of Educational Computing Research and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include mobile learning, software quality, network security and technology acceptance. He is a certified recognized Reviewer by several leading journals in IEEE, Elsevier and Springer.

Ziad Dawahdeh, School of Computer and Communication Engineering, UniMAP University, Perlis, Malaysia.

Omar Almomani, received his Bachelor and Master degree in Telecommunication Technology from institute of Information Technology, University of Sindh on 2002 and 2003 respectively. Almomani received his PhD from UNIVERSITY UTARA MALAYSIA in computer network. Currently he is Associate Professor in Network Computer and Information Systems Department, Information Technology Faculty at the World Islamic Sciences & Education University. His research interests involves mobile ad hoc networks, Network Performance, Multimedia Networks, Network Quality of Service (QoS), IoT, Network modelling and Simulation, Grid Computing, Network Security and Cloud Security.

Adeep Alsaaidah, received his Bachelor degree in computer engineering from faculty of engineering at Balqa applied university and his Master degree in networking and computer security at NYIT University. Alsaaidah received his PhD from university USIM Malaysia in computer network. Currently he is Assistance Professor in Network Computer and Information Systems Department, Information Technology Faculty at the World Islamic Sciences & Education University. His research interests include Network Performance, Multimedia Networks, Network Quality of Service (QoS), IoT, Network modelling and Simulation, Network Security and Cloud Security.

Ahmad Al-Khasawneh is a professor of computer information systems. He holds the PhD and M.Sc. of information systems and computer engineering from Newcastle University, Australia and B.S in computer and automatic control engineering. Dr. Khasawneh has 25 years of experience in ICT field and in ICT applications and acts as technical advisor to the Royal Jordanian Airlines (NDC Jordan) director on issues related to the development of travel industry and ICT strategy. Prior to joining the Hashemite University of Jordan, he held several key positions with major international ICT consultancy and solutions firms and lecturer in IT related topics at Newcastle University, Australia. One of his key positions is the director of eLearning center and, he is the former dean of the Prince Hussein Bin Abdullah II for Information Technology at Hashemite University. Currently, he is the director of center of information and communication technology and eLearning. He is managing and coordinating three Tempus projects; and four erasmus+ project, and a head and member of the many committees of another Tempus and Erasmus+ project. He is very well-known in the EU project management.

Saleh Khawatreh, Associate professor of Computer Engineering, Al Ahliyya Amman University, Jordan.