Research on Application of Packet Encryption Technology in Information Security Algorithm

Yuxi Zhou*, Mingjie Ma, Zenghui Jiang
Guilin University of Electronic Technology, Guilin, China
*Corresponding author’s e-mail: zhouyuxi@guet.edu.cn

Abstract. As the focus of the development of the whole society in the era of big data, information security is also the main direction of the practice and development of technological innovation. On the basis of understanding the current information transmission security and its algorithm research, this paper analyzes how to use this technology to guarantee information security according to the block encryption principle.

1. Introduction

In essence, data encryption is to change a set of data containing parameter K into E, and transform the explicit information M into E to form ciphertext C. In other words, encryption refers to C=Ek (M), decryption refers to M = DJ (M), while M = DJ (Ek (M)), this is the perfect information security encryption process. In this case, the parameter k represents the encryption key, j represents the decryption key, E refers to the encryption algorithm, D refers to the decryption algorithm. In general, cryptography can be divided into two types: if the encryption key K and the decryption key J are the same, it belongs to the symmetric cryptography; while when the two are different, it belongs to the asymmetric cryptography, also known as the public key cryptography. This paper mainly discusses the application of block encryption in information security algorithm.[1-4]

Transportation data and information in the network system are easily affected by internal and external factors, such as counterfeiting, tampering, interception and other threats, which can not only fail to guarantee the perfection of information acquisition, but also threaten the security and effectiveness of the internal system. Proposing appropriate encryption technology is also known as an effective weapon to deal with related problems. High-quality encryption technology can hide their identity while not being intercepted or interrupted in the transmission process. Assuming that the relevant verification information can be added to further verify whether the obtained information is forged or tampered with. Therefore, in the new era, in the face of increasing information data, it is necessary to strengthen the exploration of encryption technology and improve the requirements of practical research and development technology. From the analysis of the development and promotion of encryption technology, it can be seen that the earliest widely used encryption is Caesar encryption, which belongs to the representative of alternative
encryption method, and can be used in practice to prevent external intrusion while camouflage. The biggest advantage of this technology is that the encryption and decryption process is very convenient and simple, only need to replace the original letter fixed with other letters can get a bunch of unintelligible characters. Although this form of encryption meets the requirements of encryption, but because it is very simple, so the decryption process is very simple. Permutation encryption is different from other forms, which can be rearranged on the basis of breaking the order. This encryption technology is also called block encryption, which can improve the propagation of ciphertext. It is important to note that while this approach has a positive effect on preventing cracking and tampering, the actual encryption process is cumbersome and error prone. If there is a problem in a certain link of encrypted transmission, the whole translation will be affected, so it is not often used to process large-scale data information.[5-7]

2. Packet encryption

In the existing cryptographic system, the single-key block cipher is the basic content to guarantee information security, which can be used to construct stream cipher, message authentication code and hash function, etc., and can also be the core of data integrity mechanism and message authentication technology. In practical application, block password has high requirements, which can not only guarantee information security on the basis, but also have high requirements for platform operation mode, operation speed and storage quantity.

In essence, block ciphers encode a plaintext message into a sequence of numbers X0, X1... , xi... Divide into groups growing into n x= (x0, x1... Xn-1), and the key k= (k0, k1... Under the control of kT-1), it is transformed into an output number sequence of equal length Y = (y0, y1... Ym-1), and its encryption function E is, where Vn and VM respectively represent the vector space of N and M dimensions, and K represents the key space. Combined with the analysis of Figure 1 below, it can be seen that the biggest difference between it and the stream cipher is that all the output numbers are not only associated with the plaintext numbers, but with a group of length n plaintext numbers.

![Figure 1. Block diagram of block encryption](image)

Usually it is M = N, but if it is M > N then you can get the block password for data expansion, otherwise you can get the block password for data compression. In binary condition, both x and y belong to binary sequence, and both xi and yi belong to GF (2).

2.1. Substitution

Assuming that the packets of plaintext and ciphertext are both n bits, then all the packets of plaintext will have 2n value probabilities. In order to ensure the reversibility of encryption operation, all plaintext groups must have a unique ciphertext group, and only then can the
transformation be reversible. As shown in Figure 2 below, it refers to the substitution structure of n=4. There are 16 possible input states in the 4-bit input, and a certain state can be mapped to one of the 16 states by using the transformation structure, and each output state should be represented by 4 ciphertext bits. This is one of the most common aspects of block encryption and can be used to define all reversible mappings between plaintext and ciphertext.

![Substitution structure](image)

**Figure 2.** Substitution structure

### 2.2. Diffusion and confusion

To put it simply, diffusion is to integrate the characteristics of the plaintext statistics into the ciphertext. The specific operation requires that all contents of the ciphertext can be affected by the plaintext multiple times, such as the English message $M= M_1, M_2, M_3...$. The encryption operation formula of

$$y_n = \text{chr}\left(\sum_{i=1}^{k} \text{ord}(m_{n+i}) \mod 26\right)$$  \hspace{1cm} (1)

Where $\text{ord}(m_i)$ represents the sequence number corresponding to the letter $m_i$, and $\text{CHR}(I)$ represents the letter corresponding to the calculation sequence number $I$.

Obfuscation makes the statistical relationship between the ciphertext and the key more complicated, so that the intruder cannot obtain the key. In practice, complex and variable substitution algorithms are mainly used to achieve the desired effect, while simple linear substitution functions are difficult to achieve the goal.
The above two ways fully show the essential properties of block cipher, and have become the basic content of block cipher design.

2.3. Feistel cipher structure

Most block cipher architectures are proposed based on Feistel network architectures, which can obtain simple substitution ciphers by using product ciphers, and can execute two or more basic cipher systems in sequence, so that the final result can be stronger than the result composed of all basic cipher systems. Figure 3 below shows the Feistel network structure diagram. The encryption algorithm will input the plaintext and key \( K \) with the length of \( 2W \), and then divide all the plaintext groups into left and right halves \( L_0 \) and \( R_0 \). After many iterations, the left and right sides will be recombined to form a new ciphertext group. Wherein, the input function of the ith iteration is:

\[
L_i = R_{i-1} \\
R_i = L_{i-1} \oplus F(R_{i-1}, K_i)
\]

(2)

![Figure 3. Feistel network structure diagram](image)

Where \( K_i \) represents the sub-key used in round \( I \), which is obtained according to key \( K \). In general, the key of each wheel is different, and also different from \( K \).

The decryption process of this cryptographic structure is similar to the encryption process, both regard the ciphertext as the input content, but the order of using the sub-key \( K_i \) is completely opposite to the encryption process. In other words, \( K_n \) is used in the first round, \( K_{n-1} \) is used in the second round... And then the last round uses \( K_1 \). Figure 4 below is a diagram of Feistel's encryption and decryption process, with the former operating from top to bottom and the latter operating from bottom to top. Thus, the functional relationship between the input and output of round 16 in the process of encryption and decryption can be obtained as follows:

Encryption:
\[ LE_{16} = RE_{15} \]
\[ RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16}) \]  

Decryption:
\[ LD_1 = RD_0 = LE_{16} = RE_{15} \]
\[ RD_1 = LD_0 \oplus F(RD_0, K_{16}) = RE_{16} \oplus F(RE_{15}, K_{16}) \]
\[ = [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16}) \]
\[ = LE_{15} \]  

\[ (3) \]

\[ (4) \]

**Figure 4.** Encryption and decryption flow chart

### 2.4. Results

Combined with the above analysis, it can be seen that the two forms of block encryption are suitable for different types of information security requirements, and the final rendering effect is different. From the perspective of practical application, the application modes of block encryption are mainly shown in the following table. In the practical design application, designers need to make reasonable arrangements according to the requirements.[8-10]

**Table 1.** The working mode of table packet encryption

| **model**       | **describe**                                      | **Typical applications**                      |
|-----------------|--------------------------------------------------|-----------------------------------------------|
| Codebook (ECB)  | Each plaintext packet is encrypted independently with the same key | Secure transmission of a single data(such as an encryption key) |
| Ciphertext Block Linking (CBC) | The input to the encryption algorithm is the XOR of the previous ciphertext group and the next plaintext group | Packet oriented universal transport certification |
| Ciphertext      | S bits are processed once, and the cipher text   | Universal transport for data streams           |
3. Conclusion
To sum up, information security, as the focus of the current computer system operation, is also an important content for enterprises to explore in the continuous innovation. Applying block encryption technology to practical work can not only improve the level of information security, but also accelerate the research pace of current information security algorithms.

References
[1] Xie, X., Zhou, X., Liu, Y. (2019) Research on Authentication of User Information in Cloud Manufacturing[J]. Recent Patents on Engineering.
[2] Ingemarsson, I., Wong, C. K. (2003) Encryption and Authentication in On-Board Processing Satellite Communication Systems[J]. IEEE Transactions on Communications, 29(11):1684-1687.
[3] Yao, Y., Wang, Z. (2020) Privacy information antistealing control method of medical system based on cloud computing[J]. International Journal of Communication Systems.
[4] Wei, P., Zhen, Z. (2018) Research on security of information sharing in Internet of Things based on key algorithm[J]. Future Generation Computer Systems, 88(NOV.):599-605.
[5] Luo, Y. L., Du, M. H. (2013) Image Encryption Algorithm Based on Quantum Logistic Map in Wavelet Domain[J]. Journal of South China University of Technology(Natural Science Edition), 41(6):53-62.
[6] Haleem, M. A., et al. (2008) Joint Encryption and Compression of Correlated Sources with Side Information[J]. Eurasip Journal on Information Security.
[7] Zhang, L., Zhang, Z., Kang, Y., et al. (2019) Research on Double-Layers optical information Encryption Based on Ghost Imaging[J]. Optics Communications, 455:124585.
[8] Shi, W., Kumar, N., Peng, G., et al. (2015) On the security of a certificateless online/offline signcryption for Internet of Things[J]. Peer-to-Peer Networking and Applications, 8(5):881-885.
[9] Meng, X. F., Cai, L. Z., et al. (2006) Two-step phase-shifting interferometry and its application in image encryption.[J]. Optics letters, 31(10), 1414-6.
[10] Yuan, Y., Fukushima, K., Xiao, J., et al. (2021) Memory-onstrained implementation of lattice - based encryption scheme on standard Java Card platform[J]. IET Information Security.