Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9, 740-751
2025
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v9i9.9940

The design of safe transmission system by sets of automatically variation key information

Yingjie Huo[1], Haolin Huang[2*], Gulmira Isaeva[3], Wenya Huang[4]
[1,2,3,4]Kyrgyz National University named after Jusup Balasagyn, Kyrgyzstan; Huoyingjie18@gmail.com (Y.H.) Huang601075571@163.com (H.H.) Gulmira.isaeva12@gmail.com (G.I.) hwenya666@gmail.com (W.H.).

Abstract: It's often found in the internet that the cryptosystem can be divided into two parts, symmetric encryption system and asymmetric encryption system. The key which is used in the cryptosystem is a fixed set recently, but there are deficiencies in security. If someone try to crack the code, it is easy to make the key unsafe after a long time that resulting in the secret information leakage. The experiment was carried out using Matlab mathematics software by elliptic curve cryptography, and, tested through ZigBee facilities of the wireless transmission systems. The purpose of this paper is to project that based on the original construct which does not break the cryptosystem. We can increase the safety and do not increase the extra computed complexities. The concept in this paper is that the original used key can change automatically in server, and produces lots of sets at once. The original used key can change automatically in server, and produces lots of sets at once in this paper. Therefore, the cryptosystem can be used for long. When we transmit the information every time, the changing key will increase the difficulties that may be cracked every time. We can increase the safety and do not increase the extra computed complexities. If there is someone trying to crack the code, it is easy to make the key unsafe after a long time, resulting in the secret information leakage. Therefore, the cryptosystem can be used for long, and when we transmit the information every time, the changing key will increase the difficulties that may be cracked every time. The time and security of this cryptographic system were tested on the wireless transmission device Zigbee. The security is 15 times higher than the original mechanism when the time is longer acceptably.

Keywords: *Asymmetric encryption system, Cryptosystem, Key list, Symmetric encryption system.*

1. Introduction

The symmetric key-based cryptography is an efficient method used in Wireless sensor networking (WSN). However, symmetric key-based cryptography model suffers from numerous problems such as low memory, low scalability, and requires key materials. Various techniques were incorporated to overcome the limitations of low energy efficiency in sensor nodes. The clustering technique is well known for WSN limitations. The lifetime of the sensor nodes is increased with optimization algorithm-based routing protocols. The ant colony optimization (ACO) algorithm is applied in solving all types of optimization problems especially in wireless routing protocols. A deep learning approach enhances the performance of WSN to estimate the energy to be produced within a time period. The locations of sensor nodes are changed due to the external and internal factors. The deep learning technique provides accurate localization and optimization. The transmitted data in WSN are secured with

When the nodes are used in "unattended and harsh" environment, the sensor nodes become damaged and defective. The consumption of energy while delivering the packets from the channel to the base station is considered as the main challenge The adequate energy in the node causes the packet to drop while data transmissions. The features and challenges of secure routing and data transmission. The encrypted key and cracked key in symmetric encryption system are the same key. The major problem is

History: Received: 27 June 2025; Revised: 12 August 2025; Accepted: 15 August 2025; Published: 11 September 2025
* Correspondence: Huang601075571@163.com

that how the sender transmits the encrypted key to the receiver in safety after the information was encrypted, and let both share the secret key to decode it. If we use the key list in a trusted internet, maybe we can solve this problem.

The main purpose of this study is to study how to enhance ZigBee's transmission function. In addition to being usable on smaller processors, it is also necessary to consider whether the transmission has better security. This research is to apply the authentication of the elliptic curve cryptosystem to the host connected to the ZigBee device using the AES cryptosystem and key list for encryption and decryption. In the use of authentication, the host uses the characteristics of the elliptic curve cryptosystem to strengthen the security of its original host, which can make the authentication between the hosts more secure. In addition, using the key list to match the AES cryptosystem can save the time and can be more secure than before through the generated key list.

2. Paper Review

The hardware and software engineers responsible for the development of the ellipsometer have access to research and surveys on related topics and useful references [1]. To make the execution of software and hardware cryptographic design unique, a scheme called the C programming platform is proposed to support this process.The conclusion is that the technologies employed in the hardware and software and their performance correspondingly enhance the knowledge of both areas, which is required in the current user concept. Rathee, et al. [2] proposed an "ACO-based Quality of Service (QoS) aware Energy Balance Secure Routing (QEBSR) algorithm" to secure wireless sensor networks (WSNs).

The experimental results confirm that the proposed method is superior to the other two algorithms. And,enhanced heuristics are used to determine the end-to-end latency of data transmission and propose a trust factor for routing paths.

Haseeb, et al. [3] proposed a routing protocol called the "Secure and Energy-Efficient Heuristic Routing (SEHR) Method" to identify and prevent harmonizing data for efficient performance. The framework then protects the network from attacks by adversary groups for high security and low complexity. Network disconnections and link failures are reduced through routing maintenance policies. The proposed protocol incorporates artificial intelligence (AI)-based heuristic models to analyze and implement intelligent and consistent learning frameworks.

The elliptical system was then tested later and evaluated at good standard speeds. The demonstration criteria for the proposed specification have also been completed. A key distribution protocol is proposed to securely provide verifiedbits and anonymous structure keys through ECC-based cryptanalysis capabilities. Because elliptic curve cryptography consumes less energy and power, it is becoming increasingly feasible for resource-constrained remote sensor systems Louw, et al. [4].

Halidoddi and Pandu [5] suggested a "two-level security" for data conversion through wireless sensor networks (WSNs). A bat optimization algorithm based on multi-objective trust (MOTBOA) is introduced to perform secure clustering and routing operations. The effectiveness of the provided method is verified by multiple parameters of the network.An improved homomorphic cryptographic system (EHC) has been created for data security on the network. Finally, the experimental results confirm that the proposed method performs well in system performance.

Veerabadrappa and Lingareddy [6] proposed "Multi-objective Trust-Perception Hybrid Optimization (MOTAHO)" to enable secure data transmission in wireless sensor networks (WSNs). The proposed approach is used to provide security against distributed denial-of-service (DDoS) attacks. Finally, the experimental results show the best performance of the MOTAHO method provided.This optimization is achieved through mixed moth flame optimization (MFO) and flock optimization (CSO), as well as various different types of constraints.

The designed system encountered the basic requirements of the key distribution plan, which needs secure viewing and effective capabilities in wireless sensor networks. The suggestion for future work is to conduct more comprehensive tests to discover all weaknesses and measures that need improvement. Eliminating human administrator intervention to make the system more flexible would also be

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

beneficial. A development effort in advanced image encryption algorithms is underway. This scheme met the minimum requirements considered to be secure and efficient key distribution schemes. Further observations indicated that the framework was indeed stable and could be easily adapted to multiple tasks by adding functions only in the client application. A flexible coding algorithm based on AES, RSA, and elliptic curves has been applied to the encryption of compressed images AsmaChaouch [7].

VenkataRao and Ananth [8] proposed a secure cluster head (CH) selection based on a hybrid optimization algorithm (HOA) to generate routing paths for protecting data transmission. The Shamir Secret Sharing (SSS) method was used to provide mutual authentication among nodes. The effectiveness of "HOA-IoT-WSN" was reviewed in terms of packet loss rate (PLR), packet delivery ratio (PDR), average end-to-end delay (AEED), and network overhead. The optimization was accomplished by combining the Grey Wolf Optimization (GWO) and Moth-Flame Optimization (MFO) algorithms.

Shivakumaraswamy [9] proposed the "Cost-Centric Cuckoo Search Algorithm (CCCSA)" to address energy and security issues in wireless sensor networks. The suggested approach was combined with the "Ad hoc On-Demand Distance Vector (AODV)" routing protocol. Adaptive routing paths were generated using AODV. Experimental results confirmed that the proposed method achieved advanced security for the network.The "K-Means Clustering Algorithm (KMC)" was employed to perform the clustering function. The provided method was used to select adaptive cluster heads (CH) among the ordinary nodes in the clusters.

Halidoddi and Pandu [10] proposed using the "grasshopper optimization algorithm (GOA) and elliptic curve cryptography and Diffie-Hellman (ECCDH) key exchange algorithm" for node selection and secure path generation. The effectiveness of this method has been validated and compared with the benchmark "Security and Energy-Aware Heuristic Routing (SEHR) method and the Security Routing Protocol Based on Multi-Objective Ant Colony Algorithm (SRPMA)." The primary objective of this method is to select the most energy-efficient accurate path and enhance the system lifetime of wireless sensor networks (WSN).

Ganesh and Amutha [11] have proposed a method for efficient and secured routing for WSN with "Signal-to-Noise Ratio (SNR)-Based Dynamic Clustering (SDC) model". In the inter clustering routing, the error recovery was adopted to avoid the end-to-end error recovery. The security of the network was accomplished by separating the malicious nodes with sink-based routing method.

Finally, a reasonable correlation is provided between the three most well-known encoding algorithms: AES, RSA, and elliptic curves. Based on our table results analysis, the ECC algorithm is the most secure and reliable. Compared to the RSA and AES encryption algorithms, the ECC algorithm is considered to have the highest level of security.These three popular encryption algorithms were evaluated in terms of encoding speed, security and security level, size of encrypted JPEG or PNG images, key generation, throughput, and time. The key generation time for each encryption algorithm is used to calculate the pixels of the image at the source end.

In this article, elliptic curve cryptography (ECC) has a long history and has been studied by mathematicians for hundreds of years. It is an open key encryption method.

3. Materials and Methods

3.1. Symmetric Encryption System

We can do every kind of replacement to plaintext through the encryption algorithm. And, the input to encryption algorithm is the secret key. The key is unrelated data to plaintext, we use the key not only to encrypt the plaintext but also to crack the cipher text. That is, we use the same secret key to encrypt or crack the text in symmetric encryption system, so the transceiver must own the same key. Therefore, how transmit the key to receiver validly and guard the information against hikers is an important problem [12-15].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

3.2. Asymmetric Encryption System

Everyone has public key and private key in asymmetric encryption system. The private key must be kept by individual carefully. Under the asymmetric encryption system, every participator can get everyone's public key and own his own private key, so the private key doesn't be transmitted in the net. If the public key encrypted one message, then it must be cracked by the private key, and vice versa.

3.3. key list

Key list is a simple idea; it produces over a set of key based on the original key set and list them. It is why at first we have to transmit every key for every use, but if we apply key list to transmitting, we can use them for so long. But before generating key list, we must pass the random number test.

3.4. Random Number Test

3.4.1. FIPS PUB 140-1 Random Number Test

FIPS PUB 140-1 is security requirements for cryptographic modules to Federal Information Processing Standards Publication. The test including cryptographic modules random number is as follow:

3.4.1.1. Monobit Test

Random number generator generated 20,000 continuous bits (0 or 1). We define X to the sum of 20,000continuous bits, if 9654<X<10346, then this random number test was passed.

3.4.1.2. Poker Test

Random number generator generated 20,000 continuous bits. These 20,000continuous bits were cut for 5,000 continuous four bits integer. The range of the integral number is between 0 ~ 15. Define f(i) as the appearing times of the integral number, and the range of i between 0≦i≦15, here is the computation:

$$X = \frac{16}{5000}\left(\sum_{i=0}^{15} f(i)^2\right) - 5000$$

If 1.03 < X < 57.4, then this test was passed.

3.4.1.3. Runs Test

Runs test is the length of 1 continuum or 0 continuum in 20,000 continuous random bits, and add up the data. No matter how the bit is 1 or 0, if the length of runs data fit the Table 3-1 that the range of added numbers and there are 12 tests. If one is not allowed, then the random number test is not passed.

Table 1.
Bit Repeat Value Cumulatives.

Bit repeat value	Cumulative number
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
>=6	90-223

3.4.1.4. Long Run Test

Long run test is a length of 34 or above of 1 continuum or 0 continuum in the 20,000 continuous random number bits. Added the long run data, it has 2 tests, including 1 or 0 test. If one of these two data is not 0, then the random number test is not passed. There are total 16 tests of random number of FIPS PUB 140-1. 16 represents that all tests are passed; 0 represents that all are not allowed; 3 represents that there are 3 tests passed, and so on [16].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

3.5. System Construct

Procedure I (Figure 1): First, through the random number tests, the server generated a set of key lists.

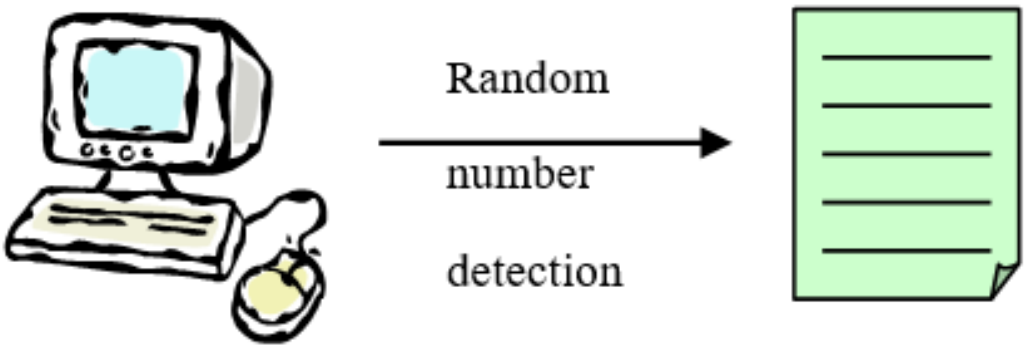


Figure 1.
Through the random number tests, the server generated a set of key lists.

Procedure II (Figure 2): Send the key list and the chosen calculational methods to the other side.

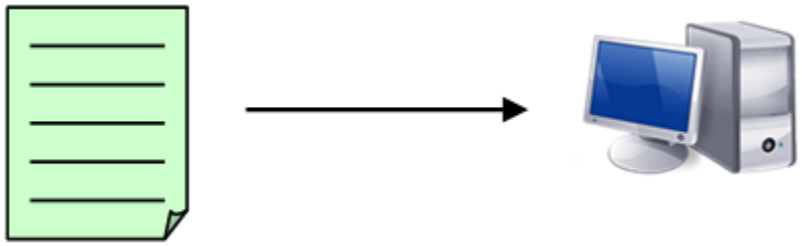


Figure 2.
Send the key list and the chosen calculation methods to the other side.

Procedure III (Figure 3): Encrypted the information by the key list, and sent the cipher text to the other side.

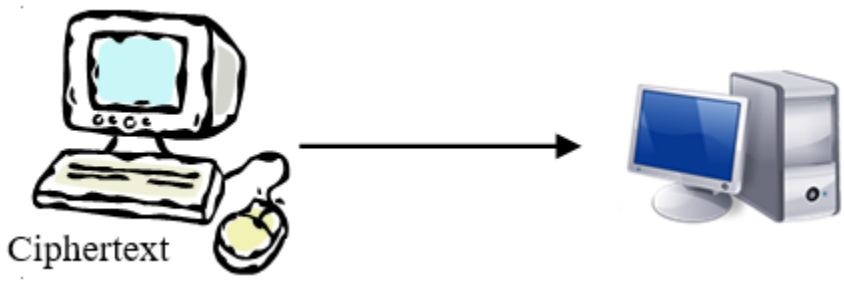


Figure 3.
Encrypted the information by key list, and sent the cipher text to the other side.

Procedure IV (Figure 4): The other side cracked the cipher text which became the plaintext later by key list.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

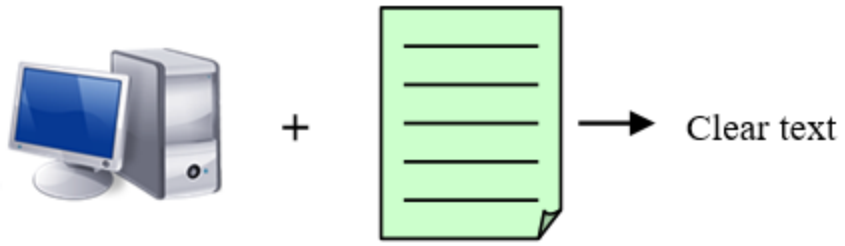


Figure 4.
The other side cracked cipher text which became the plaintext later by key list.

Procedure V (Figure 5): The key list changes the other new key list through the calculational method, raising the calcultaional complexities.

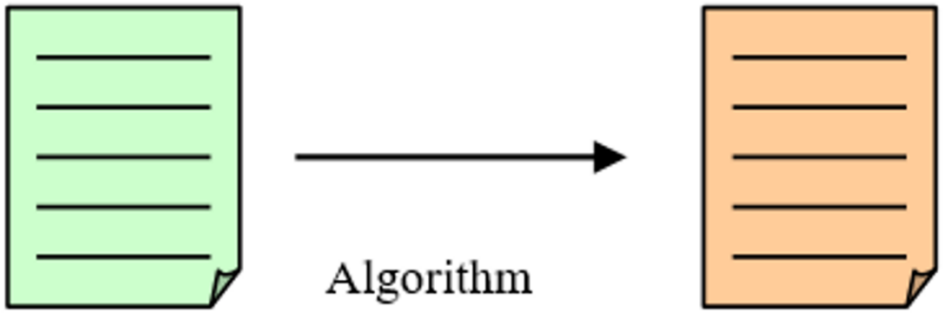


Figure 5.
The key list changes the other new key list through the calculation method, raising the calculation complexities.

3.6. Research Method

The difference between symmetric encryption system and asymmetric encryption system is the sending of key and public key. We can send the information to the other side base on trust in symmetric encryption system; while, in asymmetric encryption system, we must send the information to the other side via the third person.

The third person who we trust most is CA, which is often to appear in the net in asymmetric encryption system. Therefore it would be a long-time development via CA transmitting the key, and no one would doubt its procedure.

Why using key list in symmetric encryption system is that after transmitting, key list would be used for a long time. However, we cannot use CA to transmit a set or change the list in asymmetric encryption system [15-17]. So, in this paper, we consider the use of symmetric encryption system and key list without asymmetric encryption system. It is always a major problem that the management and sending of key in cryptosystem, so I provide two possible methods to solve this problem.

3.6.1. Method I:

Encrypt the key list and transmit. This method is encrypting and cracking the cryptosystem twice. The advantage is because we have encrypted the text, when the third one thieved the ciphertext, he must crack to get the wanted information. But the disadvantage is that when computing, we must use the cryptosystem twice. The computed complexities arise their level, so we are not sure whether it could be used to PDA or other smaller computed processing unit.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

3.6.2. Method Ii

Change the calculational method of key list, and differ from the original key list. We use key list to encrypt and crack directly. We suppose, under the same situation, there are two sides with the same condition, the same calculational method, the same encrypted and cracked method, and same key list. If the calculational method is that the input value adds 1, here is the situation. As shown in Table 2, the change of the key could make the thieved key list invalid. But how we choose the calculation method is also a research direction.

Table 2.
Key list with algorithm changes examples.

No.	Key	Algorithm	No.	Key
01	0001		01	0002
02	0002		02	0003
03	0003		03	0004
04	0004		04	0005
05	0005		05	0006
06	0006		06	0007
07	0007		07	0008
08	0008		08	0009
09	0009		09	0010
10	0010		10	0011

4. Result

The experiment was carried out using Matlab mathematics software. The following is the result of random number detection using Matlab software.

Result 1: A single bit is used as a comparative experiment

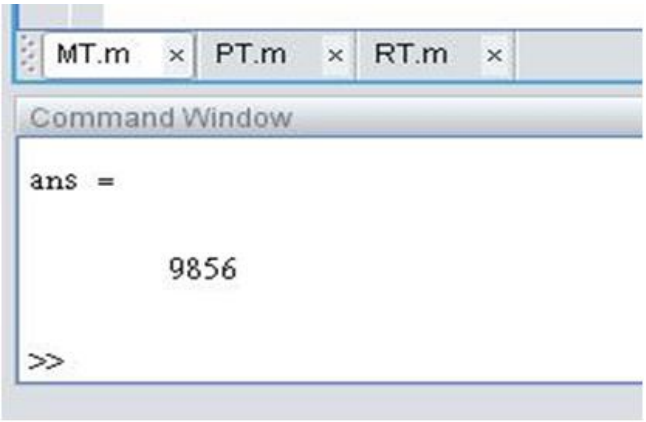


Figure 6.
Matlab for random number detection - taking a single bit as an example.

The result is 9856, passing the conditions of $9654 < X < 10346$.

Result 2: Using the Parker test as a comparative experiment

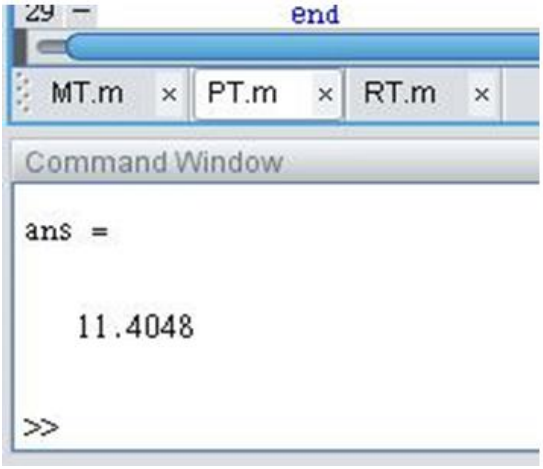
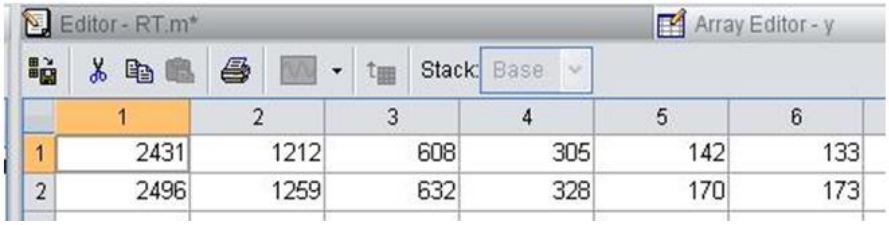


Figure 7.
Matlab for random number detection - taking the Parker test as an example.

The result is 11.4048, passing the condition of $1.03 < X < 57.4$.
Result 3: Using bit repeats as a comparison experiment



	1	2	3	4	5	6
1	2431	1212	608	305	142	133
2	2496	1259	632	328	170	173

Figure 8.
Matlab for random number detection - taking bit repetition as an example.

The data indicates that the first column is a 1-bit repeat value, the first behavior is repeated 1 time, the second behavior is repeated 2 times, the third row is repeated 3 times, the fourth row is repeated 4 times, and the fifth line is repeated. The value is 5 times, the sixth line repeats the value more than 6 times; and the second column is the 0-bit bit repeat value and the first column; the results meet the conditions of Table 1. Into the process of encryption and decryption, this article takes AES as an example.
First, the plain text is selected as "YDU", as shown in Figure 9.

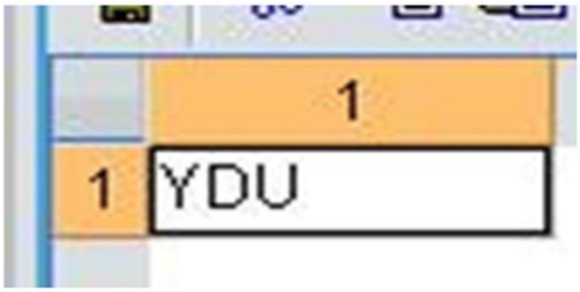
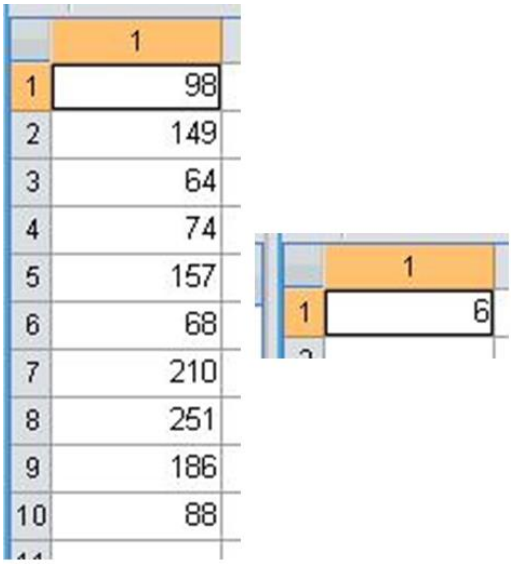


Figure 9.
Matlab for AES encryption - plain text selection.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

Then generate a list of keys, this article randomly selects 10 random numbers from 0 to 255 to form a list of keys, and randomly selects one of the 10 random numbers as the encryption key, as shown in Figure 10.



	1
1	98
2	149
3	64
4	74
5	157
6	68
7	210
8	251
9	186
10	88

	1
1	6

Figure 10.
Matlab for AES encryption - key list.

The plaintext "YDU" is encrypted to obtain the ciphertext, as shown in Figure 11.

	1	2	3	4	5	6	7	8
1	200	160	190	114	78	231	68	80

9	10	11	12	13	14	15	16
79	44	249	12	92	175	182	98

17	18	19	20	21	22	23	24
240	14	36	179	68	206	204	186

25	26	27	28	29	30	31	32
169	85	239	77	1	144	188	99

Figure 11.
Matlab for AES encryption - ciphertext acquisition.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

The ciphertext and key list are transmitted, and the decryption operation is performed to obtain the plain text "YDU", as shown in FIG.

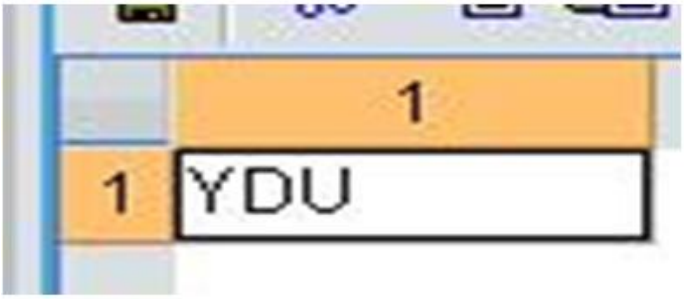


Figure 12.
Matlab for AES decryption - clear text acquisition.

Perform the action of changing the key list, and assign the original key list to the algorithm to obtain a new key list, as shown in Figure 12.

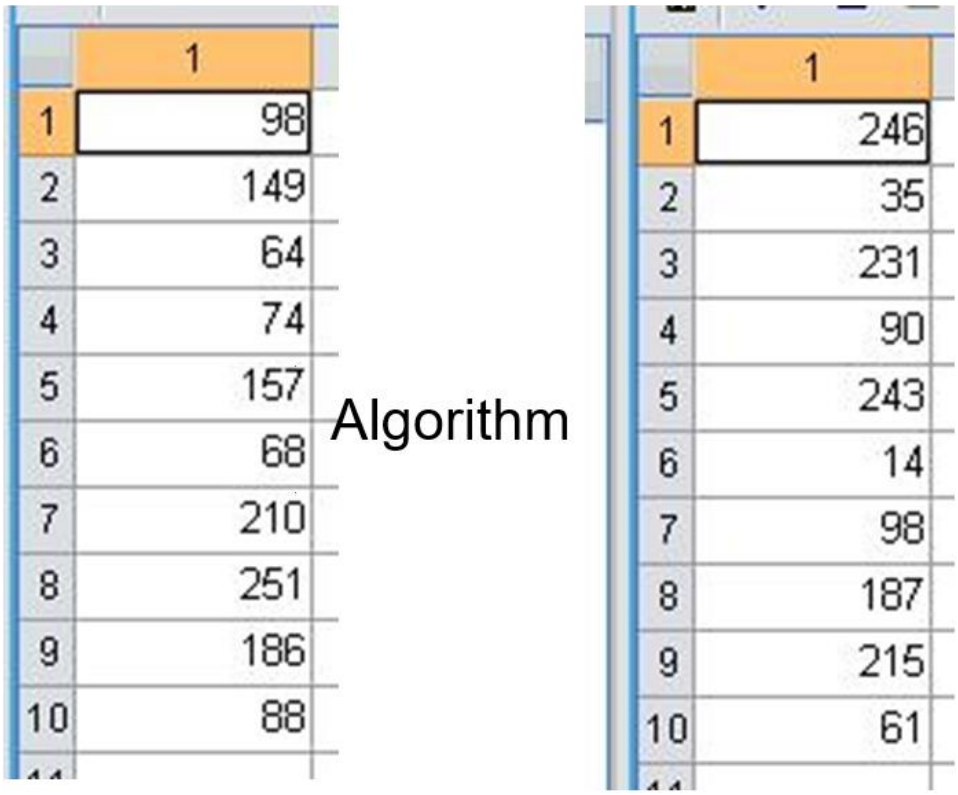


Figure 13.
Matlab key list changes - new key list acquisition.

Since the new password system is used in a different way than the original one, it is necessary to consider the ciphertext during decryption. In addition to considering whether it will be damaged or destroyed by the ciphertext, the time and safety also be focused through the decryption and transmission processes.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940

In addition to the time that the key list to be generated by the host is more likely to take time, the transmission and verification time is increased from the original time of 0.3115 (seconds) to 0.9739 (seconds). The security is more 15 times higher can be verified by experiment in this study.

5. Conclusion

The topic of this paper is that use the key list to correspond with symmetric system, and we can use the one-time key more times.With the key list to correspond with symmetric system, we can use the one-time key more times. We need transmit the key list once, but under what kind of situation that we can transmit is a problem. Because the key list could save time that one-time key transmitted, it not only saves the original time but also keeps the original construct of symmetric encryption system.

Key list corresponding to calculational method could let the life of key list prolong. We just need to update the calculational methods and the key list along with the updated calculational method also update. Recently, the internet and wireless cable grows rapidly, we immerse ourselves in cables, data and so on. Therefore, the main goal that we keep the text that can be circulated in the safely, integral, secret, usable, undeniable, and controllable can be reached by the suggested way in this paper.

The time and security of this cryptographic system were tested on the wireless transmission device Zigbee. The security is 15 times higher than the original mechanism when the time is longer acceptably.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] D. Hankerson, S. Vanstone, and A. J. Menezes, *Guide to elliptic curve cryptography*. New York: Springer-Verlag, 2004. https://doi.org/10.1007/b97644

[2] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 170-182, 2019. https://doi.org/10.1109/TEM.2019.2953889

[3] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network," *IEEE Access*, vol. 8, pp. 163962-163974, 2020.

[4] J. Louw, G. Niezen, T. Ramotsoela, and A. M. Abu-Mahfouz, "A key distribution scheme using elliptic curve cryptography in wireless sensor networks," presented at the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), 2016.

[5] G. Halidoddi and R. Pandu, "Secured data transmission using multi-objective trust based bat optimization algorithm and enhanced homomorphic cryptosystem for WSN," *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 1, pp. 214-224, 2022. https://doi.org/10.22266/ijies2022.0228.20

[6] K. Veerabadrappa and S. C. Lingareddy, "Secure routing using multi-objective trust aware hybrid optimization for wireless sensor networks," *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 1, pp. 540-548, 2022. https://doi.org/10.22266/ijies2022.0228.49

[7] AsmaChaouch, "Belgacem bouallegue and ounibouraoui software application for simulation-based AES," presented at the RSA and Elliptic-Curve Algorithms 2nd International Conference on Advanced Technologies for Signal and Image Processing, 2016.

[8] S. VenkataRao and V. Ananth, "A hybrid optimization algorithm and shamir secret sharing based secure data transmission for IoT based WSN," *International Journal of Intelligent Engineering & Systems*, vol. 14, no. 6, pp. 498-506, 2021.

[9] S. M. Shivakumaraswamy, "Security and energy aware adaptive routing using cost centric cuckoo search algorithm," *International Journal of Intelligent Engineering & Systems*, vol. 14, no. 6, pp. 596-604, 2021.

[10] G. Halidoddi and R. Pandu, "A GOA based secure routing algorithm for improving packet delivery and energy efficiency in wireless sensor

networks," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 6, pp. 311-320, 2021.
[11] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms," *Journal of Communications and Networks*, vol. 15, no. 4, pp. 422-429, 2013.
[12] Y. Shen, *Modern cryptography overture [Lecture notes]. Department of mathematics.* Taitung, Taiwan: Donghai University, 1993.
[13] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory IT*, vol. 22, no. 2, pp. 644–654, 1976.
[14] W. Diffie and M. E. Hellman, "Privacy and authentication: An introduction to cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp. 644– 654, 1996.
[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.
[16] Y. Chen and B. Lin, "Chaotic stream ciphers using logistic map," in *Proceedings of the National Computer Symposium (NCS). Institute of Physics, National Taiwan University, Taipei, Taiwan*, 2001.
[17] M. Abdalla, Y. Shavitt, and A. Wool, "Key management for restricted multicast using broadcast encryption," *IEEE/ACM Transactions on Networking*, vol. 8, no. 4, pp. 443-454, 2000.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 9: 740-751, 2025
DOI: 10.55214/2576-8484.v9i9.9940