Improved Symmetric Key Technique Using Randomization

Anshu Chaturvedi[1] and Hirendra Singh Sengar[2(✉)]

[1] Department of Master of Computer Applications, M.I.T.S., Gwalior 474005, India
anshu_chaturvedi@yahoo.co.in
[2] SOS in Computer Science & Applications, Jiwaji University, Gwalior 474011, India
hirendra.sengar@gmail.com

Abstract. Cryptography is the process of turning something readable into something unreadable. Nowadays, internet is being used by the people for exchanging information electronically. The rapid growth of internet increased the number of electronic transactions made by internet users. The information traveled over the internet is very much confidential which need to be secured from unauthorized access, resulted the need of cryptography. In this paper, an innovative technique has been proposed where the three symmetric keys were generated through a randomization process and used for encryption and decryption. Combination of three random keys was used in the encryption process which makes this technique unbreakable and secured against brute force attack and other similar attacks. This technique generates different-different ciphertext each time for the same message which also ensures the protection against various cryptanalytic attacks. This technique can be used to encrypt and decrypt the alphanumeric data in milliseconds which makes the technique more efficient.

Keywords: Symmetric key cryptography · Encryption · Decryption
Cryptanalysis

1 Introduction

The symmetric key cryptography is also known as secret key cryptography where same keys are used for both encryption and decryption.

Cryptanalysis is a technique used to find out the weaknesses in the system for breaking the code used in the encryption process without knowing the secret keys. Cryptanalysis is the study of knowing how the system works and finding a private key. Cryptanalysis is also known as the technique for cracking the code or breaking the code. The cryptanalyst can use one or more attacks' model to break the cipher, depending on what information is available and what type of cipher is being analyzed.

In network security and cryptography domain, some major cryptanalytic attacks are as follows-

- Ciphertext only attack (Brute force attack)

S. Verma et al. (Eds.): CNC 2018, CCIS 839, pp. 432–442, 2019.
https://doi.org/10.1007/978-981-13-2372-0_38

- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack

2 Literature Review

Johari et al. [1] used three keys for encryption and decryption. Three prime numbers served as the keys. Some mathematical operations like addition, subtraction and multiplication were performed on keys to create different cipher texts. They also performed binary operations like shift operations on binary values of the ASCII characters to enhance the security level.

Kamalakannan et al. [2] presents the FPGA implementation of elliptic curve cryptography. The ASCII value of each character of text message mapped to the affine point. By using matrix mapping method these points were mapped again. For encryption and decryption they used ElGamal encryption and decryption techniques. The entire design is implemented on FPGA.

Singh et al. [3] removed the mapping of characters to affine points in elliptic curve. They paired up the ASCII values of plain text. The paired up values were taken as input. Their proposed technique removes mapping overheads and both the parties are not bothered about sharing of common lookup table. Any type of script can be encrypted or decrypted by using their proposed technique.

Paira et al. [4] developed innovative symmetric key cryptography algorithm on the basis of concepts of data structure and binary to gray code conversion techniques. They proposed the folding logic along with the circular shift operation. The proposed algorithm is secured against brute force attack and Man-In-Middle attack.

Iyer et al. [5] created a hybrid operation model using two cipher techniques AES and ECC. A QR code equivalent of the keys is generated in image form which is then used by the system to extract the key in the text form. This provides an extra level of security to the AES key. For the second level of the security, ECC public key was used to encrypt AES key. Later on, the encrypted AES key was used to encrypt the base64 encoded plain text to convert it into a corresponding cipher text. The resulting cipher text is already compressed and has undergone two levels of mixed encryption, ECC and AES. Their proposed idea and methodology provides a much better level of security than single model individually.

Shoukat et al. [6] studied about research issues of cryptographic elements and concluded that requirement of randomness in both the key and data blocking to get higher security. They analyzed that they can achieve higher security by creating random probabilities under the optimal key length. They also analyzed that hybrid encryption scheme can provide more security.

Shrivastava et al. [7] proposed an algorithm that has two rounds and both of these rounds, uses ASCII code of characters. In their proposed work, two operations addition and XOR used for encryption process and other two operations subtraction and addition used for generating two sub keys. Removing the correlation between cipher text and plain text is the objective of their algorithm. No of rounds reduced up to only

two rounds makes the algorithm faster. Since they are encrypting plain text twice with a different key, thus they get a strong cipher which is difficult to break.

Raja et al. [8] developed high security encryption mechanism by performing rotation and flipping operations on matrix. Their method ensures two levels of security, first one is data encryption by generating encrypted array and performing matrix operations and second one is authentication by hash value computation.

Mathur et al. [9] proposed a technique in which Advanced Encryption Standard algorithm was used to encrypt plain text and ECC algorithm was applied to encrypt the AES key. They also used software countermeasures to prevent possible vulnerabilities posed by the timing side channel attack. They tested their system on the basis of some parameters those are: key length, no. of rounds, algorithm, maintenance of keys and attack performed. They also focused on verifying cache timing attack and investing some of the countermeasures by implementing them.

Naik et al. [10] developed the color substitution method that encrypts the text into a single image after converting each character to a color block. The sender must specify the values for RED (R), GREEN (G), and BLUE (B) channels. All the characters of text are then converted to color blocks formed by combining the values of RED (R), GREEN (G) and BLUE (B). The block size and selected channel form the key.

Patel et al. [11] developed a cryptographic technique to secure the information stored in mobile devices through cloud computing, they used a hybrid approach for secure transmisson of data by combining capabilities of ECC and blowfish algorithms. For increasing the computational complexity they used random numbers. They also randomized the number of rounds of blowfish for performance improvement. Generally, subkeys stored in EEPROM on a mobile phone can be easily hacked by attacker so they developed the enhanced blowfish technique for data protection with some modifications.

Prof. Kallam et al. [12] a block cipher technique is developed by them involves color substitution with iterative and modular arithmetic functions. They used large key of 128 bits and further it was divided into four subkeys by using subkey generation algorithm. First two keys are the input of the function selected on the basis of third key out of available functions then the output of the function gives the incremental values for color substitution and last key used for transposition of the cipher. They performed cryptanalysis and found that their technique generates a strong cipher.

Joshi et al. [13] proposed an efficient technique that increases the complexity of decryption performed by attacker by reducing the length of the encrypted message. They reduced the size of the cipher text by half so that the total size of the key and the cipher text is equal to the size of the original message. Their proposed technique is protected against brute force attack because each time a new key is generated for the message.

Bendovschi [14] analyzed the attack reported in last five years and provides a general view on cyber crime from the perspective of specialized literature, international law and historical facts and then she presented some countermeasures for ensuring security and to control the cyber crime around the globe.

Chandra et al. [15] proposed content based algorithm that performs some logical operations on binary values like circular bit shifting operation and binary addition.

Plaintext was encrypted two times to generate the secured cipher text using binary addition operation. Folding method was used for generating the secret key.

Shemin et al. [16] proposed a new method by combining three cryptographic techniques visual cryptography, quantum cryptography and steganography. In their proposed method visual cryptography hides the authentication details of the customer by generating two shares for customer and bank respectively. For ensuring the security of one time password, quantum cryptography was used and for the security of customer's share steganography was used. Their work saves customers through man in middle attack and identity theft issues.

Pozo et al. [17] used a secret key and a series of prime numbers generated through bi-directional matrix. The time taken in encryption and decryption process is very short which optimizes the battery of smart phone. The algorithm runs in quadratic polynomial complexity and because of such mathematical complexities, attacker is unable to intercept the message.

Ahmad et al. [18] proposed technique encrypts product's order and payment information by ECC algorithm and send both the things parallely over the network. At the time of decryption, recipient decrypts the message through private key and encryption algorithm. Their proposed technique overcome the failure of SET. Through their proposed work they assure the secure E-transactions.

Patil et al. [19] analyzed and compared all the popular cryptographic algorithms. The experiment has been done on different files of various sizes. Their experiment shows that time taken by the blowfish is the least among other algorithms and the time taken by the RSA algorithm is the highest, if time and memory are major factors then blowfish is the best suited algorithm, if cryptographic strength is major concern then AES is best suited algorithm and if network bandwidth is major factor then DES is best suited.

Kester et al. [20] proposed image encryption technique for the security of image data in health sector. In health sector safety, privacy and security of medical images is major concern. Unauthorized access to medical data will violate the privacy of patients. They proposed an effective security information system with a fully recoverable and reversible technique for authentication and security of medical images and all the pixel values remain same as it was before.

3 Security Analysis of Existing Proposals

Security analysis of the existing proposals over various cryptanalytic attacks has been done here.

In Johari et al. [1] method, they used three mathematical equations given below in decryption process to get the plain text back.

$$D1 = (N + K3) \bmod 26 \tag{1}$$

$$D2 = (D1 - K2) \bmod 26 \tag{2}$$

$$D = (D2 * K1^{-1}) \bmod 26 \tag{3}$$

where k1, k2 are the first two keys and third key is generated by performing the inverse modulo operation on first key k1. D1 and D2 are set of intermediate values and D is set of final calculated decimal values.

After performing the cryptanalysis, we found that values of N (N is a set of encoded values [0, 1, …, 25] used for alphabets) can be easily determined from cipher text message by performing UNICODE to decimal conversion, right shift operation, binary to ASCII conversion and assigning encoded values to characters.

With some modifications in the mathematical formulas, by putting the guessed values in formulas and with the help of values of set N, the attacker can easily decrypt the whole plain text message.

Modified Mathematical formulas are given below

$$K1 = |D1 - N| \tag{4}$$

$$K2 = |D2 - D1| \tag{5}$$

$$K3 = \text{Inverse modulo } (D2/D) \tag{6}$$

They used "modulo by 26" operation that always generates value between 1 to 26 numbers as shown below

$$(11 + 7) \bmod 26 = 18 \tag{7}$$

$$(18 - 3) \bmod 26 = 23 \tag{8}$$

$$(15 * 21) \bmod 26 = 3 \tag{9}$$

For getting all keys, only 26 * 26 = 676 combinations of numerical values of D1 have to be guessed. By putting these guessed values in the above mentioned formulas, the first key k1 can be easily determined. Cryptanalysis is as shown below (Table 1).

As soon as values of first key in third and fourth columns are equal, that value is the final value of first key. In subsequent cryptanalysis process, the values of keys k2 and k3 can also be determined by using these modified mathematical equations. Once the values of these keys are determined, the values of set D can also be determined easily. This contains ASCII values of characters of the plain text message. By converting these values to their corresponding ASCII characters, we can easily get the plain text message back hence this method is vulnerable to the chosen ciphertext attack and brute force attack.

In Johari et al. [1] method order of letters and words of cipher text message is not changed during the message transmission. No transposition, rotation and reversal operations done on ciphertext. Each letter in the ciphertext has the same position as it had into plain text message which makes this method vulnerable to the different cryptanalysis attacks.

Table 1. Cryptanalysis of triplicative cipher technique

First guessed value	Second guessed value	K1 = |D1 – N|	K1 = |D1 – N|
1	1	10	15
1	2	10	14
.	.	.	.
.	.	.	.
18	18	7	2
18	19	7	3
18	20	7	4
18	21	7	5
18	22	7	6
18	*23*	*7*	*7*
.	.	.	.
.	.	.	.
26	26	15	10

4 Proposed Technique

4.1 Encryption

1. Get the plain text message and store it into an array of characters.
2. Generate three keys k1, k2 and k3 by using the random number generation procedure. The value of each key is a random number under the range of 256.
3. Convert each character value of plain text message to its equivalent UNICODE value and multiply each value with the three symmetric key values and store the resulted big integer values of characters into another array.
4. Reverse the array of big integer values of the characters.
5. Send the values of this array as ciphertext to the receiver side.

4.2 Decryption

1. Get the cipher text and store it into an array of numeric values.
2. Now reverse the array of numeric values.
3. Divide the each value of the array of the numeric values by using the three symmetric key values and convert these UNICODE values into their equivalent character values and store it into an array of characters.
4. The resulting array contains the required message (Fig. 1 and Table 2).

4.3 Simulation of Text Encryption and Decryption

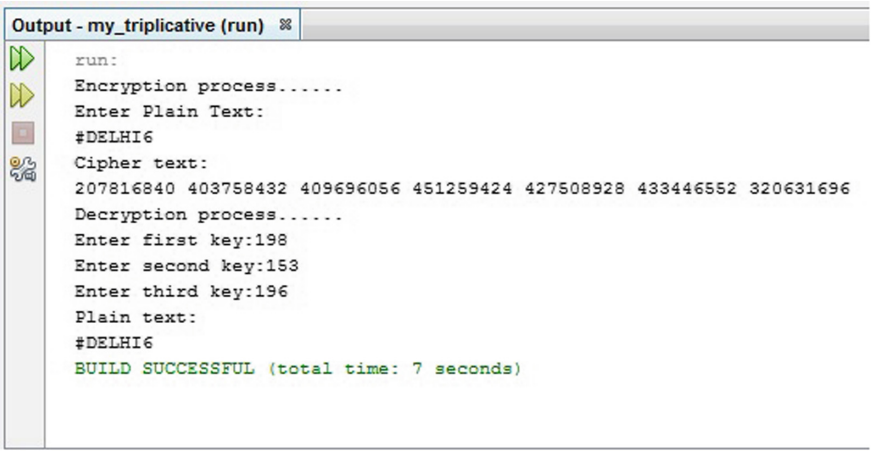

Fig. 1. Output for encryption and decryption of alphanumeric data

Table 2. Simulation environment

Operating system	Windows 7 Ultimate
Processor	Intel Core i3 2310 M
Memory	2 GB
IDE	NetBeans
IDE version	8.1
Language used	JAVA
JAVA version	1.8.0_91

5 Performance Comparison

5.1 Encryption and Decryption Time

Figure 2 shows that Triplicative cipher technique takes more time for encryption than the proposed technique. The use of various mathematical operations like shift operations, modulus operations, arithmetic operations and binary conversions makes triplicative cipher technique slower as compared to proposed technique. Triplicative cipher technique [1] also used encoding of alphabets to their positional value hence this mapping process makes encryption procedure slower (Fig. 3).

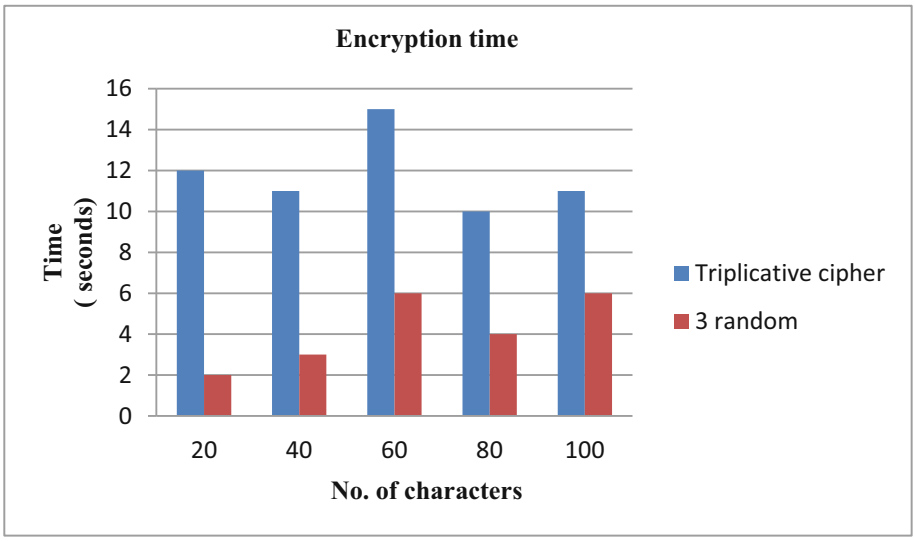

Fig. 2. Encryption time vs no. of characters for triplicative and 3 random (proposed technique)

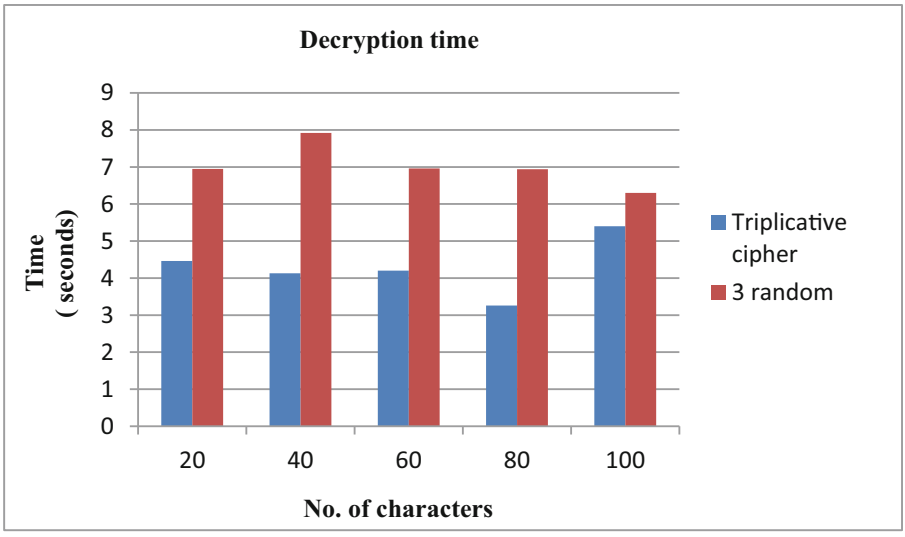

Fig. 3. Decryption time vs no. of characters for triplicative and 3 random (proposed technique)

Figure 4 shows the comparison of total time for both the algorithms, calculated by using the following equation.

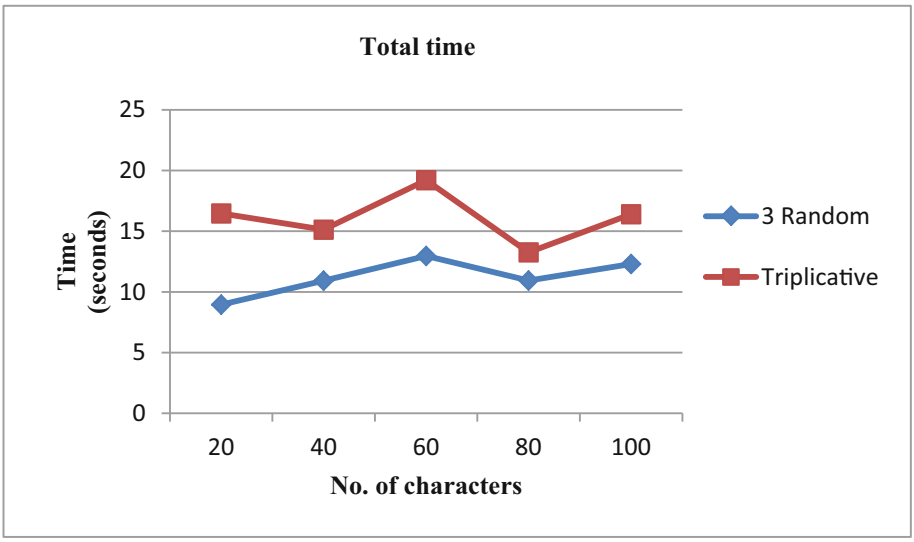

Fig. 4. Total time vs no. of characters for triplicative and 3 random (proposed technique)

$$\text{Total Time} = \text{Encryption time} + \text{Decryption time}$$

The total time taken by proposed technique is less than the triplicative cipher technique which makes proposed technique more efficient than triplicative cipher technique.

5.2 Time Complexity and Cryptanalyis

In the proposed work, combination of three keys used for encryption and decryption of messages. Each can be of any random number from 1 to 256 so the length of these three keys are k1(256), k2(256) and k3(256), hence the total number of key combinations required for symmetric key encryption is

$$256 * 256 * 256 = 16777216$$

The attacker has to guess 16777216 key combinations which is not possible in very short period and if the attacker gets the keys, the sender will have generated new cipher text and changed keys for the same message in that duration so the attacker would not be able to decrypt the cipher text hence the proposed algorithm is stronger than the triplicative cipher technique and secured against ciphertext only attack and brute force attack.

6 Conclusion

In our research work, we have implemented a innovative symmetric key algorithm through randomization where three random keys were used in encryption and decryption process. After evaluating the algorithm based on the some parameters we can say that this algorithm is secured against various cryptanalytic attacks. Total time taken in the encryption and decryption process is very less which makes the algorithm efficient for resource constraint devices.

References

1. Johari, R., Bhatia, H., Singh, S., Chauhan, M.: Triplicative cipher technique. In: International Conference on Information Security and Privacy, pp. 217–223. Elsevier, New Delhi (2015)
2. Kamalakannan, V., Tamilselvan, S.: Security enhancement of text message based on matrix approach using elliptical curve cryptosystem. In: 2nd International Conference on Nanomaterials and Technologies (CNT), pp. 489–496. ELSEVIER (2015)
3. Singh, L., Singh, K.: Implementation of text encryption using elliptic curve cryptography. In: Eleventh International Multi-Conference on Information Processing, pp. 73–82. Elsevier (2015)
4. Paira, S., Chandra, S., Safikul Alam, S., Bhattacharyya, S.: Symmetric key encryption through data structure and binary-gray conversion. In: Shetty, N.R., Prasad, N.H., Nalini, N. (eds.) Emerging Research in Computing, Information, Communication and Applications, pp. 1–10. Springer, New Delhi (2015). https://doi.org/10.1007/978-81-322-2550-8_1
5. Iyer, S., Sedamkar, R.R., Gupta, S.: A novel idea on multimedia encryption using hybrid crypto approach. In: 7th International Conference on Communication, Computing and Virtualization, pp. 293–298. Elsevier (2016)
6. Shoukat, I., Bakar, K., Iftikhar, M.: A survey about the latest trends and research issues of cryptographic elements. Int. J. Comput. Sci. Issues **8**(3), 140 (2011)
7. Shrivastava, M., Jain, S., Singh, P.: Content based symmetric key algorithm. In: International Conference on Computational Modeling and Security, pp. 222–227. Elsevier (2016)
8. Raja, Y., Perumal, S.: WSES: high secured data encryption and authentication using weaving, rotation and flipping. ICTACT J. Commun. Technol. **6**(4), 1200–1207 (2015)
9. Mathur, N., Bansode, R.: AES based text encryption using 12 rounds with dynamic key selection. In: 7th International Conference on Communication, Computing and virtualization, pp. 1036–1043. Elsevier (2016)
10. Naik, M., Tungare, P., Kamble, P., Sabnis, S.: Color cryptography using substitution method. Int. Res. J. Eng. Technol. **3**(3), 941–944 (2016)
11. Patel, P., Patel, R., Patel, N.: Integrated ECC and blowfish for smartphone security. In: International Conference on Information Security & Privacy, pp. 210–216. Elsevier, Nagpur (2015)
12. Kallam, R., Kumar, S., Babu, A.: A modern play color cipher involving dynamic permuted key with iterative and modular arithmetic functions. Int. J. Adv. Res. Comput. Sci. **2**(3), 208–213 (2011)

13. Joshi, A., Wazid, M., Goudar, R.: An efficient cryptographic scheme for text message protection against brute force attack and cryptanalytic attacks. In: International Conference on Intelligent Computing, Communication & Convergence, pp. 360–366 (2015)
14. Bendovschi, A.: Cyber-attacks – trends, patterns and security countermeasures. In: 7th International Conference on Financial Criminology, pp. 24–31. Elsevier (2015)
15. Chandra, S., Mandal, B., Alam, Sk., Bhattacharyya, S.: Content based double encryption algorithm using symmetric key cryptography. In: International Conference on Recent Trends in Computing, pp. 1228–1234. Elsevier (2015)
16. Shemin, P.A., Vipinkumar, K.S.: E–payment system using visual and quantum cryptography. In: International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST), pp. 1623–1628. Elsevier (2016)
17. Pozo, I., Iturralde, M.: A encryption mechanism for instant messaging in mobile devices. In: International Workshop on Mobile Computing Security, pp. 533–538 (2015)
18. Ahmad, K., Shoaib, M.: E-commerce security through elliptic curve cryptography. In: International Conference on Information Security & Privacy (ICISP), pp. 867–873
19. Patil, P., Narayankar, P., Narayan, D.G, Meena, S.M.: A comprehensive evaluation of cryptography algortihms: DES, 3DES, AES, RSA and Blowfish. In: International Conference on Information Security & Privacy. Nagpur: ELSEVIER, pp. 617-624 (2015)
20. kester, Q., Nana, L., Pascu, A., Gire, S., Eghan, J., Quaynor, Nii.N.: A cryptographic technique for security of medical images in health information systems. In: The Second International Symposium on Computer Vision and the Internet (VisionNet): Signal Processing, Images Processing and Pattern Recognition (SIPP), pp. 538–543. Elsevier