Eng. Sci., 2022, **19**, 279–284

Engineered Science

DOI: https://dx.doi.org/10.30919/es8d705

A Table-Based End to End Encryption Technique Without Key Exchange

Aakash Bharadawaj Srinivasan,[1] Hemalatha S[2,*] and Ramathmika[2]

Abstract

Communication has become an integral part of all beings—both living and non-living. In most cases, everyone likes to keep their communication personal and secure. Additionally, high-level information is expected to be secure. One of the methods to secure information is encryption, where the information is safeguarded so that it cannot be detected by anybody other than the intended recipient. In an encryption method, key management is essential for proper communication. The exchange of keys may lead to leakage, modification, or change of the keys during transmission. Even in public-key cryptography, the key management problem exists. The proposed method aims to reduce this problem by eliminating key transfers during the encryption-decryption process. The present study uses the Internet Protocol (IP) addresses of the sender and the receiver to securely encrypt the message. The channel is tightly secured in the proposed algorithm as there is no key transfer during encryption and decryption techniques. A table generated by a polynomial function that produces non-linear outputs is used for producing the ciphertext. This ensures that the communication is secure against multiple man-in-the-middle attacks. The complexity of the proposed algorithm is computed and is found to be Big O notation (O(n)).

Keywords: Encryption; Decryption; Key Exchange; Cipher; IP address.
Received: 08 November 2021; Revised: 11 February 2022; Accepted: 05 May 2022.
Article type: Research article.

1. Introduction

Encryption and decryption are important in the secure transmission of a message. Without proper cryptic algorithms in place, the message can be easily intercepted and misused. A man-in-the-middle can attack using brute force and can easily capture the message transmitted. Almost all the data transmitted is sensitive in today's world and anyone cannot afford to leak important information. Anything from a basic messaging app to a bank's internal server is prone to cyber-attacks and hence the sensitive information must be dealt with cautiously.

Encryption is the most sought-after method to ensure the secure transmission of information. Numerous encryption methods are in use today. Most of these techniques use a key to encrypt—which plays a major role in generating the cipher. Key management is understandably one of the biggest problems in the cryptosystem. The key, along with the message, can be fed to a supercomputer and brute force techniques can break down the ciphertext within minutes. To avoid such a threat of exposure the key must be eliminated.

The algorithm used in the encryption process is equally important. A loosely encrypted message is equivalent to a simple transmission of plaintext without any security. Hence, in most encryption algorithms, public or private keys are used to strengthen the cryptic message. The key protects the transmitted message using various encryption techniques. But unfortunately, even the keys are subjected to attacks. Once the key and the encrypted message are obtained, they can be fed into super processors for decryption.

The method proposed in the present study, which does not involve any key exchange, is based on a table constructed at both the sender's and the receiver's sides. The message to be encrypted is mapped to the table and the character obtained is substituted to generate the cipher. Another round of encryption is employed to reduce the length of the generated cipher.

In the proposed methodology, the transmission of the key doesn't occur and hence, the risks of using a key for public and private key encryption techniques are eliminated. A detailed comparison of multiple published studies is carried out and the similarities and differences between these

[1] *Robert H. Smith School of Business, University of Maryland, College Park, Maryland 20742, USA.*
[2] *Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal -576104, Udupi, Karnataka, India.*
**Email:* hema.shama@manipal.edu (H. Shama)

algorithms with the proposed algorithm are laid down.

A conventional cryptographic method is usually symmetric—where a single key is used for both encryption and decryption, or asymmetric—where a public key is used for encryption and a private key is used for decryption. In both models, the keys are essential, i.e., there should be an occurrence of key exchange for the communication to be effective. Most of the encryption algorithms found in the literature study or being used currently in different applications require a key and hence, key management is one of the major concerns to the researchers.

Encryption is extensively used in almost all domains of technology, such as networking, e-commerce, banking, and database management. In some cases, the encrypted data transmission is assessed using the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).[1] TCP guarantees data transmission by acknowledgment services and when packets are lost, retransmission happens. UDP sends packets without confirmation and multiple packets are lost in a single call. The chaining encryption algorithm for low-power wide-area networks (LPWAN) uses a key that is assigned to each message using hash functions.[2] However, the algorithm fails if there is a collision in the hash function. An efficient data encryption method based on Blockchain Technology prevents data loss and data distortion in an E-Commerce Platform.[3] It is a simple and effective process to encrypt E-Commerce data. In the encryption and decryption process, the bit error rate and the packet loss rate are low. But the algorithm uses a key-based encryption structure to ensure the accuracy of data. The key transfer might be easily compromised in this technique and might lead to a data leak.

Chinese cryptographic bases are used in an encryption method to secure instant messaging by exploiting blockchain and machine learning algorithms.[4] This involves the transfer of both the private and public keys of the users for message authentication. A cryptographic hash is used for message integrity and message encryption is used for protecting the privacy of users. Since this technique involves a private key, the key must be transferred before the message and hence information can be tapped during the transfer. Cryptography and graphs are explored vastly in the encryption techniques and public-key encryption methods are proposed based on a graph.[5] Here, the graph generated from the given message is encrypted. The encryption is based on the properties of the matrices which are generated from the graph. The properties of the graphical codes are used for decrypting the message. These proposed algorithms have key generation, sender-side graph generation, and receiver-side decryption. This might prove costly as the key is used to form the matrix for the required graph in the encryption process.

In a hybrid cryptosystem, which is a combination of Hill Cipher and Elgamal, the encryption is carried out using Hill Cipher and the Hill cipher key is encrypted using Asymmetric Elgamal.[6] The running time of this algorithm is directly proportional to the length of the text used during the encryption and decryption process. This algorithm uses public and private keys for its encryption technique and the final data is sent to the web application platform. A drawback of the study is that the running time increases as the length of the text increases.

Rivest Cipher 4 RC4+ and Variably Modified Permutation Composition (VMPC) algorithms have a three-pass protocol scheme that is adopted for key exchange.[7] The complexity of the algorithm comprises the process of the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). The symmetric algorithm proposed in the study cannot be signed and hence it is prone to a man-in-the-middle attack. A fast cryptosystem with identical encryption and decryption process employs one keystream generator, plaintext operations, and 180-degree matrix rotation.[8] This proposed method is an alternative for establishing secured communications. But for message transfer in e-commerce platforms, encryption is not stable.

The encryption techniques in Wireless Sensor Networks emphasize the need for an increase in security levels in wireless networks and a reduction in energy consumption.[9] The study increases the security in the key transmission phase by using dynamic keys but fails to address the location-prone attack on the dynamic key transfer. The hacker can navigate the location or use Virtual Private Network to morph the location used. Further, in the physical layer encryption against chosen plaintext attacks, the algorithm discusses the ciphertexts which are dynamically generated by incorporating random input data.[10] The algorithm requires a huge space to store the key.

Encryptions using hill cipher usually have the key matrix generated randomly. In certain scenarios, the key matrix is generated using sequential advancement and predetermined by permuted procedures.[11] An algorithm based on a public key is proposed for healthcare where a receiver can use a private key system and the data is sent to the cloud.[12] Unfortunately, the listed studies are very much prone to public and private key attacks.

A concept called designated cloud server using authenticated encryption technique is used for the remote storage system.[13] The authenticated encryption technique proposed doesn't allow an attacker to decipher the text. A modification of the Cayley-Purser algorithm is carried out using a general linear group instead of a Galois field.[14] This ensures the key of the algorithm is harder to obtain but doesn't eliminate the key. A compression encryption scheme that focuses on encrypting multimedia content uses Latin Square Cipher and symmetric keys.[15] Although the algorithm promises high speed, the Latin Square Cipher uses a short key. Asymmetric image encryption which uses the Massey Omura scheme requires the sender and the receiver to agree on public parameters before the encryption begins.[16] An optical encryption algorithm involving a focus tunable lens uses the fractional order of the transform as an encryption parameter.[17] In the novel color image encryption process, the encryption

and inverse processes are put forward for large key space to counter brute force attacks.[18] For encryptions ranging across multi-users, a Multi Key Homomorphic encryption supports an optimized re-linearization algorithm that uses rescaling technology.[19] A new lightweight block cipher called SCENERY is applied to hardware and software platforms.[20] The encryption process of SCENERY uses an 80-bit key. All these methods involve key exchange for the encryption-decryption process.

2. Proposed encryption method

A good communication channel is determined by its strong encryption algorithm. The message transmitted will be subjected to various attacks by hackers. A small loophole in the encryption process can lead to compromising sensitive data. The encryption method proposed in the present study is depicted in Fig. 1 and it works as follows:

Two polynomials—generator polynomial (G(x)) and producer polynomial (P(x)) should be selected. The Functions of G(x) and P(x) are carefully computed after multiple trailed runs. A linear equation (3x-4) is taken for G(x) (Equation (1)) because the generator function runs multiple times. Taking anything more than a binomial tends to increase the time complexity of the algorithm. The coefficients of the binomial are 3 and 4 as that is the maximum integer number that can be assigned without increasing the length of the string during encryption. For the same reason, there is a '-' (minus) sign to bring down the length of the encrypted string. A quadratic equation (x^2-x+1) is taken for P(x) (Equation (2)) because P(x) has lesser iterations than G(x) and can afford to stay in the quadratic equation. The goal is to have a higher degree equation as it brings down the possibility of brute force. Several trial runs were conducted for P(x) and with an effort to reduce the length of the encrypted string, the '-' (minus) is used as mentioned before.

The iterator value x for the polynomials is computed from the IP addresses of the sender and the receiver. The initial values P(1) and G(1) are computed after passing the polynomials through the Euler's constant. The subsequent values of G(y) and P(y) for 1 < y < = 256 are computed from G(y-1). If P(y) > 99999, only the first 5 digits are taken to make sure the message is not long. A cross table is constructed mapping each of the 256 American Standard Code for Information Interchange (ASCII) characters to one distinct P(y) value. Hence, the message is replaced by a numerical value or string of decimal digits after substituting the values from the cross table for every character in the message. This resultant encrypted message may end up being too large. So, a complex cipher table is constructed, which maps a group of two or three digits to a single ASCII character. The method is explained in detail in the following sub-sections. One example is also given as an illustration.

2.1 Encryption

Step 1: Obtain the IP addresses of the sender and the receiver namely S and R respectively.

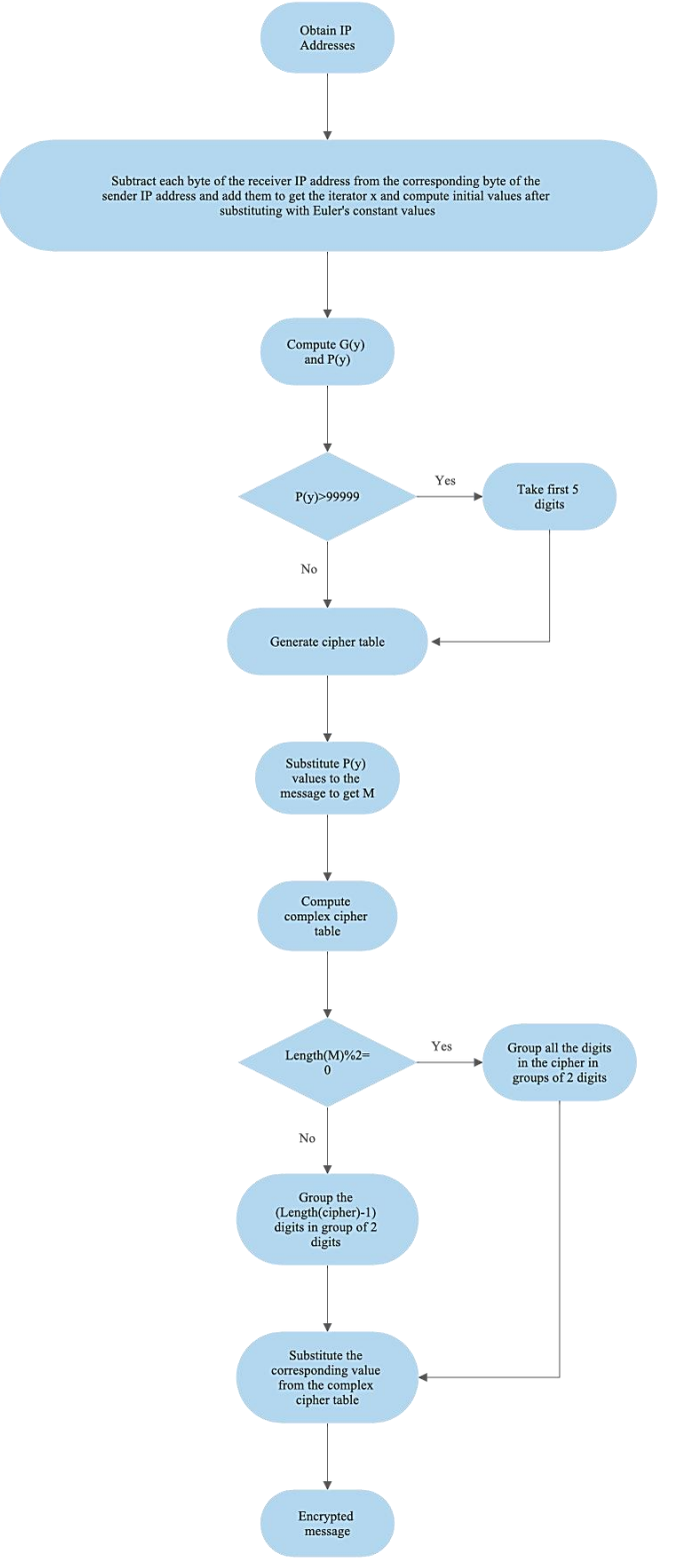

Fig. 1 Flowchart of the proposed algorithm.

Step 2: Obtain Generator G(x) and Producer P(x) using Equations (1) and (2), respectively.

$$G(x) = 3x - 4 \quad (1)$$

$$P(x) = x^2 - x + 1 \quad (2)$$

Step 3: Subtract each byte of the receiver IP address from the

corresponding byte of the sender IP address and add the resultant differences to get the iterator x.

Step 4: Substitute each digit of the iterator x with the value from the corresponding positions after the decimal point of the Euler's constant (2.71828182845904523536028 7…)

Step 5: Compute initial values using Equations (3) and (4):

$$G(1) = G(x) \quad (3)$$

$$P(1) = \mathrm{P}(\mathrm{G}(1)) \quad (4)$$

Step 6: Compute 256 values for P corresponding to all the 256 ASCII characters and store it in the cipher table with the mapping P(1) for a, P(2) for b, and so on. Hence, the cipher table will have 2 columns - a list of alphabets and characters in one column and its corresponding P(y) values in the other column. P(1) is computed using Equation (1). Since there are 256 characters, P(2) to P(256) are computed as follows Equations (5) and (6). For values of y = 2 to y < = 256:

$$G(y) = G(G(y-1)) \quad (5)$$

$$P(y) = \mathrm{P}(\mathrm{G}(\mathrm{y})) \quad (6)$$

If P(y) > 99999, take the first 5 digits.

Step 7: Obtain the cipher by substituting from the cipher table for each character in the plaintext. If the cipher length is to be reduced, construct the complex cipher table and obtain the reduced ciphertext as follows.

Step 8: If the Length (cipher) % 2 = 0, then group all the digits in the cipher in a group of 2 digits else, group the (Length(cipher) – 1) digits in a group of 2 digits.

Construct the complex cipher table by mapping each pair of digits to the printable characters. If the length of the cipher is odd, keep the unpaired digit as it is in the final ciphertext. Fig. 1 explains the processing of the IP addresses to get the iterator x and encrypt the message using the cipher table as described in steps 1 through 8.

2.2 Decryption

Obtain the decipher table using IP addresses and the complex decipher table similar to the complex cipher table at the sender side. If the ciphertext received contains alphabets and other characters, use the complex decipher table to get the message containing digits, and then group them in a sequence of 5 digits. Now, use the decipher table to get the plaintext.

The algorithm is illustrated with examples along with a cipher table and complex cipher table in the Supporting document.

2.3 Security Analysis

The algorithm involves the IP addresses of the sender and the receiver. Two equations namely the generator polynomial and producer polynomial as mentioned in Equations (1) and (2) are also used. Once the message is substituted for the generated words from the producer polynomial, a layer of morphing is carried out with the help of a cipher table before the message is finally transmitted.

Even if the hackers tap the IP addresses of the sender and the receiver, it will be difficult for them to predict the generator and the producer polynomial. Guessing these polynomial functions will not work for the man-in-the-middle as the first iterator has to be fed to the generator polynomial, without which the algorithm will not work. The Euler's constant is an essential part of the algorithm and finding out the usage of the same is highly unlikely. Moreover, the producer polynomial is linked to the generator polynomial and if the connection is not laid out, decoding the message is tedious. In addition, another cryptic table is used to morph the already encrypted text, and hence, it is a Herculean task for the hacker to obtain the following and do them in the right sequence. In conclusion, it is very hard to tap the components of the algorithm and lay the algorithm in the correct sequence to break the encryption.

The importance of combining the IP address with the Euler's constant, an irrational number is explained in this paragraph. If an irrational number like Euler's constant, without the IP address, is used in the initial encryption phase, all the letters will have a different value. The drawback is that when the hacker taps one million messages and maps them, he/she will find a pattern with all 'A's in the message having the same corresponding encrypted text, all 'B's in the message having the same corresponding encrypted text, and so on. When the IP addresses are included, a communication message between Sender 1 and Receiver 1 will have a different corresponding ciphertext when compared to a communication message between Sender 2 and Receiver 2 as the IP addresses are all different. The encryption algorithm based on a chaotic map has 4 values as keys and the key is randomly chosen between these values.[8] This technique makes it difficult to decrypt but if the hacker has more data, he/she can segregate and map it. In the present study, the IP addresses deal with this issue and give out a different ciphertext for the same character as the IP addresses change during every communication passage.

3. Result in analysis

The algorithm is analyzed by plotting the non-linearity graph of P(y) and by computing the time complexity. This algorithm was tested in a system with a Lenovo i5 processor, 256 GB Solid State Drive (SSD), and 8 GB Random Access Memory (RAM).

3.1 Non-linearity

The plot of P(y) values for the alphabets is shown in Fig. 2 explaining the random behavior of P(y) corresponding to the alphabets used. From the graph, it is evident that the P(y) values do not form linear lines and hence are not prone to value-range guessing and mapping of cryptic messages. One common technique of breaking encryption algorithms is by predicting values after analyzing the patterns of the algorithm. As plotted in the graph, for the algorithm in the present study, the values are completely different for every conversation happening between two distinct people. In addition to this, the result of the first phase of encryption goes through a complex cipher table and thus increases the security of the message.

Hence, it becomes difficult for the man-in-the-middle to understand the sequence and predict the next value.

Using brute force to decode the encryption algorithm proposed in the present study, will take multiple iterations and it has to go through two table mapping. It would result in a guessing game and no pattern can be drawn as the P(y) values when plotted on a graph as in Fig. 2 gives no significant inference.

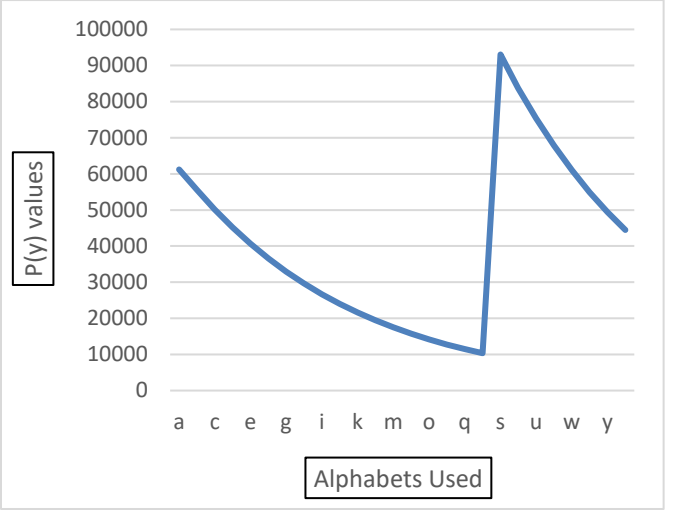

Fig. 2 The unpredictable graph obtained from values of P(y).

3.2 Time Complexity

The algorithm is implemented and tested end to end in the C++ programming language. The time complexity is computed as O(n) which is supported by the following steps:

Step 1: To get the IP addresses of the sender and the receiver as 4 octets each (1 octet = 8 bits), the Time Complexity = O(1).

Step 2: To calculate iterator x, Equations (7) to (11) are used.

$$x1 = SenderIP\ Octet1 - ReceiverIP\ Octet1 \quad (7)$$

$$x2 = SenderIP\ Octet2 - ReceiverIP\ Octet2 \quad (8)$$

$$x3 = SenderIP\ Octet3 - ReceiverIP\ Octet3 \quad (9)$$

$$x4 = SenderIP\ Octet4 - ReceiverIP\ Octet4 \quad (10)$$

$$x = x1 + x2 + x3 + x4; \quad (11)$$

Hence, Time Complexity = O(1)

Step 3: To compute G(1) and P(1) as G(1) = G(x) and P(1) = P(G(1)), the Time Complexity = O(1).

Step 4: To compute 256 values for P as G(y) = G(G(y-1)) and P(y) = P(G(y)), the Time Complexity = O(n).

Step 5: To construct the complex cipher table, the Time Complexity = O(1).

Hence, the worst-case time complexity from the analysis is computed as O(n). A similar time complexity of O(n) was found in VMPC[7] and Identity-Based Encryption with a Filtered Equality Test.[12] In the case of Identity-Based encryption techniques, the encryption process takes a longer time than decryption but in the present study, both encryption and decryption process complexity was found to be O(n). In location-based data encryption for wireless sensor networks[9] and chaotic encryption algorithm,[10] the time complexity was found to be 4N and 2N, respectively, where N is the length of the message.

3.3 Running time of encryption

The running time of encryption when executed in an i5 processor with 8GB RAM, is shown in Table 1 with different sample plaintexts.

Table 1. Running Time of Encryption.

Sl. No.	Plaintext	Running Time
1.	Dogs	0.002 s
2.	Horses	0.003 s
3.	Hello! How are you?	0.005 s

It is observed that the running time increases as the length of the plain text increases. Similar characteristic traits of the running time are recorded in Blockchain Technology to prevent data loss and data distortion in an E-Commerce Platform[3] and Modified Permutation Composition algorithms[7] where the running time is directly proportional to the length of the plaintext.

Studies proposed Blockchain Technology to prevent data loss and data distortion in an E-Commerce Platform,[3] instant messaging by exploiting blockchain and machine learning algorithms,[4] and Identity-Based Encryption[12] involve either a public key or a private key or both during the encryption process. The algorithm implemented in the present study completely omits the concept of using keys and secures the transfer of the message. The algorithm used in the three-pass protocol scheme for data security cannot be signed digitally.[7] The encryption method proposed in the present study can be signed digitally using various hashing techniques if required.

4. Applications

This proposed algorithm can be used for various purposes like satellite communication or rockets in space where the scientists are aware of the IP address of the satellite or the rocket. They will be able to send and receive the message successfully without any other country attempting to get their feed data. The data is very sensitive and a man-in-the-middle attack in such cases would be expensive. To secure high-level information in such scenarios, the algorithm proposed in the current study can be used.

End to End encryption has been widely used these days by various messaging mobile applications and hence the proposed algorithm can provide the required backend encryption layer for a new application. It can also serve as an additional layer of encryption over the already existing cryptic system of the application.

5. Future scope and conclusion

One of the disadvantages of this method is that the sender and the receiver should know each other's IP addresses. The future scope is to make the cipher generation more complex. Secure transmission of data involves advanced cryptography. To

ensure the safety of data, a huge leap towards encryption of data is essential. Key-based encryption techniques become very vulnerable to man-in-the-middle attacks. Furthermore, with the advancement in computing, brute force can decrypt the message once the key is obtained. The algorithm is proposed to counter the vulnerabilities posed by key transfer and hence an effort is taken to abolish the transfer of key to make it less vulnerable. In the proposed algorithm, the message is encrypted by constructing a generator polynomial and producer polynomial without using a key. Corresponding new characters are replaced in the message and the obtained ciphertext undergoes a reduction in length when values from the complex cipher table are substituted. The decryption process involves similar steps and thus the message transfer is not compromised. The complexity of the algorithm is O(n). The graph generated for the Producer polynomial (Fig. 2) shows the random behavior of the encryption process. Hence, the message is tightly secured while being transmitted in the communication passage.

Conflict of Interest

The authors declare no conflict of interest.

Supporting information

Not applicable.

Reference

[1] S. Suherman, S. Panjaitan, A. Ginting, *Journal of Physics: Conference Series*, 2019, **1235**, 012032, doi: 10.1088/1742-6596/1235/1/012032.

[2] A. Bidgoly, H. Bidgoly, *IEEE Sensors Journal*, 2019, **19**, 7027-7034, doi: 10.1109/jsen.2019.2910850.

[3] F. Gao, *Discrete and Continuous Dynamical Systems*, 2019, **12**, 1457-1470, doi: 10.3934/dcdss.2019100.

[4] H. Yi, *Safety Science*, 2019, **120**, 6–13, doi: 10.1016/j.ssci.2019.06.025.

[5] D. Sensarma, S. Sarma, *International Journal of Innovation and Technology*, 2019, **8**, 2273-2279, doi: 10.35940/ijitee.J1133.0881019.

[6] D. Rachmawati, A. Sharif, Ericko, *Journal of Physics: Conference Series*, 2018, **1235**, 1-7, doi: 10.1088/1742-6596/1235/1/012074.

[7] M. Budiman, D. Rachmawati, R. Badegeil, *Journal of Physics: Conference Series*, 2019, **1235**, 012085, doi: 10.1088/1742-6596/1235/1/012085.

[8] P. Cheng, H. Yang, P. Wei, W. Zhang, *Nonlinear Dynamics*, 2015, **79**, 2121-2131, doi: 10.1007/s11071-014-1798-y.

[9] H. Lin, *Wireless Networks*, 2015, **21**, 2649-2656, doi: 10.1007/s11276-015-0938-8.

[10] X. Yang, Z. Shen, X. Hu, W. Hu, Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission, *IEEE Photonics Technology Letters*, 2016, **28**, 2499-2502, doi: 10.1109/lpt.2016.2601659.

[11] R. Mahendran, K. Mani, Generation of key matrix for hill cipher encryption using classical cipher, *2017 World Congress on Computing and Communication Technologies (WCCCT)*, 2017, **1**, 51-54, doi: 10.1109/WCCCT.2016.22.

[12] Y. Ming, E. Wang, *Sensors*, 2019, **19**, 1-22, doi: 10.3390/s19143046.

[13] V. Chenam, S. Ali, *Computer Standards & Interfaces*, 2022, **81**, 1-21, doi: 10.1016/j.csi.2021.103603.

[14] S. Khlebus, Faris Hasoun, K. Rajaa, B. Sabri, *International Journal of Nonlinear Analysis and Applications*, 2022, **13**, 707-716, doi: 10.22075/ijnaa.2022.5559.

[15] A. Bensaoud, J. Kalita, *Journal of Information Security and Applications*, 2022, **64**, 1-21, doi: 10.1016/j.jisa.2021.10303.

[16] K. G. Abdulhussein, N. M. Yasin, I. J. Hasan, *International Journal of Electrical and Computer Engineering*, 2022, **12**, 103057, doi: 10.1016/j.jisa.2021.103057.

[17] J. Alexis Jaramillo-Osorio, W. Torres-Sepúlveda, A. Velez-Zea, A. Mira-Agudelo, J. Fredy Barrera-Ramírez, R. Torroba, *Optics & Laser Technology*, 2022, **148**, 107689, doi: 10.1016/j.optlastec.2021.107689.

[18] C. F. Duan, J. Zhou, L. H. Gong, J. Y. Wu, N. R. Zhou, *Optics and Lasers in Engineering*, 2022, **150**, 106881, doi: 10.1016/j.optlaseng.2021.106881.

[19] X. Yang, S. Zheng, T. Zhou, Y. Liu, X. Che, *Tsinghua Science and Technology.*, 2021, **27**, 642-652, doi: 10.26599/TST.2021.9010047.

[20] J. Feng, L. Li, *Frontiers of Computer Science*, 2021,**16**, 163813, doi: 10.1007/s11704-020-0115-9.

Author Information

Aakash Bharadawaj Srinivasan *has a Bachelor's in Information Technology and is currently pursuing his Masters' in Business Administration. He has published multiple papers across cryptography, Internet of Things and Natural Language Processing.*

Hemalatha S *is an Associate Professor (Senior-Scale) in the Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India. She received her MTech and Ph.D degree from MIT Manipal, India. Her research interests include information security, image processing, computer architecture and machine learning.*

Ramathmika *has Bachelor's in Computer Science and Engineering from Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India and is currently working for an IT company.*

