Ghazala Firdaus Ansaria, 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Review: Application of Data in Cryptolysis System

Research Scholar Ghazala Firdaus Ansari, Prof.Dr. Ritesh Kumar Yadav,
Prof. Dr. Versha Namdeo
Department of Computer Science Engineering
R.K.D.F. Institute of Science & Technology, SRK University,
Bhopal Madhya Pradesh India.
ghazala11oct@gmail.com

Abstract- Among the many unstable factors in network security, the most prominent is the data security with the smallest granularity in the security and confidentiality levels involved in the operation of the application system. In order to improve the status quo of network security and improve the security of the data transmission process, International Data Encryption Algorithm (IDEA) is one of the cryptographic techniques which support the concept of symmetric key encryption and decryption. It uses 128-bit key over 64-bit plain text and runs for eight and a half rounds. To enhance the technology in IDEA, a new approach is introduced in which we will introduce a full encryption algorithm (RSA) in IDEA making it run for more steps, extra to those of IDEA. Secondly, we will use two different keys for encryption and decryption respectively which was single key in IDEA. This will set up more security in IDEA by converting it into an asymmetric encryption algorithm. In addition to it, we will use 512-bit+128-bit key over 64-bit plain text to enhance data protection. This paper studies and discusses the definition, classification, principle and application of data encryption technology, and at the same time provides support for other related theories.

Keywords- International Data Encryption Algorithm, cryptographic techniques, plain text, enhances data protection.

I. INTRODUCTION

Due to the late start of China's industrial simulation software, the current virtual simulation market is basically occupied by foreign products, and the emerging forces are accelerating to enter. In order to help China occupy a field of simulation market, promote the research and development of simulation software, and ensure the security and stability of simulation network operation.

This paper analyzes the definition, classification and principle of data encryption technology, and discusses the application of some encryption technology in simulation software. Discusses the definition, classification, principle and application of data encryption technology, and at the same time provides support for other related theories.

Homomorphism Encryption (HE) was first proposed by Rivest in 1978 with the concept of "privacy homomorphism". It is a kind of encryption scheme that can directly manipulate cipher text. The basic idea is that the encryption of plaintext after addition or multiplication is equivalent to that of cipher text after encryption.

II. COMPUTER NETWORK INFORMATION SECURITY

With the advent of the "Internet of Everything" era, cyberspace, as the fifth space in addition to land, sea, air, and sky has formed network forms such as the Industrial Internet, the Internet of Vehicles, social networks, and the Industrial Internet. Due to the influence of various factors, computer network information security is difficult to effectively

guarantee and it is prone to problems such as information loss, leakage, decryption, tampering, interception, etc., which poses a huge threat to the normal operation of all walks of life and even affects people. The normal use of information will endanger allergic personal and property safety and even national security [4].

These threats can be roughly summarized as the following:

1. The vulnerability of the computer network itself:
The complexity, sharing, real-time and accessibility of computer networks determine the vulnerability of the computer itself. Among them, the advantage of the shared network feature is the rapid generation and transmission of network information, which facilitates information sharing between users, but it has also become a breakthrough point in the theft of network information today.

2. Hacking illegal intrusion and attack:
The rapid development of the network is generally positively related to the development of the Capabilities of technical personnel. As the network becomes more and more complex, the attack Capabilities of hackers are also advancing with the times. Hacking is the most serious security problem facing the network. In the first half of 2021, hackers attacked Colonial which is the largest fuel pipeline Operator in the United States and forced the United States into a national emergency. In the end, Colonial paid the hackers 75 bitcoins. The purpose of most hackers' attacks is to extort money and some are because of hobbies.

3. Other factors such as improper operation:
Other factors that cause computer network insecurity include man-made factors, natural factors and some accidental factors. Human factors are the fundamental reason for the insecurity of computer Information networks. At present, many people still do not have enough security awareness. They think that there is nothing too important in their electronic equipment or that there will be no such boring people coming to steal information, so they do not consider the operation of the machine from the perspective of security when setting the password or using it, which makes the criminals organic. It can Take advantage of it. This situation has brought harmful effects to electronic equipment. There are also people with insufficient security technology capabilities, improper operations, incomplete test points. During security testing before the system goes online and insecure server configuration when deployed online, which leads to vulnerabilities in the system, which also brings hidden dangers to the security of the WEB side.

III. PRINCIPLES OF CRYPTOGRAPHY

Cryptography is implemented using following tools:

- A plain text
- A cipher text
- Key
- An Encryption algorithm
- A Decryption algorithm

Plain Text is conventional readable file without dispensation and formatting. This plain text is transmitted by sender to receiver.

IV. DEVELOPMENT OF HOMOMORPHISM ENCRYPTION TECHNOLOGY

Homomorphic Encryption (HE) was first proposed by Rivest in 1978 with the concept of "privacy homomorphism" [1]. It is a kind of encryption scheme that can directly manipulate cipher text. The basic idea is that the encryption of plaintext after addition or multiplication is equivalent to that of cipher text after encryption. Before the concept of homomorphic encryption was proposed, some encryption algorithms met homomorphism, for example, Hill encryption algorithm met the addition homomorphism [2].

With the introduction of the concept of privacy homomorphism, more homomorphic encryption schemes have been proposed. Rivest, Shamir, and Adleman proposed RSA algorithm based on number theory when the concept of homomorphic encryption was born [3], which satisfies any multiplication homomorphic operation.

In 1984, Goldwasser and Micali used probability encryption to propose a GM algorithm based on trapdoor function and quadratic residue [4], which was the first homomorphic public- key encryption algorithm with semantic security. However, this scheme only satisfies the addition homomorphism of any submodule 2 and has low efficiency. In 1985,

ElGamal, an asymmetric encryption algorithm based on public key cryptosystem and elliptic curve cryptosystem, was proposed [5]. The algorithm satisfies any multiplicative homomorphism and can be used for encryption and signature. In 1994, Benaloh proposed an improved probabilistic encryption algorithm [6], which can encrypt r bits at a time, but this algorithm can only perform a finite number of addition homomorphic operations. The famous Paillier encryption scheme based on the quadratic residue was proposed in 1999 [7].

This scheme is a random encryption scheme, which can perform any addition homomorphic operation. In 2005, Boneh, Goh and Nissim proposed the BGN cryptosystem based on bilinear pairings [8].

This algorithm satisfies any addition omomorphism and one multiplication homomorphism. It is the nearest scheme to the idea of homomorphism. These algorithms either satisfy the homomorphism of addition, such as GM and Paillier, or the homomorphism of multiplication, such as RSA and ElGamal, and BGN, which satisfies the homomorphism of multiple addition and single multiplication.

They all basically have a single homomorphism, so they are all called single homomorphic encryption algorithm. Gentry proposed the first homomorphic encryption scheme based on ideal lattices in 2009[9], which can add and multiply ciphertext any number of times. Then homomorphic encryption technology entered a period of rapid development.

Homomorphic encryption technology can be divided into three categories: the first is an ideal lattice-based fully homomorphic encryption scheme proposed by Gentry, which is to construct a Somewhat Homomorphic Encryption (SWHE) on the ideal of various rings, then compress the decryption circuit to reduce polynomials, and finally complete the fully homomorphic encryption under the assumption of cyclic security through bootstrapping technology.

The second is an integer-based homomorphic encryption scheme [10], which is based on Gentry's idea but does not require operations based on ideal lattices of the polynomial ring. All operations are based on integers. The third is a fully homomorphic encryption scheme based on LWE (Learning with Errors) or R-LWE (Learning with Errors over Ring). This scheme is based on fault-tolerant learning and constructs a fully homomorphic encryption scheme using non-linearization, such as BGV encryption scheme [11].

1. Single Homomorphic Encryption Algorithm:

Before the concept of "privacy homomorphism" was put forward, some algorithms met some homomorphic requirements, such as Hill Cipher. After the concept of homomorphic encryption was put forward, more homomorphic encryption algorithms were proposed, such as RSA, Paillier, ElGamal and other encryption algorithms [13].

With the development of cloud technology, many homomorphic encryption algorithms make full use of the parallel performance of the cloud environment to improve the efficiency of encryption and decryption. More research and application of homomorphic encryption technology also improve the security of data in the cloud environment [14].

2. The basic concepts:

2.1 Hill cipher:

The Hill Cipher is a polygraphic substitution cipher based on linear algebra, invented by Hill in 1929. The encryption is:

$$C = E_k(M) = KM \bmod 26 \qquad (1)$$

Where K is a key matrix and M is an n-component vector, each letter is represented by a number modulo 26: A = 0, B = 1, C=2..., Z = 25.

M (consisting of a string of letters) is multiplied by K (an n× n matrix), against modulus 26.

The key matrix used for encryption must be reversible, otherwise, it is impossible to decrypt. The decryption is:

$$M = D_k(C) = K^{-1}C \bmod 26 \qquad (2)$$

Where K-1 is the inverse matrix of K and C is the cipher text.

2.2 RSA (Rivest–Shamir–Adleman):

RAS is a block cipher algorithm [3], whose plaintext and cipher text are integers between 0~n-1. Generally, the size of n is 512 bits or 1024 bits of the

binary number. Key generation: p, q are two large prime numbers p≠q and n=p*q.
According to Euler's theorem Φ(n)=(p-1)(q-1), the integer e is randomly selected to make gcd(Φ(n),e)=1,1<e<Φ(n) and d≡e-1modΦ(n), where the public key is KP={n,e} and SK={d}. The encryption is:

$$C=Ekp(m)=me \bmod n \quad (3)$$

Where m is the plaintext, and e is the public key. The decryption is:

$$M=D_{sk}(C)=C^{d} \bmod n \quad (4)$$

Where C is the cipher text and d is the sk. It can be seen from the encryption that the RSA algorithm satisfies the homomorphism of multiplication.

3. Efficiency comparison of single homomorphicen cryption algorithms:

Table 1. Mathematical problems on which single homomorphic encryption algorithms are based

Algorithms	Hill	RSA
Mathematica lproblems	Linear transformation matrix	Integer factorization

Table.1 shows the mathematical problem on which each algorithm is based. Through the above analysis, it can be seen that these curity of the Hill encryption algorithm is general. These curity of RSA and ElG amalis relatively good, which can meet the requirements of general encryption, and the security of the Paillier encryption algorithm is the highest.

Table 2. Time of Encryption and Decryption.

Time/Algorithms		
Encryption（s）	23	198
Decryption（s）	22	274

V. CONCLUSIONS

With the wide application of cloud computing, the security of cloud platform has become one of the core issues of the cloud computing, which restricts the development of cloud computing. Homomorphic encryption can directly process ciphertext data, effectively ensuring the security of cloud user data. However, there are still some problems to be solved in homomorphic encryption, which can be summarized as for single homomorphic encryption algorithms: Hill encryption algorithm with symmetric encryption is not safe, so most commonly used encryption algorithms are public key encryption algorithms. However, the current public key encryption efficiency is not high, and the encryption and decryption speed needs to be improved.

For fully homomorphic encryption algorithms : the current circuit homomorphic encryption algorithms should be – BNA replaced by the algebraic homomorphic encryption algorithms; the ciphertext expansion rate and computational complexity should be reduced and the computational efficiency should be improved; more research and improvement should be needed in the NTRU based fully homomorphic encryption and vector-based fully homomorphic encryption.

REFERENCES

[1] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[C] Foundations of Secure Computation. New York: Academic Press, 1978: 169-179.
[2] Hill L S. Cryptography in an algebraic alphabet [J]. The American Mathematical Monthly, 1929, 36(6): 306-312.
[3] 0Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems [J]. Communications of ACM, l978, 21(6): 120-126.
[4] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.
[5] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions of Information Theory, 1985, 31(4): 469-472.
[6] Benaloh J, Tuinstra D. Receipt-free secret- ballot elections [C] Proc. of the 26th Annual ACM Symposium on the Theory of Computing, New York, ACM, 1994: 544-553.
[7] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [J]. Proc Eurocrypt, 1999, 547(1): 223-238.

[8] Haque S et al. Alzheimer's disease: Resting-State Brain Networks and Deep Learning Methods Design Engeering 2021 (7):15961-15971.

[9] Haque S et al. A Deep Learning Model in the Detection of Alzheimer Disease Vol.12 No.10 (2021), 4013-4022.

[10] Boneh D, Goh E J, Kobbi N. Evaluating 2-DNF formulas on ciphertexts [C] Theory of Cryptography - Second Theory of Cryptography Conference, LNCS 3778. Berlin: Springer, 2005: 325-341.

[11] Gentry C. Fully homomorphic encryption using ideal lattices [J]. Proc. of the Annual ACM Symposium on Theory of Computing. 2009, 19(4) :169-178.

[12] Dijk M, Gentry C, Halevi S, et al. Full homomorphic encryption over the integers [C] Proc. of EUROCRYPT'2010, LNCS 6110, Berlin: Springer, 2010: 24-43.

[13] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Full homomorphic encryption without bootstrapping [C] Proc. of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012: 309-325.

[14] Aiswarya R, Divya R, Sangeetha D, et al. Harnessing healthcare data security in cloud [C] Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, IEEE, 2013: 482-488.