TELKOMNIKA, Vol. 11, No. 12, December 2013, pp. 7386~7391
e-ISSN: 2087-278X

The Application of ElGamal Encryption Technology to the Information Security of Digital Library

Zhang Fujun
Library of Shandong University of Science and Technology, Qingdao, Shandong, China, 266590
e-mail: alibzhang@126.com

Abstract

Nowadays, the construction and application of digital library leads a new era of the way people obtain knowledge and information, and promotes the academic exchanges and social progress. Digital library, however, also involves great risk; hacker attacks become the main threat of the information security of digital library, and may probably cause the loss and damage of the information resources in library. This article mainly introduces the advantages and the potential safety hazard of digital library, and then makes an analysis aiming at the information security of digital library, and finally puts forward an algorithm based on ElGamal encryption to protect library information encryptedly, and effectively guarantee the information security of digital library.

Keywords: *digital library, information security, encryption technology, ElGamal algorithm*

1. Introduction

Along with the progress of the society, the limited resources of the traditional library can not meet people's spiritual needs. Compared with the traditional library, digital library has the advantages of rich resources, not easy to damage, easy access to information and that resources can be shared, etc [1]. With the advent of the information era, the rise of digital library becomes the gospel on the road to learning, and more and more people search for the documents and information they need through the network. digital library realizes the storage of huge capacity and magnanimity information processing, and makes digital library users to get huge information resources. However, digital library has hidden troubles in addition to the great advantages, for example, hackers and computer virus can lead to the information loss of digital library. Today great importance is attached to intellectual property, so it will lead to huge losses if part of the secret information is lost. ElGamal algorithm can not only be used for data encryption, but be used for digital signatures, and its security relies on the problem of divergence logarithm in finite domains [2]. When the information of the library, use ElGamal algorithm to encrypt information, which effectively protects the information of digital library which is in the process of transferring to the user from stealing and damaging by illegal users.

2. The Overall Design

The design method of this article is the modification of database access to the process of digital library. Decipher the data according to the users request and show it in the client, encrypt the data submitted by the client and then submit it to submit digital library database. Add security management module between the database management system and database application system in digital library to complete the functions of the above analysis, encryption and decryption, and key management, etc. The database encryption system adopted the way of above-mentioned has the following characteristics:

(1) It is completely transparent to the end-user of digital library.

(2) It solves the most important problem of the information security of digital library. Hackers are still difficult to get the required information; even they steal the information data of digital library, because all the data have been encrypted. In addition, after the database of digital library is encrypted, we can set plaintext that is not necessary for system administrator to see, which greatly improves the security of the data [3].

Received June 18, 2013; Revised July 23, 2013; Accepted August 24, 2013

(3) The data is encrypted in the client and ciphertext is transmitted in the internet which increases the security of network transmission.

(4) It is totally independent of database application system, and can realize the encryption function without changing the database application system of digital library which saves the trouble of modifying original application system.

(5) The encrypted and decrypted calculation of data in the client, does not affect the system effectiveness of database server, and the encryption and decryption calculations of data does not delay basically.

(6) Because the interface software needs to be changed, the development tool for different clients and the management tool of database in server, can design special interface software to shield all kinds of database and enhance its extensibility.

(7) It is unrelated with the application progress. It can put the encrypted requests into a database. When the encrypted requests (encryption dictionary) change, the system administrator can complete the new encryption requests by performing the corresponding module of encryption modification. It has certain flexibility.

The overall design scheme of encryption system is as follow:

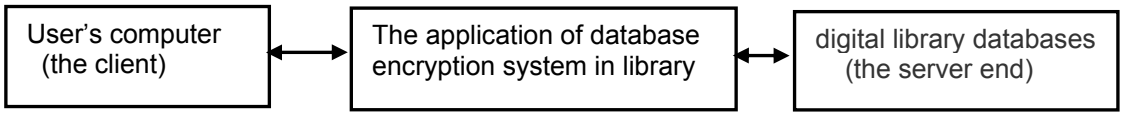

Figure 1. The Overall Design Scheme of Encryption System

3. Digital Library

The concept of digital library was proposed in the early 1990s, became a focus technique of the information era, and was regarded as the point of information construction in many developed countries [4]. So far, it reaches a consensus to construct and develop digital library throughout the world. We are in the information age today, and the dissemination and communication of information directly affects the production, economic and political fields, etc. Digital library will change the previous information storage methods which regard the books as the main carrier, break through the limitation of space and time in the process of disseminating information, and promote the progress of science and technology and the development of the society.

Digital library is in essence a multimedia information repository, takes distributed massive groups of information database as resources, takes the network as transmission platform, and overcomes the space and time limitation to make the users to get the information they need through the network. Compared with the traditional library, digital library has the following advantages:

1. Rich in resources: the stored books in traditional library books are very limited. People often can't find the information they need in the library, but there are massive information and data stored on the network, the information stored on the internet is much richer than that in library.

2. The information is hard to damage: mostly the information is recorded in the form of books in traditional library. After used for a long time, the books may be damaged, lost, and so on unavoidably, which greatly damage the integrity and accuracy of information.

3. The information is easy to gather: compared with the traditional library, digital library breaks through the limit of space and time. Users no longer need to run to a specific library, no longer need to check books out, as long as there is Internet and computer, you can get the information in the digital library.

4. Resources can be shared: in traditional library, the number of same books is limited, and users who can obtain information will also be limited, which greatly reduces the sharing of information. In digital library, tens of thousands of users can have access to the same information, the sharing of digital library resources is unmatched by traditional library [5].

Today, information transmission deeply affects the progress and prosperity of a country and throughout the world. Digital library is the product of social informatization and

digitalization, adapts to the change and demand of the times. Many developed countries hold on to the construction of digital library and digital library has become an important symbol to evaluate the information infrastructure of a country. The transition from traditional library to digital library is inevitable for social progress.

Digital library provides massive information and convenient service for users, meanwhile, it is also a new challenge for the security of information. During the process of transmitting massive information to users, digital library can not ensure that the information is not stole or damaged by illegal users. Hackers may look for the security vulnerability to steal the user's information or damage stored information in the process of data transmission and open interface offers opportunity for illegal access.

So we put forward an encryption algorithm technology based on ElGamal to guarantee that the data information in digital library will not be stolen or damaged in the process of transmission.

4. ElGamal Digital Signature Algorithms

4.1. The Generation Method of Key Pair

ElGamal algorithms can not only be used in data encryption, but in digital signature and the security relies on the problem of divergence logarithm in finite domains.

Firstly, choose a prime number p, and two random number g, x, where g < p and x < p, calculate $y = g^x (\mathrm{mod}\ p)$, of which y, g, and p are the public keys. The private key is x. G and p can be shared by a group of users.

When ElGamal is used in digital signature, signed information is M. Choose a random number k, in which k and p - 1 are relatively prime. Calculate $a = g^k (\mathrm{mod}\ p)$ and solve the following equation b: $M = xa + kb (\mathrm{mod}\ (p-1))$. The signature is (a, b) and random number k must be discarded. The produce flow chart of signature (a, b) is shown in Figure 2:

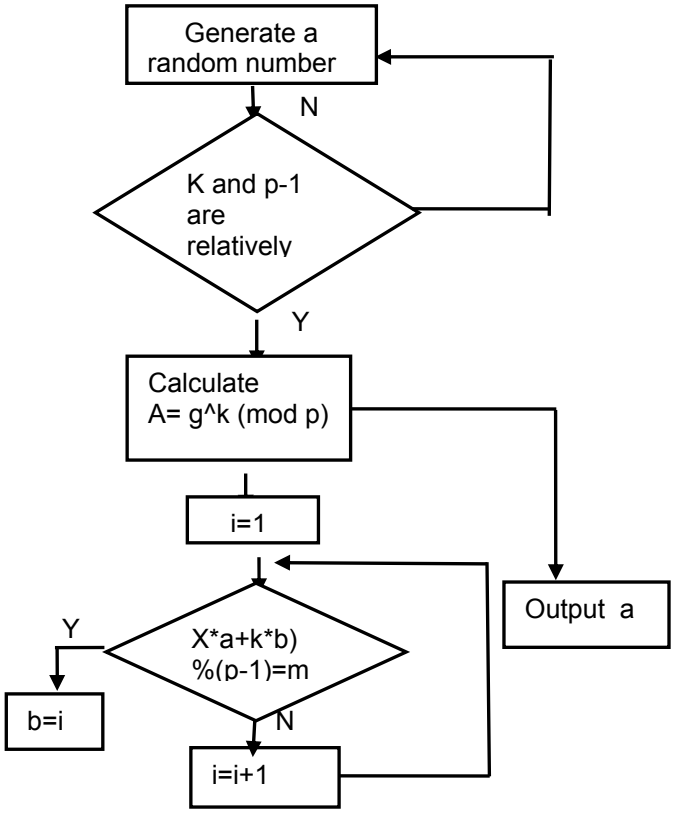

Figure 2. The Produce Flow Chart of Signature (a, b)

Verify the following equation $y^a * a^b (\mathrm{mod}\ p) = g^M (\mathrm{mod}\ p)$

At the same time, verify whether it satisfies the condition: $1 <= a < p$, otherwise the signature is easily forged. The verification flow chart of digital signature is as follows:

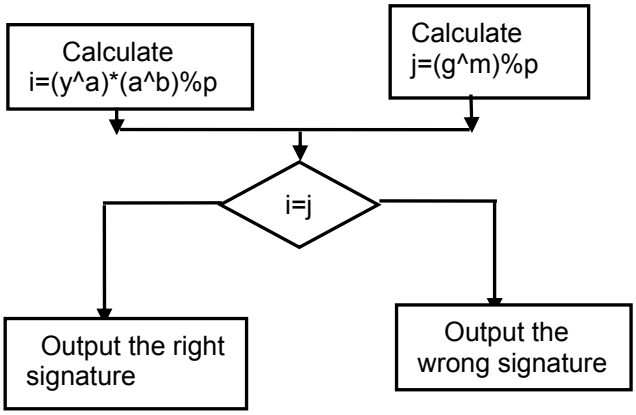

Figure 3. The Verification Flow Chart of Signature

The security of ElGamal signature relies on the calculation of discrete logarithm of the multiplicative group (IFp)*. Prime number p must be large enough and p-1 contains more than one large prime factor to resist attacks of Pohlig & Hellman algorithm [6]. M generally should adopt the HASH value of information. The security of ElGamal mainly depends on p and g. If selection is improper, signature may be forged easily, should guarantee the g is irreducible to large prime number factor of p-1.

4.2. ElGamal Digital Signature Scheme

There are two users A and B in the system. A sends messages to B and signs them. B verifies after he receives the messages and the signature.

1) System Initiation

Select a large prime number p, and g is the primitive element of GF (p). H: GF (p) → GF (p), is a one-way Hash function. System stores the parameters p, g and h in the shared file, so each user in the system can obtain above parameters from the shared file [7].

2) The process of digital signature to the messages sended

Assumed that A will send message m[1, p-1] to B and sign the message m.

The first step: A selects x[1, p-1] as privacy key and the calculation $y = (\mathrm{mod}\ p)$ as public key and then deposits public key y in shared file.

The second step: Select k[1,p-1] and $\gcd(k,(p-1)) = 1$ randomly and calculate $r = (\mathrm{mod}\ p)$.There is signing equation for the common ElGamal digital signature scheme: $ax = bk + c(\mathrm{mod}(p-1)$. Where (a, b, c) is a replacement of mathematical combination (h(m), r, s). We can solve s through signing equation. Then (m, (r, s)) is the digital signature of A to message m.

The third step: A sends (m,(r,s)) to B.

3) The process of verification of digital signature

When B receives the message (m, (r, s)) sended by A, he obtains the system communal parameter p, g and h and A's public y from the open files of system and A. According to (m, (r, s)), he calculates (a, b, c) to verify the validity of the equation $y = (\mathrm{mod}\ p)$.

5. Generation of Security Parameters

5.1. The Analysis of Safety Algorithm

The security of ElGamal algorithm is based on the problem of divergence logarithm of finite domains. Even the message m is given, it's also very hard to calculate private a and random integer k through cryptograph (γ, δ) and public key (p, α, αa) because a and k are indexes.

5.2. Three Methods of Primality Testing Used Commonly

At present, there are three methods of primality testing commonly used: Fernat primality testing based on Fernat's little theorem, Solovay-Stassen primality testing based on the Euler's quasi-prime number, and Miller-Rabin primality testing based on strong quasi-prime number [8].

When the first two methods test successfully every time, the probability that n is a prime number is greater than 50%, while, if Miller-Rabin primality testing succeeds every time, the probability that n is a prime number greater than 75%. Every method tested whether n is quasi-prime number many times to make the probability that n is prime to 100%.

5.3. Miller-Rabin Primality Testing

Set that n is an odd composite number, then the probability that n is the strong quasi-prime number for The Base b, 1≤b≤n-1, is not more than 25%. Given that odd integer n≥3 and safety parameter k, and variable i=1 [9].

Set n - 1= 2 st, of which t is an odd number. Randomly select integer b, 2≤ b≤ n - 2. Calculate d= (b, n).

Judge: if d > 1, then turn to step 12; Otherwise, turn to step 4.

Let J = 0, calculate r ≡ bt mod n. Judge: if r ≡±1 mod n, turn to step 10; Otherwise, go to step 6.

Let j = j + 1, if j < s, turn to step 8; Otherwise, turn to step 12.

Calculate r = r2 mod n.

Judge: if r = -1 mod n, turn to step 10; Otherwise, turn to step 6.

Let i = i + 1 (n passes a round of primality testing), if k ≤ l, turn to step 1, and if n passes rounds of testing, output "pass", and turn to step 13.

If n is composite number (n does not pass this round test), output "no pass", and turn to step 13.

The end.

6. The Environmental Results

In this article, b takes four fixed values 2, 3, 5 and 7, which are all prime numbers, that is, a large number is tested four times by Miller-Rabin primality test. The probability that an integer n is a prime number which passes a prime testing is greater than 75%, so the probability is greater than (1-1/44) if n passes the test four times.

Through the test, we can randomly choose large prime Numbers p and q, and through p and q, we can calculate the safety parameters n. It is very easy to multiply two large prime numbers, however, it's hard to factorize the product. N guarantees the security of the system to a certain extent.

In this article, n = (2 p + 1) (2 q + 1). Part of the data generated by the operation of program are shown in the figure below, of which p\q means the product of p and q, and is used for selection of the private key y and y. After getting the values of private key y and Y, then calculate $z = g^y \bmod n$ n. PK = (n, a, a0, g, h, m, z, z) is the public key of system. Among them, a, a0, g, h and m are the quadratic residue of n (omitted here) [10]. The values of Arbar and beita coact to calculate x, and the values are generated under the action of the user and the digital library. This article only needs to use x for calculation, and there is no need to know the value of x in detail, so I randomly select the related data from the scope of the standard, and get x through analogue computation. X is equal to the user's private key which is used to calculate the user's information C2 = ax mod n and the data information $T_4 = m^x \bmod n$ [11]. The result chart of ElGamal security parameters is shown in Figure 4:

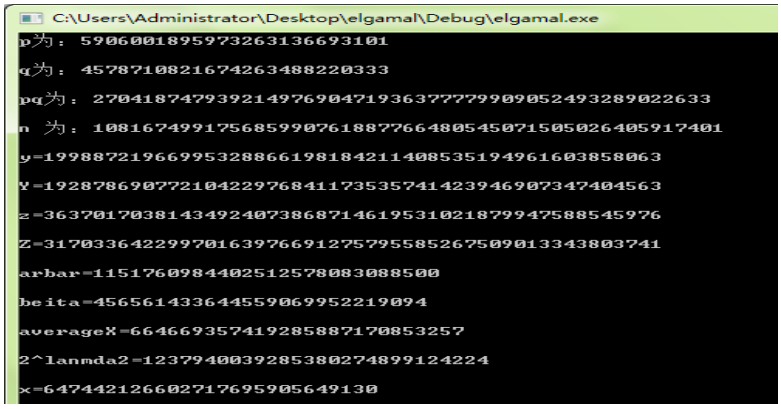

Figure 4. The Result Chart of ElGamal Security Parameters

7. Conclusion

For the construction and extensive application of digital library in the current information age, this article briefly introduces the advantages of digital library compared with traditional library, expounds the contribution of digital library to the progress of scientific and technological and society. At the same time, analyze the information security of library, and put forward a kind of technology based on the combination of ElGamal encryption algorithm and digital library, to effectively protect the information resources in digital library. By means of C Language, generate the key pair, and verify the digital signatures.

In this article, we understand the basic principle and realization method of ElGmal algorithm, and realize the process from the secret key generating, signature generating to the signature, at last, make a primality testing for ElGmal algorithm [12]. Experimental results prove that ElGmal algorithm is helpful to avoid the threat of theft or damage of digital library information during the transmission, and safeguards the interests of digital library.

References

[1] Zhu Yihong. Cloud Computing and Traditional Library: Subversion or Change. *Lantai World.* 2011; 28(8): 76-77.
[2] Sun Lihong. Public Key Cryptosystem Based on Multiplicative Group. *Journal of Liaoning Technical University (Natural Science).* 2011; 30 (3): 464-467.
[3] Tang Zhuoliang. Total Innovation of Knowledge Economy and University Library and Information Service. *Library and Information Service.* 2000: 16-17.
[4] Zhou Bo. Study on the Service Mode of Digital Library. *Modern Information.* 2010; (10): 44- 47.
[5] Shao Zuhua. Signature Scheme Based on Discrete Logarithm without Using One-Way Hash Function. *Electronic Letters.*1998; 34(11): 1079-1080.
[6] Tiersma HJ. Enhancing the Security of ElGamal's Signature Scheme. *IEE Proc Computers and Digital Techniques*.1997; 144(1): 47-48.
[7] Lu Jianzhu, Chen Huoyan, Lin Fei. Multi-digital Signature Algorithm and the Security of ElGamal. *Journal of Computer Research and Development.* 2000; 37(11): 1336-1339.
[8] Zhou Li, Xu Ye, Wan Jian. Multi-digital Signature Algorithm and the Security of ElGamal. *Journal of Computer Research and Development.* 2007; 27(3): 41-43.
[9] Qi Ming, Xiao Guo-zhen. Enhancing the Security of Generilized ElGamal Type Signature Schemes. *Acta Electronica Sinica.*1996; 24 (11): 68-72.
[10] ELGAMAL T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transaction on Information Theory.* 1985; 31(4): 469-472.
[11] Shang Yulian, Jia Wuyuan, Zhang Lanhua. A General Threshold Signature and Authenticated Encryption Scheme Based on ElGamal System. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(7): 3789-3797.
[12] Wang Guofu, Zhang Faquan, Ye Jincai. Remote Control Techniques to the Digital Storage Oscilloscope by GPIB and VISA. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(4): 1835-1840.