ESTABLISHING A MATHEMATICAL MODEL FOR ENCRYPTION AND DECRYPTION OF COMMUNICATION NETWORK DATA

Na Yang
Department of Basic Education, Shangqiu Institute of Technology,
Shangqiu, Henan 476000, China
E-mail: 1350013027@sqgxy.edu.cn

Abstract - Data in communication networks need to be secured during transmission. This paper improved the mathematical model of advanced encryption standard (AES)-based encryption and decryption based on chaos theory. The key of AES was obtained using Logistic mapping and Chebyshev mapping. Random words were added to further improve the randomness of the key. The improved mathematical model was established and tested for its security. It was found that the key obtained from chaotic sequences fully passed the NIST test. Compared with $x_0 = 0.1$, the results of encryption and decryption obtained when $x_0 = 0.1 + 10^{-15}$were completely different, which proved the sensitivity of the key and the stronger randomness of the ciphertext obtained after encryption. Compared with AES, the improved mathematical model spent only 1/3 time in encryption and decryption, showing a higher efficiency. The results demonstrate the reliability of the improved mathematical model for data encryption and decryption in communication networks. This mathematical model can be applied in practical communication networks.

Keywords: Communication network, Data transmission, Mathematical model, Encryption, Chaos.

1. Introduction

With the development of technology, more and more data are transmitted through communication networks [1], and they are generally transmitted publicly. Therefore, under malicious attacks, the data in the network can be easily stolen or tampered with, which seriously threatens the security of communication [2] and may lead to the leakage of personal privacy, the theft of commercial secrets, etc., and the impact is immeasurable. In order to improve the security of communication network data in the transmission process, it is necessary to encrypt the data [3]. The mathematical model of encryption and decryption can use some algorithms to modify the original data, making it difficult for attackers to crack, thus achieving the security of data transmission. At present, the encryption and decryption mathematical models commonly used in the world include advanced encryption standard (AES), data encryption standard (DES), and so on [4].

The research on encryption and decryption techniques is becoming an increasingly important issue. Rahmani [5] designed an asymmetric encryption amplification that combined Arnold cat mapping, hyperbolic function, and Chebyshev mapping to encrypt audio and data. The designed method was found to have good efficiency through experiments. Laia et al. [6] combined the DES algorithm with a random number generator Blum-Blum-Shub (BBS) to increase the security of the key. Since the random number of the key generated by the BBS algorithm was unique, it did not influence on the encryption and decryption time. Golovko et al. [7] used the XOR algorithm for data encryption. This algorithm overlayed the encrypted text with a sequence of random numbers to achieve encryption and decryption. They created EDcrypt software and applied it to travel company information protection. Arroyo et al. [8] obtained the cipher text by the Polybius cipher, then compressed the cipher text by the Hoffman coding algorithm, and embedded it into an image by steganography. They found through experiments that the method had better performance in file size, similarity, etc. This paper established a mathematical model of encryption and decryption for communication network data. Based on chaos theory, the model obtained the AES key by two chaos mappings. The security of the model was verified by experimental analysis. This model can be applied in practical communication networks. This work provides theoretical support for securing data transmission.

2. Mathematical Model of Encryption and Decryption Combined with Chaos

2.1 Chaos Theory

In the process of data transmission, it is necessary to ensure transmission integrity,

confidentiality, etc. Encrypting the original data can hide the real information and thus ensure the security of the data [9]. As cryptography is constantly studied, the mathematical model of encryption and decryption has also been explored more and more deeply, and more and more new techniques have been applied in cryptography, such as chaos theory [10].

Chaos has a wide range of applications in meteorology and physics [11], and it has qualities such as pseudo-randomness and unpredictability, which have many commonalities with the requirements of cryptography. Hence, chaos cryptography emerged. At present, there is no complete definition of chaos, and the following two definitions are widely agreed upon.

(1) Li-Yorke definition [12]: it is assumed that there exists continuous mapping $f(x)$ in $[a, b]$. A system is chaotic if the following conditions are satisfied.

① The periodic point of f has no upper bound.

② In closed interval I, there exists uncountable subset S that satisfies the followings. For any $x, y \in S$, $x \neq y$, there is $\lim_{n\to\infty} sup|f^n(x) - f^n(y)| > 0$; for any $x, y \in S$, there is $\lim_{n\to\infty} inf|f^n(x) - f^n(y)| > 0$; for any $x, y \in S$ and y is any periodic point of f, there is $\lim_{n\to\infty} sup|f^n(x) - f^n(y)| > 0$.

(2) Devaney definition [13]: it is assumed that there exists a continuous mapping in metric space V: $f: V \to V$. A system is chaotic if the following conditions are satisfied.

① Initial value sensitivity: there exists $\delta > 0$, for any $\varepsilon > 0$ and $x \in V$, there exist y and natural number n in the ε neighbourhood of x that make $d(f^n(x), f^n(y)) > \delta$.

② Topological transfer: for any open sets $Z, Y \in V$ in V, there exists $m > 0$ that makes $f^m(Z) \cap Y \neq \emptyset$.

③ The periodic points of f are dense in V.

2.2 Advanced Encryption Standard Algorithm

In cryptography, the mathematical models of encryption and decryption are mainly divided into symmetric and asymmetric [14], among which, AES is the most widely used one in symmetric cryptography [15]. The number of encryption rounds of AES is different according to different key lengths, as shown in Table 1.

Table 1. Number of encryption rounds under different key lengths

	Key length (32-bit words)	Number of encryption rounds
AES-128	4	10
AES-192	6	12
AES-256	8	14

The AES encryption and decryption process consists of four main elements.

(1) Byte replacement: One byte is converted to another by looking up the S-box.

(2) Row shifting: The state matrix is left cyclically shifted by different offsets.

$$\begin{pmatrix} A_{00} & A_{01} & A_{02} & A_{03} \\ A_{10} & A_{11} & A_{12} & A_{13} \\ A_{20} & A_{21} & A_{22} & A_{23} \\ A_{30} & A_{31} & A_{32} & A_{33} \end{pmatrix} \xrightarrow{ShiftRows} \begin{pmatrix} A_{00} & A_{00} & A_{00} & A_{00} \\ A_{11} & A_{12} & A_{13} & A_{14} \\ A_{22} & A_{23} & A_{20} & A_{21} \\ A_{33} & A_{30} & A_{31} & A_{32} \end{pmatrix} \tag{1}$$

(3) Column mixing: The result of row shifting is multiplied by the fixed matrix to get the confused matrix:

$$\begin{pmatrix} A_{00} & A_{01} & A_{02} & A_{03} \\ A_{10} & A_{11} & A_{12} & A_{13} \\ A_{20} & A_{21} & A_{22} & A_{23} \\ A_{30} & A_{31} & A_{32} & A_{33} \end{pmatrix} \xrightarrow{MixColumns} \begin{pmatrix} A'_{00} & A'_{01} & A'_{02} & A'_{03} \\ A'_{10} & A'_{11} & A'_{12} & A'_{13} \\ A'_{20} & A'_{21} & A'_{22} & A'_{23} \\ A'_{30} & A'_{31} & A'_{32} & A'_{33} \end{pmatrix} \tag{2}$$

(4) Add round keys: Bit-by-bit Xor operation is performed on round key K and the matrix obtained after column mixing.

$$\begin{pmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{pmatrix} \xrightarrow{AddRoundKey} \begin{pmatrix} b_{00}\oplus k_{00} & b_{01}\oplus k_{01} & b_{02}\oplus k_{02} & b_{03}\oplus k_{03} \\ b_{10}\oplus k_{10} & b_{11}\oplus k_{11} & b_{12}\oplus k_{12} & b_{13}\oplus k_{13} \\ b_{20}\oplus k_{20} & b_{21}\oplus k_{21} & b_{22}\oplus k_{22} & b_{23}\oplus k_{23} \\ b_{30}\oplus k_{30} & b_{31}\oplus k_{31} & b_{32}\oplus k_{32} & b_{33}\oplus k_{33} \end{pmatrix} \tag{3}$$

Taking AES-128 as an example, its encryption round number is 10, and the initial key is 128 bits. Taking 32 bits as a word, the 128-bit key is divided into four words, denoted as $w[0]$, $w[1]$,$w[2]$, and

$w[3]$. Then, the four words are expanded to 40 new words, denoted as $w[4]$,$w[5]$, ……$w[43]$.

The expansion formula is: ① When $0 \le i \le 3$:

$$w[i] = (key[4i], key[4i+1], key[4i+2], key[4i+3])$$

② when $4 \le i \le 43$ and $i = 0 mod 4$:

$w[i] = w[i-4] \oplus w[i-1]$; ③ when $4 \le i \le 43$ and $i \ne 0 mod 4$,

$$w[i] = w[i-4] \oplus (SubWord(RotWord(w[i-1])) \oplus Rcon[i/4])$$

In the equation, $SubWord$ refers to byte substitution. After dividing the 21-bit independent variable by four equal parts, the S-box substitution is performed. $RotWord$ refers to byte shift. Finally, xor is performed on the substituted byte and $Rcon[i]$. After ten rounds of the above transformation, the encryption operation is completed, and decryption is the inverse process of encryption.

2.3 The Improved Mathematical Model for Encryption and Decryption Combined with Chaos

The security of AES is related to the key. According to AES, if an attacker gets a round key, it is possible to get the next round key by the extension of AES.

To further improve the security of AES, this paper combines chaos theory to improve AES. Two chaos mappings are used to generate ideal random sequences. Bitwise Xor is performed on the sequence to obtain the chaotic key stream as the initial key of AES. The improved mathematical model uses two two-dimensional chaotic mappings, and the key stream is generated as shown in Figure 1.

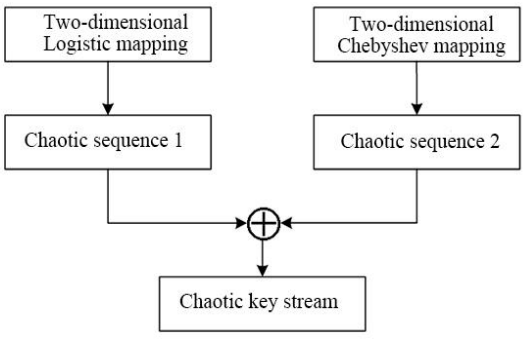

Figure 1: Chaotic key stream generation process

The equation for the two-dimensional Logistic mapping is:

$$\begin{cases} x_{n+1} = \mu\lambda_1 \times x_n \times (1 - x_n) + \gamma \times y_n \\ y_{n+1} = \mu\lambda_2 \times y_n \times (1 - y_n) + \gamma \times x_n \end{cases}, \quad (4)$$

where λ_1, λ_2, μ, and γ are control parameters. $\mu = 4$ usually, and when $(x_0, y_0) = (0.1, 0.11)$, $\gamma = 0.1$, and $\lambda_1 = \lambda_2 = 0.89$, the system is in a chaotic state.

The equation for the two-dimensional Chebyshev mapping is:

$$\begin{cases} x_{n+1} = \cos(m \arccos x_n) \\ y_{n+1} = \cos(n \arccos y_n) \end{cases}, \quad (5)$$

where m and n are the control parameters. When $n \ge 2$, the system is in a chaotic state.

In addition to the chaotic sequence, random word G is added to perform xor with the last round key to get the current round key. The encryption process of the improved mathematical model is as follows. ① The plaintext is divided into blocks in a size of 16 bytes (128 bits); ② 1000 iterations are performed to get the composite chaotic sequence; ③ the round keys of the first round are generated: $w[4] = G[1] \oplus w[0]$, $w[5] = G[1] \oplus w[1]$, $w[6] = G[1] \oplus w[2]$, and $w[7] = G[1] \oplus w[3]$; ④ the round key of the i-th round is generated according to the following equation:

$$w[i] = \begin{cases} w[4i] = G[i] \oplus w[4i-4] \\ w[4i+1] = G[i] \oplus w[4i-3] \\ w[4i+2] = G[i] \oplus w[4i-2] \\ w[4i+3] = G[i] \oplus w[4i-1] \end{cases}. \quad (6)$$

All plaintext blocks are encrypted and then stitched in order to get the ciphertext. Decryption is the inverse operation of encryption.

3. Results and Analysis

The test was carried out in MATLAB 2010 environment. $(x_0, y_0) = (0.1, 0.11)$, and the improved mathematical model was used for encryption and decryption. First, the randomness of the key in the improved mathematical model was tested using the NIST test.

The test results of the Logistic sequence, Chebyshev sequence, and hybrid sequence were compared, as shown in Table 2.

Table 2. Whether the sequence passes the NIST test

test	Logistic sequence	Chebyshev sequence	The hybrid sequence
Frequency test	YES	YES	YES
Grouping frequency test	YES	YES	YES
Runs test	YES	YES	YES
Approximate entropy test	YES	YES	YES
Accumulated sum test	YES	YES	YES
Longest runs test within a block	YES	YES	YES
Binary matrix rank test	YES	YES	YES
Spectrum test	YES	YES	YES
Non-overlapping pattern matching test	YES	NO	YES
Overlap pattern matching test	YES	YES	YES
Global general statistics test	NO	YES	YES
Linear complexity test	YES	NO	YES
Random deviation test	NO	YES	YES
Random variable deviation test	NO	YES	YES
Serial test	YES	NO	YES

It was seen from Table 2 that both the Logistic sequence and the Chebyshev sequence failed the NIST test completely, while the hybrid sequence passed the NIST test, indicating that the hybrid sequence had better randomness and a more secure key.

Then, the sensitivity of the key was analyzed. With other parameters unchanged, the same text in the communication network was encrypted and decrypted in the case of $x_0 = 0.1$ or $x_0 = 0.1 + 10^{-15}$. The results are as follows.

Original plaintext: The overall strength of the first two cold air is weak, but the third strong cold air will bring significant cooling and may drop the temperature below 0 ℃, but the dry cold air dominates, less rainfall, mostly cloudy weather.

Encryption of plaintext with $\boldsymbol{x_0 = 0.1}$: U樓A?b?0検?均???蒲V绌]]?窺?脫{?炌Z巛?掙~VC熵?ph/禑魁?0,$~.⍰炆锽\廣bㄨ???埱誫?_鍰欣WY[攔&3wS訃_糵ま?葤?睹?钗d燚w骔阚q_x001D__x0016_+罄d$2s筳@S窗Z戞'勿dL蒠?靐{\骿晧_x0016_)?擅穗sa痜?E俚偐?闪??ぷ`4b

Decryption of ciphertext with $\boldsymbol{x_0 = 0.1}$: The overall strength of the first two cold air is weak, but the third strong cold air will bring significant cooling may drop the temperature below 0 ℃, but the dry cold air dominates, less rainfall, mostly cloudy weather.

Encryption of plaintext with $\boldsymbol{x_0 = 0.1 + 10^{-15}}$: ⍰汆诠WNaCt褥昭w]⍰_x001D_峪鮫z+ 2 銖i槵⍰瘋N淩虢`e/I?6>釷鑚廬3矝⍰謏K諮僞蕔BN"鎶莿W?a鍦_x0016_CZ⍰}宠?u皡1潛J慭珑揂诪6?6惃FEン暗艘73?汩A堆爈9T

Decryption of ciphertext with $\boldsymbol{x_0 = 0.1 + 10^{-15}}$: 澌K?＃Ч?;齜傁莔z?䞓婯l?肱豯臢]??禑种荽J}▼楚掕?罪?+yS?ｅDT?⍰K姚?,⍰儗萸隟槃N籠v⍰⍰鐔1鱵斋溹鳰?珲|\2獮X⍰Rh?~-雉灉x5⍰⍰E训鴖?c?v洺W66`2郹La'lK斓

It was found from the above results that there was no information related to the original plaintext in the ciphertext obtained after encryption by the improved mathematical model. Moreover, the chaotic key generation process was complicated, and the attacker could not know all the keys to crack the ciphertext. In addition, when there was an extremely small change in the key, the ciphertext obtained after encryption was completely different, and no information related to the plaintext was obtained after decryption. These findings verified the security of the improved mathematical model.

The improved mathematical model was used to encrypt a string of plaintext containing 2034 bytes in the communication network. The statistical characteristics of the text data before and after encryption were compared: ① variance: $\sigma^2 = \frac{\sum(x-\beta)^2}{N}$; ② extreme difference: $R = x_{max} - x_{min}$. In the equations, x refers to the ASCII value of the text characters, β is the average of the ASCII value of the characters, and N is the number of characters. The results are shown in Table 3.

Table 3. Comparison of statistical features of text data

	Variance	Extreme difference
Plaintext	936.256	326
Ciphertext	8.364	12

It was seen from Table 3 that the plaintext had some statistical properties; after encryption, the frequency difference of the distribution between the ciphertexts was very small, i.e., there was great randomness and no statistical property, which proved the security of the ciphertexts.

Finally, the encryption and decryption efficiency of the improved mathematical model was compared with the original AES for the same segment of text data, and every model was run three times. The results are shown in Figure 2.

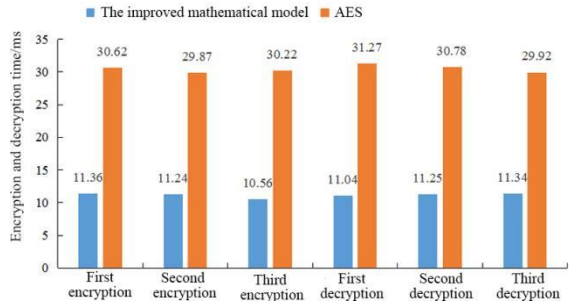

Figure 2: Comparison of encryption and decryption efficiency

It was seen from Figure 2 that the improved mathematical model took about 11 ms for encryption and decryption, while AES took about 30 ms. In comparison, the encryption and decryption efficiency of the improved mathematical model was significantly higher than AES, and the required encryption and decryption time was only one-third of AES, which verified that the improved mathematical model was reliable for the encryption and decryption of communication network data.

4. Conclusions

This paper designed an improved AES mathematical model combined with chaos for the encryption and decryption of communication network data. This model obtained the key of AES by two chaotic mappings. Moreover, the performance of the improved mathematical model was analyzed.

The experiment found that the key obtained by this method had good randomness and high sensitivity, small changes to the key would not yield the correct plaintext, and the ciphertext encrypted by the improved mathematical model had strong randomness. Moreover, the comparison of encryption and decryption efficiency suggested that the encryption and decryption time of the improved mathematical model was also significantly shorter than that of AES, which verified that the improved mathematical model was reliable and can be applied in the encryption and decryption of actual communication network data.

References

[1] Al-Rummana G A, Shinde G, Al-Ahdal A. "MapReduced Based: A New Stream Cipher Technique for Data Encryption," International Journal of Engineering and Advanced Technology, 2020, 9(5):763-769.

[2] Lata K, Chhabra S, Saini S. "Hardware–Software Co-Design Framework for Data Encryption in Image Processing Systems for the Internet of Things Environment," IEEE Consumer Electronics Magazine, 2022, 11(4): 92-97.

[3] Zhong J. "Network Communication Data Encryption Method Based on Wireless Channel Characteristics," International Journal of Circuits, Systems and Signal Processing, 2021, 15:1242-1251.

[4] Ratnadewi, Adhie R P, Hutama Y, Ahmar AS, Setiawan MI. "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)," Journal of Physics Conference, 2018, 954:1-8.

[5] Rahmani A. "A Hyperbolic Arnold's Cat Map-Based System for Multimedia Data Encryption," International Journal of Multimedia Data Engineering and Management (IJMDEM), 2021, 12(2):57-71.

[6] Laia O, Zamzami E M, Sutarman. "Analysis of Combination Algorithm Data Encryption Standard (DES) and Blum-Blum-Shub (BBS)," Journal of Physics: Conference Series, 2021, 1898(1):1-7.

[7] Golovko G, Matiashenko A, Solopihin N. "Data encryption using xor cipher," Control, Navigation and Communication Systems, 2021, 1(63):81-83.

[8] Arroyo J, Barbosa C P, Aborde M V, Yara F, Delima AJP. "An Improved Image Steganography through Least Significant Bit Embedding Technique with Data Encryption and Compression Using Polybius Cipher and Huffman Coding Algorithm," International Journal of Advanced Trends in Computer Science and Engineering, 2020, 9(3):3376-3383.

[9] Sari I C, Zarlis M, Tulus T. "Optimization of Data Encryption Modeling Using RSA Cryptography Algorithm As Security E-Mail Data," Journal of Physics: Conference Series, 2020, 1471(1):1-4.

[10] Nguyen N, Pham-Nguyen L, Nguyen M B, Kaddoum G. "A Low Power Circuit Design for Chaos-Key Based Data Encryption," IEEE Access, 2020, 8:104432-104444.

[11] Rusu-Anghel S, Mezinescu S S, Lihaciu I C. "Experimental stand and researches on pantograph-catenary contact force control using chaos theory," Journal of Physics: Conference Series, 2021, 1781(1):1-11.

[12] Schmitt-Grohé S, Uribe M. "Deterministic Debt Cycles in Open Economies with Flow Collateral Constraints," Journal of Economic Theory, 2021, 192:105195.

[13] Dennunzio A, Formenti E, Grinberg D, Margara L. "Dynamical Behavior of Additive Cellular Automata over Finite Abelian Groups," Theoretical Computer Science, 2020, 843:45-56..

[14] Gafsi M, Hajjaji M A, Malek J, Mtibaa A. "Efficient Encryption System for Numerical Image Safe Transmission," Journal of Electrical and Computer Engineering, 2020, 2020(5):1-12.

[15] Khandare N B, Chaudhari N S. "Secure and location privacy in geographical data with electronic codebook mode-advanced encryption standard," International Journal of Vehicle Information and Communication Systems, 2021, 6(1):22-39.