Research on Digital Signature in Electronic Commerce

Hongjie Zhu, Daxing Li

***Abstract*—With the development of Internet, digital signature becomes more and more important for the electronic commerce security because of its data integrity protecting and privacy. This paper is to propose a kind of digital signature based on public key. By this way, both digital signature and defending illegal interpolation and replication of digital products are effectively realized. Finally, a material digital signature system is given with Java.**

***Index Terms*—Electronic Commerce; digital signature; encrypting with public key.**

I. Introduction

With the development of network and software technology, applications of internet make great influence on traditional working. At the same time, E-commerce emerged and developed rapidly, playing great role in business activity. With contrast to traditional business pattern, E-commerce has characteristic of great convenience and high efficiency [1]. Even though, the volume of trade by E-commerce of the whole world today is still little. That E-commerce lies on computer and communication technology which has a lot of security flaw is the reason. E-commerce needs reliability and high security [2]. The data transferred on E-commerce system must have the characteristic of anti-deniability, integrity, security, and identity-authentication. Security restricts the development of E-commerce. Digital signature can resolve the problem because of its data integrity protecting and privacy. So digital signature is widely used in E-commerce system [3].

In this paper, the theory and application of digital signature is described, and the realizing method of digital signature in E-commerce is introduced detailed. At last, a digital signature system realized in Java is proposed.

II. Digital Signature Technology

A. Functions of Digital Signature

Digital Signature is a method to encrypt a message (such as documents, contracts, notifications) which will be transferred, adopting data-exchanging protocol and data-encrypting algorithm. An abstract is produced in this procession. The abstract is like signature or seal which can be used by receiver to verify the identity of the sender [4].

The functions of digital signature: (1)Assuring data integrity. Once the message changes a little, the abstract will change a lot for hash function's peculiarity, so that avoids the message being distorted. (2)Anti-denibility. Using public key cryptography algorithm, the sender can't deny that he has sent the message for he has the private key. (3)Avoiding receivers forging message that is claimed to be from the sender.

B. Public Key Encrypting Scheme

As the base of digital signature technology, public key encrypting technology should be introduced first in the following content.

In the traditional cryptography system, the cipher code used in the process of encrypting plain text into cipher text and in the inverse process is the same. This method is called symmetric cryptography technology.

Public key encrypting scheme is a kind of unsymmetric cryptography technology. It resolves the difficult problems in application. Its basic idea: the keys of the two parties are different. Every user has a key pair. One is private key which is saved by the user himself, another one is issued in public places such as internet for downloading or enquiring. Public key algorithm is very slow (with contrast to private algorithm). It is designed for a little data, but not for much data. It is usually used together with hash function in digital signature.

C. Hash Algorithm

Hash algorithm is an algorithm which is used to compute a data fingerprint of a data block. It is a one-way function which satisfies the following conditions:

1) can receive data with any length;
2) can produce abstract with fixed length;
3) can compute abstract easily;
4) can not compute message from abstract;
5) It is impossible to find two different messages which have same abstract.

Hash function can make short abstract with fixed length for the binary data with any length. The popular hash algorithms are MD5, Secure Hash Algorithm (SHA, having all kinds of security level.) and so on.

III. Principle and Procession of Digital Signature

A. Principle of Digital Signature Technology

Digital signature technology is realized by public key

Manuscript received January 7, 2008.

Hongjie Zhu is with the School of Information Science and Technology, Shandong Institute of Light Industry, Jinan China. (phone: 86053189631256; fax: 86053189631256; e-mail: zhj@sdili.edu.cn).

Daxing Li is with the Institute of Network Secutity, Jinan China. (e-mail: ldxl@sdu.edu.cn).

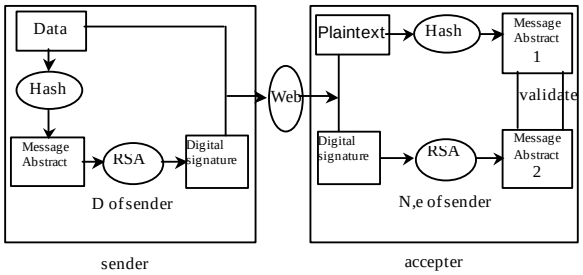

Fig.1 digital signature algorithm

encrypting technology combining with data decomposition function. Decomposition function is hash function. Firstly, the message is made into abstract with help of hash function; Secondly, the abstract is encrypted by the sender's private key, the result is the digital signature. The receiver can identify the sender's identity by testifying the digital signature. The testifying procession is:

The message is recovered from the abstract with the sender's public key. Then the abstract is computed again by the recovered message. Comparing this abstract with the former one, if they are equal, it is assured that the file is integrated and correct, and the signature is true. If the file is distorted or a signature is forged, the two abstracts will be different from each other. Then the procession of testification of the digital signature will fail. Signing procession is described as Fig 1:

Fig 1 tells that the digital signature algorithm consists of signing algorithm and testifying algorithm. Nowadays, the popular digital signature algorithm is RSA and DSA.

(1) RSA is developed by Rivest, Shamir and Adleman. It is first issued in 1978. Plain text is Encrypted by group. The length of every group is less than or is equal to $\log(n), n$ is a integer. Algorithm description:

The sender chooses two prime integer p, q which is possessed by him.

$n = pq$ is public.

e is public and is choosed freely. e is co-prime with $(p-1)(q-1)$.

$$d = e^{-1} \bmod (p-1)(q-1)$$

The private key is $\{d, n\}$,public key is $\{e, n\}$, M is plain text, C is cipher text. encrypting: $C = M^c \bmod n$, disencrypting: $M = C^d \bmod n = M^{ed} \bmod n$.

Due to number theory, it is impossible to compute e from d while it is easy to compute d from e.

The data which will be signed is transformed into a hash value with fixed length. The hash code is M which is encrypted into digital signature(DS). DS along with data is sent to receiver. The receiver computes the hash value of the received data as M' with the same hash algorithm, disencrypting the DS1(perhaps different from DS).The validity of the signature will be known by comparing M and M'.

(2) DSA is based on the difficulty of computing logarithm. DSA is proposed by ElGamal and Schnorr. Description of the DSA:

① p is prime and $2^{L-1} < p < 2^L$, $512 < L < 1024$, L is multiple of 64, and it is public.

② q is the prime factor of $(p-1)$ which can be divided exactly by q , and satisfies $2^{159} < q < 2^{160}$, could be public.

③ $g = h^{(p-1)/q} \bmod p$, of which h is a integer, and satisfies $1 < h < (p-1)$, can be computed and be public.

④ The user's private key X, random integer or false random integer q which satisfies $0 < x < q$, is private.

⑤ The user's public key y, satisfying: $y = g^k \bmod p$.

⑥ k is random integer or false random integer, satisfying: $0 < k < q$.

When signing, computes:

$r = (g^k \bmod p) \bmod q$;

$s = [k^{-1}(H(M) + xr)] \bmod q$, getting the signature: (r, s) .

When testifying, computing:

$w = (s')^{-1} \bmod q$;

$u_1 = [H(M')w] \bmod q$;

$u_2 = (r')w \bmod q$;

$v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$;

Needing to verify: whether v is equal to r' , if then, the signature is valid.

M is the data which is to be signed: $H(M)$ produces the hash code of M using SHA-1,and M', r', s' is the actual data which receiver gets as M, r, s 。

B. Realization of Digital Signature Technology in E-commerce System

E-commerce is the abbreviation of Electronic Commerce, E-commerce means trade transaction online by the public network using TCP/IP technology. The appearance of E-commerce results the transformation from pen-text to E-text. For example, a computer system can deal with time and date by adding time stamp to a file automatically. Digital signature scheme is secure, because these schemes are based on encrypting technology usually and the security relies on the concrete algorithm. Common digital signature algorithm should assure that the signature is anti-deniable, anti-repeated and the message is impossible to be changed. The signature should resist all kinds of existing attack. The choice of digital signature algorithm and hash function relies on the following factors:

1) At present, there is not an effective cryptgraphy attack. The output of SHA is 160 bit hash value. It can resist end-seeking attack more effectively with contrast to other hash algorithm.

2) In digital signature algorithm, signning key is private, verifying key is public. Such mode is very suitable for official document circulation, such as official document sender can make signature with private key, however, official document receiver can verify the signature with public key. So, DSA should be adopted to realize digital signature. The secrecy is assured, at the same time the efficiency is increased. By the analyzing above, the realizing procession of digital signature can be described as following:

①The file sent is encrypted into abstract of 128bit;

②The sender encrypts the abstract S1 with his private key into signature F;

③ A random key K is produced, with which the message will be encrypted into P1;

④ The symmetric key K and digital signature F is encrypted with the receiver's pubic key into P2;

⑤P1 and P2 is sent to the receiver;

⑥The receiver disencrypt P2 with his private key into symmetric key K and digital signature F;

⑦F is disencrypted with the sender's publickey into abstract S1;

⑧P1 is disencrypted into original text with the symmetric key K;

⑨The recovered original text is encrypted into another abstract S2 using SHA;

⑩Comparing S1 to S2, if they are equal, the transferred message isn't damaged and distorted, vice versa.

IV. REALIZING DIGITAL SIGNATURE IN JAVA

Java has superiority in realizing digital signature [5]. We produce a digital signature for data using JAVA security API and prove its correctness [6].

The first job to make digital signature is to produce a key-pair. Key is produced in random integer generator. In Java, it is generated by class of KeyPairGenerator. In this case, a "DSA" key-pair with the length of 1024 bit is generated as following:

Step 1: programe structure

The digital methods are included in java. security software pack, so all content of the pack should be inputed. The software pack of java.io should be inputed too, because it includes the methods of inputing files.

```
Import java.io.*;
Import java.security.*;
```

Step2: generating public key and private key

Key-pair is generated by class of KeyPairGenerator. In this case, a "DSA" key-pair with the length of 1024 bit is generated as following:

1) create a key-pair generator

```
KeyPairGenerator
KeyGen=KeyPairGenerator.getInstance("DSA");
```

2) Initialize the key-pair generator

Using empty constructing function of Secure Random, a "seed" value needed by a random integer generator is generated:

```
KeyGen. initialize(1024, new SecureRandom());
```

Step 3: sign digital signature

After key-pair generating, the signature will be made. In this case, class of Signature is used to make signature, the signing steps:

1) Signature object(object). A signature object which is generated and verified with DSA algorithm can be produced as following:

```
Signature dsa=Signature.getInstance ("SHA/DSA");
```

2) initialize the signature object. Before being used in signing(or verifying), the signature object should be initialized first. A private key is needed in the initializing procession:

```
PrivateKey Priv=Priv.getprivate( );
Dsa.initSign(Priv);
```

3) Data being signed should be provided to signature object.In case of data in file,the data should be read once a word.

Step 4: Validate the signature

It needs three aspects to validate the signature: the date, the signature and the public key corresponding to the private key using in signature. There is an example for using Signature:

```
Signature dsa=Signature.getInstance("DSA");
```

1) First, you must initialize the signature objects in order to validate it.

This needs a public key to finish the initialization, which can be drawn from the private keys produced in step 2.

```
PublicKey pub=pair.getPublic( );
Dsa.initVerify(pub);
```

2) Offer the data which needs to be validated to the signature objects.

Just like what's done in signing, only one byte is read in document. The data is provided to signature objects by transferring. Just as step 3, the computing method is omitted.

3) Validate the signature

Whether the signature is ture or not can be validated once the signature objects are given.

```
Boolean verifies=dsa.verify(sig);
System.out.println("Signature verifies:"+verifies);
```

In this step, only primary computing methods are given and some innormal situations in executing and basic inputting and outputting sentences are not considered.

V. CONCLUSION

The public confidence is the key to E-Commerce building and using. It comes from the information safety and the valid protection to privacy, so information safety and privacy protection are most important problems in E-Commerce development in many countries.

The main aim of the text is to apply digital signature technology in E-Commerce system, advance the solution to the safety problems of digital signature technology in E-Commerce and offer identity certification to those who take part in E-Commerce activities, which prevents all kinds of potential safety hazards. The study and application of digital signature technology in China has a disparity with international level, so here we only talk about digital signature technology without security of the public key, and the safety of the public key will be investigated in future.

REFERENCES

[1] The Principle and Application of Internet Safety *by Shiyong Zhang* [M]. Beijing: Science Press, 2003.

[2] Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C]. Proc. of Advances in Cryptology-CRYPTO. 1999:431-448.

[3] Krawczyk H. Simple Forward-Secure Signatures from any Signature Scheme[C]. Proc. of the 7th ACM Conference on Computer and Communication Security. 2000-10: 1-4.

[4] 4 Malkin T, Micciancio D, Miner S. Effcient Generic Forward-secure Signatures with an Unbounded Number of Time Periods[C]. Proc. Of Advances in Cryptology-EUROCRYPT. 2002.

[5] J2EE Programme Guide *by Subrahmanyam Allamaraju (America), translated by Shuqi Ma* [M]. Beijing: Electronic Industry Press, 2002.

[6] Java Programming Base *by Shaofang Yang* [M]. Beijing: Science Press, 2001.