Journal of Theoretical and Applied Information Technology
31st May 2021. Vol.99. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL SYMMETRIC HYBRID CRYPTOGRAPHY TECHNIQUE USING LINEAR BLOCK CIPHER (LBC) AND SIMPLE SYMMETRIC KEY

[1]PRAKASH KUPPUSWAMY, [2]SAEED Q AL-KHALIDI AL-MALIKI

[1]Computer Engineering & Networks Department, College of CS & IT, Jazan University, KSA.

[2]Associate Professor, Department of Information Systems, King Khalid University, Abha, Saudi Arabia
E-mail: [1] prakashcnet@gmail.com, [2]salkhalidi@kku.edu.sa

ABSTRACT

Data encryption technique is the art of cryptology protecting valuable information or data by transforming it into an unreadable scrambled text. Cryptography algorithm is a mathematical technique used to preventing or safeguard messages from unsolicited access. In the current digital environment, public, private financial institution's data transactions conducts through open network channel only. Therefore, it is significant to implement cryptography techniques on those financial data to secure valuable things. In many sectors exploiting private algorithms such as DES, AES and public algorithms such as RSA, Diffie-hellman been using in various applications. Public key or Asymmetric key encryption technique has connection with many performance issues such as energy consumption, memory wastage and computational problems etc., Correspondingly, symmetric key algorithm also has a problem of non-repudiation, false modification etc., to overcome the above issues and enhance the confidentiality to make it stronger, hybrid cryptography techniques offered better solution. In short, the hybrid technique uses the combination of two or more encryption algorithms. The proposed hybrid algorithm is combination of enhanced hill cipher algorithm using modulo 37 and using simple positive and negative integer numbers. Many hybrid algorithm follows different logic to provide more security, we proposed here, simple and open design, straightforwardness, computational speed, more privacy. and security compared to existing hybrid encryption schemes.

Keywords: *Symmetric Key, Asymmetric Key, Hybrid Encryption, Block cipher, RSA, DES, AES etc.,*

1. INTRODUCTION

Cryptography is a technique of art and science of succeeding security by encoding the format to make them unreadable scrambled text. It consists of data encryption and data decryption procedures [27]. The technique of protective information by transforming it into an unreadable and scrambled message is called data encryption or cipher text. Again it's converted into plain text needs secret key, this transformation is called decryption or deciphering. The technique of cryptography is used in federal government, protecting e-mail messages, credit card information, corporate data, and many more applications. Some of the most popular cryptography systems such as RSA, AES, DES, Elliptic curve and e-mail Pretty Good Privacy are used in many applications because it is effective and free. Cryptography systems can be broadly classified into two significant categories, symmetric-key systems that use a single key that both the sender and the recipient have, and public-key systems that use two keys. One public key known to everyone and a private key that only recipients of messages can only apply and retrieve the original plain text [13,33]. Symmetric block ciphers are using in many government sectors to protect important documents [8,22,31,32].

Encryption techniques are the well-organized message of exchanging secure communication over insecure internet and web communication channels. Effective data encrypting model mostly depends on the strength of encryption tools, security constraints and execution spend and privacy are the most considerable features. Network communications are open and insecure, therefore, it is very easy to access or modify the original text, data, e-mail, during the time of exchanging information between two parties [15]. Several traditional symmetric key algorithms *(Figure.2)* encrypted messages has breached, however modern cryptography techniques are virtually unbreakable, but it is attacked many times by intruders. Many symmetric and traditional algorithms proved as vulnerable [22,30], and many attacks in [6,14,21]

performed on block ciphers and stream ciphers [5,22]. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important [35].

The media, communication, and financial industries have achieved rapid advances and internet mobile users are increasing significantly to send and receive their personal information or data by using many applications such as Whatsapp, Twitter, Instagram, Facebook over the open network channel [3]. Moreover, in particularly Military, Medical and Banking industries has accomplished boundless advances by the integrating with Information and communication technologies [11]. There are many traditional and modern cryptography systems that are applied in the above mentioned industries with some specified symmetric encryption algorithms such as Data Encryption Standard (DES) [32] and Advanced Encryption Standard (AES) [10,29] are the most common. Asymmetric key cryptography or public-key cryptography *(Figure.1)* requires special keys to encrypt and decrypt messages. Some of common asymmetric encryption algorithms such as RSA [12,29] and Elliptic Curve Cryptography (ECC)[18,29]are most widely using in industrial applications. ECDSA – Elliptic Curve Digital Signature Algorithm [7,29] and ECDH – Elliptic Curve Diffie Hellman [16,27] are based on ECC. Data security and privacy are one of the major issues in open access communication. Distribution or decentralization of data transmission on the internet more prone to risk and attacks. A hybrid combination of symmetric and asymmetric encryption algorithms will increase more data security as compared to a single encryption system [36].

Data or information security has always been a part of the mobile or internet users to maintain their privacy. Normally, internet and mobile users, substantially they don't encrypt all their personal data and valuable financial information. These messages are passed between different entities in order to do electronic transactions over a network. The security of a cardless electronic payment system is always a critical issue, if there are any security breaches, it will cause enormous financial fatalities [23]. Consequently, it is more chance to lose their valuable data or hacking of the system. To overcome the above problems, cryptography provides a solution to secure user data and valuable information, where the medium of transmission is susceptible to interception, by translating a message into a form that cannot be readable by unauthorized users [3].

In the present digital era, many ways have been used by unauthorized users to access or infect digital data. Protecting an individual's data or communication is a crucial issue for researchers to protect on the internet which has provided services for open access communication [39]. Many cryptographic algorithms have been implemented to safe and secure the information from an unauthorized user. Any cryptography algorithm requires some of the following fundamental features, authenticity allows only authorized users, and integrity confirms the received message not altered by anyone in the middle and scalability is applied to confirm seamless data between the authorized users [29]. To provide additional security and privacy of messages [1-2, 9, 24, 28], a hybrid security solution was initialized and applied in many business applications to secure private and sensitive data transmission on open network channel. Normally user sends the data through secured and trusted network only, but the source and target system remains connected with unsecure internet. Hybrid cryptography can full fill the requirement of security and confidentiality of user's data [4].

Proposed hybrid algorithm designed to fully fill data security and user's authenticity. It includes two phase of work at the similar processing time. In Phase I, it takes the advantages of the combination of both symmetric cryptographic techniques using Extended Hill cipher, i.e, block cipher it is a substitution traditional cryptography introduced by Lester S.Hill in 1929 based on linear algebra. [19, 20] and another using simple integer numbers. In Phase I, extended block cipher algorithm is used since it is more robust and cannot be easily attacked. The organization of this paper is as follows: Brief overviews of related works of some existing protocols are presented in Section 2. The proposed hybrid architecture model is discussed in Section 3. In Section 4, algorithm design tools were discussed in this section. Section 5, implantation process with sample message is explained in a detailed structure. Section 6, we analyze the performance and robustness of the new hybrid algorithm and finally, the main conclusion is presented in Section 7.

2. LITERATURE REVIEW

Ijaz Ali Shoukat et al. This study proposes a Generic Hybrid Encryption System based on private and public cryptography. Basically, public key algorithm has more advantage features such as secure and more reliable than private key algorithm, But, it has some limitation such as time consuming, memory wastage and more complicated process etc., Therefore, the hybrid mechanism has implemented to secure more of the user's data and get optimal solution from symmetric and asymmetric key algorithm. Authors proposed PKI based generic hybrid mechanism to find the solution of symmetric and asymmetric algorithm issues. The HES hybrid encryption system supports energy consumption and save memory requirements. Moreover, it protects from password attack, guessing attacks and provides optimal privacy. The generic Hybrid Encryption System model is suitable for all applications [15].

Sushant Susarla et al. discussed about cryptography algorithm, it has been used since a long time to keep a secret messages. Many algorithms are used for different applications; no algorithm is safe to secure message. Since any single encryption mechanism would not fulfill entire process of encryption and decryption. Therefore, authors suggested a hybrid cryptosystem combination of two or more well-known algorithms. Using of hybrid algorithms in a sequence where the output of one algorithm is the input for the next algorithm in the series provides extra security by securing the data. The hybrid mechanism along with the randomness in nature of the selection of the algorithms, their sequence, and the number of algorithms used provides a lot of safety in a multiple layered manner compared to the algorithms used as a single algorithm and moreover, it protects from well-known attacks [34].

Rawya Rizk et al. discuss about security in wireless sensor network cryptography based on the combination of both symmetric and asymmetric cryptographic techniques. The proposed hybrid algorithm is designed with high security, minimized key options and includes cryptography primitives of integrity, confidentiality, and authenticity. The author proposed a hybrid algorithm based on Elliptic curve (ECC) and Advanced Encryption Standard (AES) in the first phase and second phase RSA based XOR used. Hybrid algorithm supports Wireless Sensor Networks and it protects from many attacks of image encryption. The hybrid algorithm finds many issues such as time consumption, computation speed and more secure. The authors named the hybrid algorithm is called THCA cryptography and they compared the existing hybrid models. It is particularly suitable to support image encryption applications [29].

Prakash Kuppuswamy et al. Discussed about mobile data security which has been stored on cloud storage. Many cryptography algorithms provide security services on cloud data storage, although many applications are often attacked by intruders and ultimately end users are becoming a victim. Increasing number of mobile users and its default application and personal application software providers need to store the user's information require enormous storage such as cloud data storage facility. Therefore, many cloud storage providers rely on cryptography techniques to protect the valuable data. Author introduced a dynamic and randomness key generation procedure through Key Distribution Centre(KDC). The new asymmetric key algorithm generates the key based on users request and it can distribute the key between the users temporarily. The new model algorithm works with at least computation time and power consumption [26].

Kapoor Rahul Yadav et al. discussed the network security and its significance towards network supporters and service providers. During data exchange between the sender and receiver, cryptography technique plays a vital role to safe the data. Traditional and symmetric key algorithm is not suitable for many applications, although a new hybrid cryptography algorithm was introduced and it supports more secure and robust to protect the data transmission on open network. The proposed hybrid cryptography system is designed with the combination of well-known RSA, DES, and SHA1 algorithm. The proposed algorithm implemented on JAVA and the result shows the better performance in terms of time complexity and memory [35].

Marwan Ali Albahar et al. In this article, the authors proposed a hybrid algorithm combination of RSA, AES, and TwoFish algorithm. They proposed to implement the above hybrid algorithm on Bluetooth security. Existing Bluetooth security is widely using Advanced Encryption Standard (AES) and it doesn't support high security during the data transfer between the end devices. Proposed hybrid cryptosystems provide triple protection and it enhances the security level during the data transfer between the Bluetooth devices. Authors applied 128-bit key to encrypting the data, first applied AES and the second phase they applied

Twofish, and finally they applied RSA cryptography with 1024 key bits [22].

Prakash Kuppuswamy et al. introduced smart card security using a new symmetric key algorithm. Smart card is widely using in almost all business transactions at present digital era. Many banks provide smart cards to their customers using cryptography techniques. Many financial institutions rely on one of the cryptography algorithms such as Public key, private key and hybrid algorithm authentication scheme. Existing algorithm took more processing time and limited key size. The new algorithm works on arbitrary data, not just only alphabets or integers alone, its supporting combination of alphabets, and its more suitable and supporting to encrypt more text with minimum processing time [26].

Mahalakshmi et al. discussed cloud storage security using the hybrid cryptographic method. The data is stored in a cloud server through some service providers from smaller to larger concern the threat of data becomes a major issue. The combination of private and public-key cryptography systems makes the more security privileges. The hybrid consolidation of symmetric and asymmetric are used to secure the cloud user's data at a greater level of security. The significant benefit of using the hybrid method, it provides affordable key size, solid encryption scheme, and high-speed computational capability. Applying the private encryption and public encryption method the key size is reduced but the complexity of encryption made the unauthorized entities difficult to decrypt the data. Moreover, the authors claimed that the proposed scheme maintained the basic features of data integrity, confidentiality, and security. Hybrid cryptography level one encryption processed with AES and the second level is processed with Elliptic curve cryptography (ECC). The author described the significant benefit of the proposed algorithm that minimizes the encryption time and increases the data encryption speed [37].

Santoso et al. discussed Hybrid Cryptography Scheme. In the present environment, storing the data on cloud storage is inevitable. Cloud data storage located in many remote locations and possibly abusing the cloud user's information. Therefore, it is significant data must be secured so as not to be abused by unauthorized people. Combining data security algorithms would be more secure than a single encryption algorithm. The authors suggested Advanced Encryption Standard (AES) Twofish algorithm combination strengthen the data security from the unauthorized users. Two fish algorithm uses a 256-bit key and generated by the SHA 256 HASH function. The proposed hybrid technique provides better security in the cloud system of data uploading and downloading sequence. The implementation structure shows, it is relatively more secure, and the implementation process also better than other symmetric key algorithms [38].

3. PROPOSED HYBRID ARCHITECTURE

There are many hybrid algorithms that is widely offered depends on their purpose of application and level of security required by the industries. Most commonly RSA cryptography, 3DES, AES and Diffie Hellman key exchange algorithm is widely connected in most of the business. In this proposed model, we merged an extending Linear block cipher and a simple symmetric key using simple negative and positive integer numbers. In *Figure.3*, a hybrid architecture model designed with three exclusive operations of key generation, encryption, and decryption phases. Hybrid algorithm key generation designed on two-part, the first model generated using linear matrix invert by using modulo 37. Secondly, we have chosen the random integer negative and positive number and its inverse number. In this proposed process, it can increase the complexity of the information. The entire encryption and decryption is outlined in the given figure.

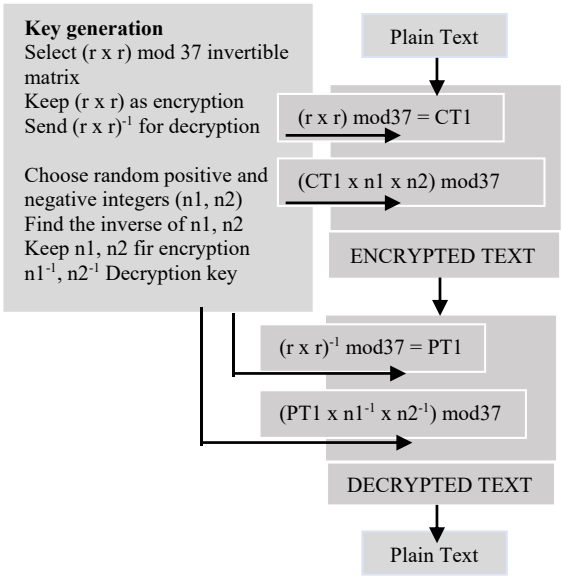

Figure 3: Structure of Hybrid crypto

4. ALGORITHM DESIGNING TOOLS

Cryptographic algorithm is a part of our life, it has been used in our everyday life, such as E-mail, passwords, debit card, credit card, computer password, mobile passwords, Internet banking, biometric systems, online purchases and many more countless applications. In earlier, the use of cryptography was restricted and applied to the safety of information in diplomatic and federal agencies only. Due to the recent development of communication technology, cryptography algorithm leads the private, public, and global industries in a significant level. In short, Hill cipher number of invertible matrices modulo 26 is the product of 2 and13. Therefore, the order of the general linear group GL (n, Z_2) and GL(n, Z_{13}) is:-:-

$$26n^2\ (1-1/2)\ (1-1/2^2)\ \ldots.(1-1/2^n)(1-1/13)\ (1-1/13^2)\ \ldots.(1-1/13^n)\ldots\ldots.. \quad (1)$$

The key space of modulo 26 hill cipher is mentioned in equation (2) and it's (5 x 5) hill cipher based key size about 114 bits.

$$\log_2(26n^2) = 4.7n^2 - 1.7\ \ldots\ldots\ldots\ldots\ldots\ldots. \quad (2)$$

Proposed algorithm based on modulo 37, it is a prime number, therefore the order of the general linear group GL(n, Z_{37}) is

$$37n^2\ (1-1/37)\ (1-1/37^2)\ \ldots.\ldots(1-1/37^n)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \quad (3)$$

The key space of modulo 37 proposed block cipher is mentioned in equation (4) and it's based on (6 x 6) square matrix and its key size about 164 bit.

$$\mathrm{Log}_2(37n^2) = 5.3n^2 - 2.1\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

We do all above activities by combining ideas from across the whole mathematical techniques from probability and statistics, group theory, combinatory and complexity theory, etc., The hill cipher and extended modulo 37 cipher requires following mathematical tools.

4.1 Square matrix

A square matrix of order n has n rows and n columns.

4.2 Determinant of matrix

Let $\boldsymbol{A}$ be an $n \times n$ matrix and c be a scalar then: $\det(cA) = c^n \det(A)$

A square matrix $\boldsymbol{A}$ is invertible if and only if det($\boldsymbol{A}$) ≠ 0. $\boldsymbol{A}$ matrix that is invertible is often called **non-singular** and a matrix that is not invertible is often called **singular**.

· If A is a square matrix then: $\det(A) = \det(A^T)$

4.3 Co-factor of matrix element

The cofactor A_{ij} is the minor M_{ij} multiplied by (−1) raised to the (i+j) power: $A_{ij}=(-1)^{i+j}M_{ij}$

4.4 Minor of element

The first minor M_{ij} associated with the element a_{ij} of an *n*th order square matrix A is the determinant of order (n−1) obtained from the matrix A by deleting the *i*th row and the *j*th column.

4.5 Adjoint matrix

If A is a square matrix of order n, then the corresponding adjoint matrix, denoted as C*, is a matrix formed by the cofactors Aij of the elements of the transposed matrix A^T.

4.6 Transpose matrix

If the rows and columns in a matrix A are interchanged, the new matrix is called the transpose of the original matrix A. The transposed matrix is denoted by A^T.

4.7 Multiplication of matrix

Let A and B be two matrices. The product of the matrices AB exists if and only if the number of columns in the first matrix is equal to the number of rows in the second matrix.

If $A = [a_{ij}]$ is an $m \times n$ matrix and $B = [b_{ij}]$ is an $n \times p$ matrix, the product AB is an $m \times p$ matrix. $AB = [c_{ij}]$, where $c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \ldots + a_{in} b_{nj}$.

4.8 Inverse of matrix

The inverse of a matrix A is defined as a matrix A^{-1} such that the result of multiplication of the original matrix A by A^{-1} is the identity matrix I: $AA^{-1}=I$.

4.9 Modular Arithmetic and Congruent relationship

Modulo and Congruence are an important and useful tool for identifying divisibility. Moreover, it is a significant features of cryptography.

If a and b are integers and n > 0, we write a ≡ b mod n to mean n|(b − a). Then it is called as "a is congruent to b modulo (or mod) n.

1. Reflexivity if, If a ≡ a mod n.
2. Symmetry is, If a ≡ b mod n then b ≡ a mod n.
3. Transitivity is, If a ≡ b mod n and b ≡ c mod n then a ≡ c mod n

5. IMPLEMENTATION OF HYBRID CRYPTOGRAPHY

In the growing internet and web applications, where the large volume of data is transferred on the open network channels, the security concern of safeguarding data privacy is a high priority and foremost task. Security and privacy has become a necessity for either a company or an individual person who is using the web and internet. Linear block cipher is a polygraph substitution classical cryptography based on linear algebra introduced by Lester S. Hill in 1929 [19, 20]. In the existing Hill cipher algorithm, the 26 alphabet letters represented and it's used modulo 26. The proposed algorithm consists 26 alphabets and 0-9 integers as it is mentioned and arranged in the below *Table 1*. The implementation of proposed hybrid algorithm briefly elaborated with sample message.

The implementation process, and further verification of proposed hybrid cryptography, we have chosen the sample text message as, "EXTENDED BLOCK CIPHER MODULO 37". The selected plain text consists of alphabets, integers, and append padding option. The arrangement of plain text is arranged in the following *Table 2*.

Table 2: Sample encryption message

E	X	T	E	N	D	E	D	B	L
5	24	20	5	14	4	5	4	2	12
O	C	K	C	I	P	H	E	R	M
15	3	11	3	9	16	8	5	18	13
O	D	U	L	O	3	7	Pad		
15	4	21	12	15	30	34	37		

The sender chooses the following encryption key and generating the private key using the procedure of linear algebra equation mentioned in Section 4. Encryption key

Sender's Encryption key is $\begin{bmatrix} 2 & 3 & 3 & 2 \\ 3 & 2 & 4 & 4 \\ 5 & 4 & 5 & 5 \\ 3 & 5 & 6 & 2 \end{bmatrix}$

$$\begin{bmatrix} -24 & -13 & 16 & 6 \\ 20 & -5 & -2 & -5 \\ -11 & 7 & -4 & 7 \\ 19 & 8 & -7 & -9 \end{bmatrix} \quad \text{mod } 37$$

Recipient's Decryption key is $\begin{bmatrix} 16 & 32 & 14 & 33 \\ 36 & 28 & 26 & 28 \\ 32 & 20 & 15 & 20 \\ 12 & 7 & 17 & 6 \end{bmatrix}$

5.1 Phase I Assumption tool (Extended hill cipher)

Plain Text is called **PT** and Cipher Text is called **CT**
Selected invertible square matrix is linear block cipher key = k.
Invertible of above matrix is ||17|| and Its inverse is 24. (17*24) mod 37 ≡ 1
Inverse of above matrix is known as decrypt key = k^{-1}

$[k] * [PT] * \text{mod } 37 = [CT1]$ …….. (1)

5.2 Phase II Assumption tool (SSK)

Choose any random integer Positive number i.e k1 and Choose any random integer Negative number i.e k2
Find the inverse of k1 on mod 37 is called $k1^{-1}$
Find the inverse of k2 on mod 37 is called $k2^{-1}$
Hybrid Encryption key = k, k1, k2
Hybrid Decryption key = k^{-1}, $k1^{-1}$, $k2^{-1}$

$[CT1] * [k1] * [k2] * \text{mod } 37 = [Cipher\ Text]$ ……..(2)

Therefore, entire encryption process: -

$[k] * [PT] * [k1] * [k2] \text{ mod } 37 = [Cipher\ Text]$ ……..(3)

Decryption process or Deriving the process of original message

$[k-1] * [CT] * (k1^{-1}) * (k2^{-1}) \text{mod } 37 = [Plain\ Text]$ ……(4)

5.3 Encryption Procedure

For the encryption purpose, we have selected 4 variable square matrix keys, therefore we are arranging here plain text as 4 variable blocks as shown in *Table 3*.

Table 3: Message blocks

4 variable block –Plain Text						
5	14	2	11	8	15	15
24	4	12	3	5	4	30
20	5	15	9	18	21	34
5	4	3	16	13	12	37

The process of hybrid algorithm use in the first phases of the extended linear block cipher algorithm procedure is shown in 1st block of the text and the remaining procedure are same, and the result is summarized in table 4.

$$\begin{bmatrix} 2 & 3 & 3 & 2 \\ 3 & 2 & 4 & 4 \\ 5 & 4 & 5 & 5 \\ 3 & 5 & 6 & 2 \end{bmatrix} * \begin{bmatrix} 5 \\ 24 \\ 20 \\ 5 \end{bmatrix} \text{mod } 37 =$$

$$\begin{bmatrix}152\\163\\246\\265\end{bmatrix} \bmod 37 = \begin{bmatrix}4\\15\\24\\6\end{bmatrix}$$

The second phase of the encryption is also mentioned in the above *Table.4*. In the above table, the user has selected one positive random integer 9, and negative integer -7, and its calculated with derived phase I variables. Finally, the hybrid encrypted text is "G Q E 2 0 U 8 0 B L 27 F 1 L C 4 27 9 7 O M 27 D 7 27 X S W".

5.4 Decryption procedure

Decryption is the process of transforming scrambled message into readable or user understandable messages. Proposed hybrid decryption process is also categorized in phase I and Phase II processing model using simple integer numbers and extended block cipher algorithm. The process of hybrid model equation and implementation procedure is presented here.

$[key\ (inverse\ of\ matrix)]\ *$
$[Encrypted\ \ Text]* [Inverse\ of\ k1] *$
$[Inverse\ of\ k2] \bmod 37 = [PLAIN\ TEXT]$

The process of decryption reveals the data which has been received from the sender. Without proper decryption code or key, the received scrambled message is not possible to retrieve into plain text or original message. Therefore, the decryption key is the leading robustness of any cryptography algorithm. Here, we have already generated a key for decrypting the message to derive the original plain text. In below the matrix calculation is the result of the block1 decryption procedure. Similarly, it has been calculated with a similar procedure to the remaining blocks and the final decrypted message is shown in *Table 5*.

$$\begin{bmatrix}16 & 32 & 14 & 33\\36 & 28 & 26 & 28\\32 & 20 & 15 & 20\\12 & 7 & 17 & 6\end{bmatrix} * \begin{bmatrix}7\\17\\5\\29\end{bmatrix} * [33] * [21] =$$

$$\begin{bmatrix}1166319\\1157310\\844767\\320166\end{bmatrix} \bmod 37 = \begin{bmatrix}5\\24\\20\\5\end{bmatrix}$$

6. EFFICACY OF PROPOSED PROTOCOL

The basic cryptography version of Hill cipher algorithm is susceptible to known-plaintext attacks since the entire encryption procedure is based on linear equations. If the intruder intercept n^2 sets of plaintext and encrypted text equivalent letters can create a linear system is enough to identify the original message. Proposed version of hybrid approach is an ideal approach as we believe that, it will satisfy the fundamental features of cryptography such as integrity, privacy, and security. Significant features of the new model protocol are the key binding of a simple positive and negative integers. The proposed multimodal algorithm approach is suitable for small and medium scale applications. Here, we identified many significant differences of the existing algorithm and the proposed model of extended linear block cipher protocol between the existing and unused Hill cipher algorithm which has been mentioned in the given *Table 6.*

7. CONCLUSION AND FUTURE WORKS

The multiple encryption or hybrid encryption algorithm along with the randomness in nature of the selection of the algorithms, their sequence, and the number of algorithms used provides a lot of safety in a multiple layered manner compared to the algorithms used as stand-alone entity and guards against many well-known attacks. Multimodal algorithm provides integrity, privacy, and more security during the data transmission between users. The user expectation of their personal data should be very safe for transmitting over the open network and it is accomplished by only very powerful algorithm.

Proposed hybrid cryptography provides effective authentication method competent time duration to calculate key generation, encryption and decryption process. In this research article, we have concluded many significant features of extended linear block cipher which has been shown in table 6. Essentially, hill cipher is not in usage due to the security aspects, the robustness is not a competent level for the industry application. However, we have strengthened the security using the prime number of modular 37. Prime numbers are a significant factor that leads the protocol of cryptography algorithm. Normally, any number has at least two factors. Prime numbers have the unique property in that they have exactly two factors 1 and the number itself. Another significant feature of the proposed algorithm, it is suitable to use a combination of alphabets and

integers. Next, it provides padding facility, key bit size, linear matrix size and key space, etc., proposed hybrid protocol is flexible to implement and it can apply many real-time applications such as financial sector, industry, federal, secure data transmission, One-time password, Cloud security, network security and many more limitless applications. This flexibility enables a wide range of industrial applications and enables the accommodation of new environmental spaces as and when they are developed in the future.

REFRENCES:

[1] Adler A, "Images can be regenerated from quantized biometric match score data," *Proceeding of Canadian conference of Electrical and Computer Engineering*, pp. 469-472, 2004.

[2] Adler A, "Vulnerabilities in Biometric Encryption Systems," *International Conference on Audio- and Video-Based Biometric Person Authentication*, vol. 3546, pp. 1100-1109, 2005.

[3] Ali E. Taki El Deen, Design and Implementation of Hybrid Encryption Algorithm, *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Volume 4, Issue 12, December-2013.

[4] Akanksha Samadhiya, Trapti ozha, "Secure Mobile Cloud Storage and Data Transmission", *Int.J.Computer Technology & Applications*,Vol 6 (4),567-570, 2016.

[5] Albahar, M., Haataja, K. and Toivanen. P, "Towards Enhancing Just Works Model in Bluetooth Pairing", *International Journal on Information Technologies & Security*, 8, 67-82, 2016.

[6] Armknecht, F, Krause, M. "Algebraic Attacks on Combiners with Memory, in Advances", *Advances in Cryptology, Lecture Notes in Computer Science, Springer*, Berlin, Heidelberg, 162-175, 2003.

[7] Balitanas, M., "WiFi protected access-pre-shared key hybrid algorithm", *Int. J. Adv. Sci. Technol*, 12, 2007.

[8] Bhanot, R., Hans, R., "A Review and Comparative Analysis of Various Encryption Algorithms", "*International Journal of Security and Its Applications*", 9, 289-306, 2015.

[9] Buhan I.R, Hartel, H, "The state of the art in abuse of biometrics", *Tech TR-CTIT-05-41 Centre for Telematics and Information Technology*, University of Twente, Enschede. ISSN 1381-3625

[10] Burr, W, "Selecting the advanced encryption standard", *IEEE Secur. Priv.* 1 (2), 43–52, 2003.

[11] Chol Soon Jang, Deok Gyu Lee, Jong-wook Han, Jong Hyuk Park, "Hybrid security protocol for wireless body area Networks", *Wireless Communications and Mobile Computing*, Vol.11, P 277-288, 2011.

[12] Frunza, M., Asachi, Gh., "Improved RSA encryption algorithm for increased security of wireless networks", *In: ISSCS International Symposium*, vol. 2, 2007.

[13] Gampala V, Inuganti S, Muppidi S, "Data Security in Cloud Computing with Elliptic Curve Cryptograph", *International Journal of Soft Computing and Engineering* (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-3, July 2012.

[14] Hermelin, M, Nyberg K, "Correlation Properties of the Bluetooth Combiner", *Information Security and Cryptology—ICISC'99,* Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 17-29, 2000.

[15] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Subariah Ibrahim, "A Generic Hybrid Encryption System (HES)", *Research Journal of Applied Sciences, Engineering and Technology* 5(9): 2692-2700, 2013 ISSN: 2040-7459, 2013.

[16] Johnson, D., Menezes, A., Vanstone, S., "*The elliptic curve digital signature algorithm (ECDSA)*, *Int. J. Inf. Security* 1 (1), 36–63, 2001.

[17] Kapoor V, Rahul Yadav, "A Hybrid Cryptography Technique for Improving Network Security", *International Journal of Computer Applications* (0975 – 8887) Volume 141 – No.11, May 2016.

[18] Kodali, R., Sarma, N., "Energy efficient ECC encryption using ECDH. In: Emerging Research in Electronics", *Computer Science and Technology,Lecture Notes in Electrical Engineering*, vol. 248. Springer, pp. 471–478, 2013.

[19] Lester S. Hill, "Cryptography in an algebraic alphabet", *Amer. Math.* Monthly 36, 306–312, 1929.

[20] Lester S. Hill, "Concerning certain linear transformation apparatus of cryptography", *Amer. Math. Monthly* 38, 135-154, 1931.

[21] Lu Y, Vaudenay, S, "Faster Correlation Attack on Bluetooth Keystream Generator", *Advances in Cryptology—CRYPTO 2004,*

Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 407-425, 2004.

[22] Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, "Novel Hybrid Encryption Algorithm Based on AES, RSA, and Twofish for Bluetooth Encryption", *Journal of Information Security*, 9, 168-176, ISSN Print: 2153-1234, 2018.

[23] Misbha iurm, Aihab Khan, Malik Sikander Hayat Khiyal, "Confidentiality of Messages in a cardless electronic payment system", *International Journal of Reviews in Computing*, Vol. 6, ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336, 15th July 2011.

[24] Prabhakar S, Pankanti S, Jain A.K, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security and Privacy Magazine,* Vol. 1, No. 2, pp. 33-42, March-April 2003.

[25] Prakash Kuppuswamy, "Enrichment of Mobile Data Security over Cloud storage using New Asymmetric key algorithm", *International Journal of Computer Sciences and Engineering* Vol.-3(10), E-ISSN: 2347-2693, Oct 2016.

[26] Prakash Kuppuswamy, Shanmugasundaram Marappan, Rajan John, "Novel Approach Design and Implementation of Smart Card Security based on Symmetric Key Algorithm", *International Journal of Computer Engineering and Applications*, Volume XII, Issue I, www.ijcea.com ISSN 2321-3469, Jan 2018.

[27] Praphul M.N, Nataraj K.R, "FPGA Implementation of Hybrid Cryptosystem", *International Journal of Emerging Science and Engineering (IJESE)* ISSN: 2319–6378, Volume-1, Issue-8, June 2013.

[28] Ratha A, Connell. J, Bolle R, "Enhancing security and privacy in biometric-based authentication systems," *IBM Systems Journal*, Vol. 40. No. 3, pp. 614 - 634, 2001.

[29] Rawya Rizk, Yasmin Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks", *Journal of Electrical Systems and Information Technology* 2, 296–313, 2015.

[30] Rege, K., Goenka, N., Bhutada, P, Mane, S, "Bluetooth Communication Using Hybrid Encryption Algorithm Based on AES and RSA", *International Journal of Computer Applications*, 71, 10-13, 2013.

[31] Shanta, J.V, "Evaluating the Performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard)", *International Journal of Computational Engineering & Management*, 15, 43-49, 2012.

[32] Singh, G, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", *International Journal of Computer Applications*, 67, 33-38, 2013.

[33] Stallings, W., "Cryptography and Network Security: Principles and Practices", *Pearson Education,* India, 2006.

[34] Sushant Susarla, Gautam Borkar, "Hybrid Encryption System", *International Journal of Computer Science and Information Technologies*, Vol. 5 (6) , 7563-7566, 2014.

[35] Vivek Kapoor, Rahul Yadav, "Hybrid Cryptography Technique to Support Cyber Security Infrastructure", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 4 Issue 11, November 2015.

[36] Smita Sharma, R.P. Singh, "The Cryptography Based Security Algorithm for Protecting Sensitive Information in Cloud Environment", *International Journal of Scientific & Technology Research*, Volume 8, Issue 11, November 2019.

[37] Mahalakshmi. B, Suseendran. G, "A Hybrid Cryptographic Algorithm for Securing Data in Cloud Storage", *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 11, 06-Special Issue, 2019.

[38] Santoso K, Muin. A, Mahmudi. A, "Implementation of AES cryptography and twofish hybrid algorithms for cloud", *BIS-ASE 2019 Journal of Physics: Conference* Series1517, 2020.

[39] Umair Khadam, Muhammad Munwar Iqbal, Meshrif Alruily, Mohammed A. Al Ghamdi, Muhammad Ramzan, Sultan H. Almotiri, "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions", *Wireless Communications and Mobile Computing* Volume 2020.

Journal of Theoretical and Applied Information Technology
31st May 2021. Vol.99. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

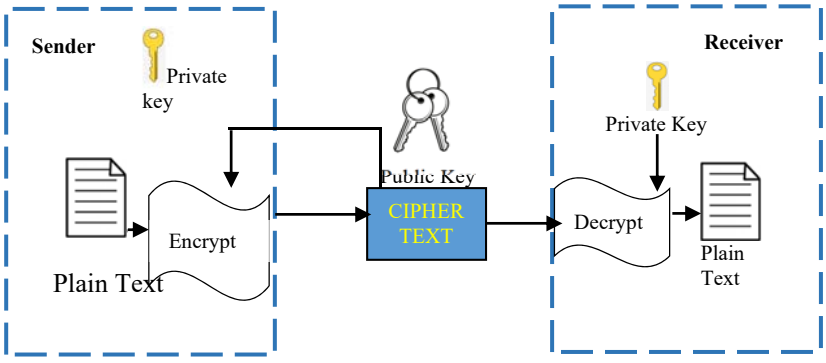

Figure 1: Asymmetric key algorithm module

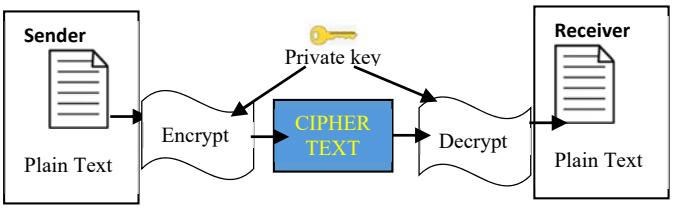

Figure 2: Symmetric key algorithm module

Table 1:. Synthetic data of proposed algorithm

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Letter	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	Pad	
Number	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	

Table.4: Encrypted message

E	X	T	E	N	D	E	D	B	L	O	C	K	C
5	24	20	5	14	4	5	4	2	12	15	3	11	3
I	P	H	E	R	M	O	D	U	L	O	3	7	Pad
9	16	8	5	18	13	15	4	21	12	15	30	34	37
ENCRYPTED TEXT													
4	15	24	6	26	12	20	26	17	28	0	14	16	28
D	O	X	F	Z	L	T	Z	Q	1	27	N	P	1
7	23	0	10	30	35	18	0	34	30	0	19	32	29
G	W	27	J	3	8	R	27	7	3	27	S	5	22
Phase I Encrypted Text - “D O X F Z L T Z Q 27 N P 1 G W 27 J 3 8 R 27 7 3 27 S 5 22”													
Phase-II SSK algorithm Choose random positive (9) & negative integer (-7) and multiply with Encrypted Text													
7	17	5	29	27	21	35	27	2	12	0	6	28	12
G	Q	E	2	0	U	8	0	B	L	27	F	1	L
3	31	0	36	34	15	13	0	4	34	0	24	19	23
C	4	27	9	7	O	M	27	D	7	27	X	S	W
Hybrid cipher Text - “G Q E 2 0 U 8 0 B L 27 F 1 L C 4 27 9 7 O M 27 D 7 27 X S W”													

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: Decryption process

7	17	5	29	27	21	35	27	2	12	0	6	28	12
G	Q	E	2	0	U	8	0	B	L	27	F	1	L
3	31	0	36	34	15	13	0	4	34	0	24	19	23
C	4	27	9	7	O	M	27	D	7	27	X	S	W
Decrypted Message using Key Inverse of (k, k1, k2)													
5	24	20	5	14	4	5	4	2	12	15	3	11	3
E	X	T	E	N	D	E	D	B	L	O	C	K	C
9	16	8	5	18	13	15	4	21	12	15	30	34	37
I	P	H	E	R	M	O	D	U	L	O	3	7	Pad

Table 6: Comparison Analysis of protocol

Features	**Linear Block cipher (mod 26)**	**Extended Linear Block cipher (mod 37)**
Text support	A to Z	A to Z and 0 to 9
Key bits	114 bits	164 bits
Modular	Mod 26	Mod 37
Matrix size	5 x 5 square matrix	6 x 6 square matrix
Key Space	$\log_2(26n^2) = 4.7n^2 - 1.7$	$\log_2(37n^2) = 5.3n^2 - 2.1$