Digital Signature In The Application Of E-Commerce Security

Chen Tianhuang
School of Computer Science and Technology, Wuhan University of Technology
Wuhan, China
thchen@whut.edu.cn

Xu Xiaoguang
School of Computer Science and Technology, Wuhan University of Technology
Wuhan, China
xuxiaoguang1013@163.com

Abstract—**How we can ensure the security of data transmitted over the Internet and the identity of each trading party is the key to the development of e-commerce. The key problem of e-commerce is security problems. This paper focuses on digital signature technology in the application of e-commerce security issues, based on the core of a digital signature algorithm, which is a DSA algorithm idea. Combining specific business e-commerce applications, the paper simulates the actual situation, analyzes and solves problems, and put particular emphasis on the research of the algorithm and the improvement of DSA.**

Keywords- digital signature; e-commerce;DSA algorithm

I. INTRODUCTION

The rapid development of Internet makes e-commerce a new model for business activities. E-commerce includes management information systems MIS, electronic data interchange EDI, electronic ordering system EOS, commercial value-added network VAN, etc. in which EDI becomes the core. E-commerce, involves numerous aspects of the complex man-machine engineering. The openness of the network and sharing nature also result in the severely affected security of the network. In an open internet platform, traditional crime and immoral behavior in social life will become more subtle and difficult to control. People transact and operate from the face to face to on line which eliminates the need to meet each other as well the limit of border and time. Thus it produces a greater security risk. Therefore, the development of e-commerce boom, e-commerce security has become a major bottleneck restricting the development of e-commerce.

How we can ensure the security of data transmitted over the Internet and the identity of each trading party is the key to the development of e-commerce. It can be said that the most critical issue is the security issue; and Digital Signatures technology is an effective solution to ensure the confidentiality of information transmission, data exchange integrity, non-repudiation of sending messages, certainty of the identity of traders. It is an important part of e-commerce security [1].

II. DIGITAL SIGNATURE

A. Digital Signature

Digital Signature is to sign through some sort of cryptographic operations which generate a series of symbols and codes to make up the electronic password, instead of handwriting signature or seal. Technical verification can be used for this kind of electronic signatures. Digital signature on digital documents is similar to the handwritten signatures which are anti counterfeit. Receiver can verify the signature, and that the document is not revised after being signed, thus ensuring the authenticity of information and integrity. International standards organization of digital signature is defined as: additional data in the data on the unit, or some of data elements of this data or password transformation can be used to transform the recipient to confirm and integrity, and protect the sources of data to the forge. Digital signature as a password technique has the following functions and properties:

- Credibility. Signature receiver can verify the received signature is indeed a legitimate signer signed.
- Unforgeability. Only signer can generate his own signature.
- Non-reusable. Signature file contains the information not be used as the signatures of other documents.
- Non-repudiation. Signer cannot deny his signature at any time.

Digital signature is a combination of the hash function and encryption algorithms to achieve (the general use of non-symmetric encryption algorithm). It is usually a message digest is encrypted, and load the message back to confirm the identity of the sender and the integrity of the information [2].

Digital Signature Algorithm in general is composed of the signature algorithm and verification algorithm .Signature algorithm or signature is secret key, only signers master; Verification algorithm is public, to facilitate others to verify. Different from the Work with the message encryption, the signature of the message is not a one-time work that is a signature of the message may require multiple authentication signatures, and in a few years might still have to verify signatures. Therefore, the safety and security requirements of the signature will be higher, and verification faster than signature, especially when dealing with online verification, to require more high speed.

B. Digital Signature Based On Public Key Algorithm

As the symmetric encryption algorithm and asymmetric encryption algorithm can both obtain a digital signature, currently we are using more frequently encrypted signature technique, namely the asymmetric encryption algorithm.

978-1-4244-5517-1/10/$26.00 ©2010 IEEE

An asymmetric encryption algorithm for digital signatures is to use the user's private key to sign the message digest of a document and using the user's public key information for signature verification [3].
Signature and validation process is shown in figure 1, specific steps as follows:

a) A first process the message once with the public hash function, get the news summary, and then use their own private key to the summary for a digital signature, load the digital signature in the message and sent back together.

b) B use A's public key to decrypt the digital signature, to get a digital signature of plaintext M1. Sender is a trusted technical management body, (the certification bodies) released.

c) B calculate the receive message with the same hash function, then get a message digest M2, then compare the two message digest M1, M2 comparison, if the same, then prove that the signature is valid, otherwise invalid[4].

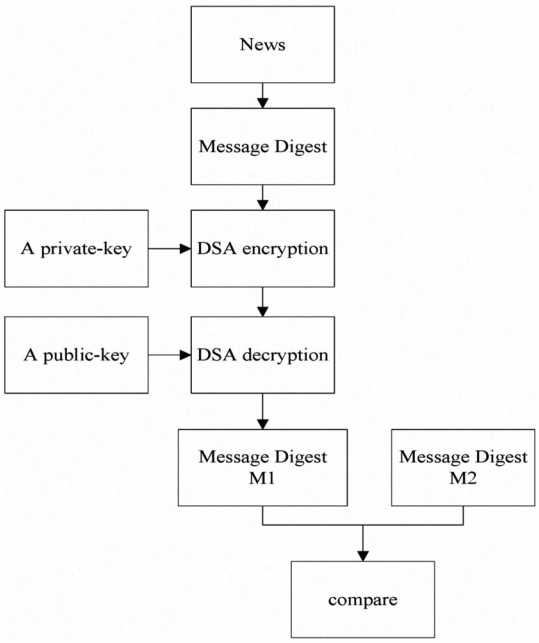

Figure 1. Diagram of the digital signature process

III. APPLING DIGITAL SIGNATURES TO IMPROVE E-COMMERCE SECURITY ISSUES

A. Examples of Digital Signature in the Agreement

Suppose there is a boss called Randy from company A as well as a boss called Victor from company B. Randy needs to transfer a file about the request for proposal, which is confidential. A boss Mars from company C is highly interested in the request for proposal of company A and B, and wants to get company A 's bid. He therefore frequently monitors their network communication in the hope of getting the bid when it is transferred through network. To prevent Mars from interception, how should we achieve secure communication?

B. Design Idea

We can use the following steps:

a) Randy uses file encryption with his private key to sign the document.

b) Randy sent the signed file to Victor.

c) Victor decrypts the file with Randy's public key to verify signatures.

This agreement can also meet our requirements:

a) Signature is authentic, when Victor use Randy's public key, he knows it's Randy's signature, rather than any other forged or tampered with.

b) Signatures cannot be forged, and only Randy knows his private key to decrypt.

c) Signature is not reusable. Signature is a function of the file, and cannot be converted into another document.

d) Signed document is unalterable. If there is any change in the file, it cannot be decrypted with Randy's public key authentication.

e) Signature is not to deny the fact. Victor will be able to verify the signature of Randy without asking Randy for help.

C. DSA digital signature algorithm used to solve the problem

1) DSA algorithm

DSA (Digital Signature Algorithm, as a part of the digital signature standard), which is another form of public key algorithm; it cannot be used as encryption, used only for digital signatures. DSA using the public key for recipient verification of data integrity and data the sender's identity. It can also be used by a third party to determine the signature and signed by the authenticity of the data [5].

Signature on the message M:

a) Sender generates a random number is Q that less than k.

b) Sender generates parameters R and S, while the R and S is the sender's signature, the sender will send them to the recipient.

c) The recipient to verify the signature by calculating: If V = R, then the signature is valid.

Description:

- Public parameters: P is 512-1024 primes; Q is 160 bits long, and with (P-1) coprime factor; G = powm (h, (P-1) / Q, P), where h is the less than the P-1 and to satisfy any number greater than 1.
- Private Key: X is less than the number of Q.
- Public key: Y = powm (G, X, P).
- Signature: k selected random number is less than Q, to calculate the R, S.
- Authentication: calculated V. If V = R, then the signature is verified.

- Sign convention: powm (x, y, z) that (x ^ y) mod z, namely (x of y-th power) mode z. "mod" for the sake of mold operator; "^" for power operator; below "*" for multiplication operator.

2) Analysis and design

According to the previous description, we have generated in realistic designing process a flow chart shown in Figure 2.

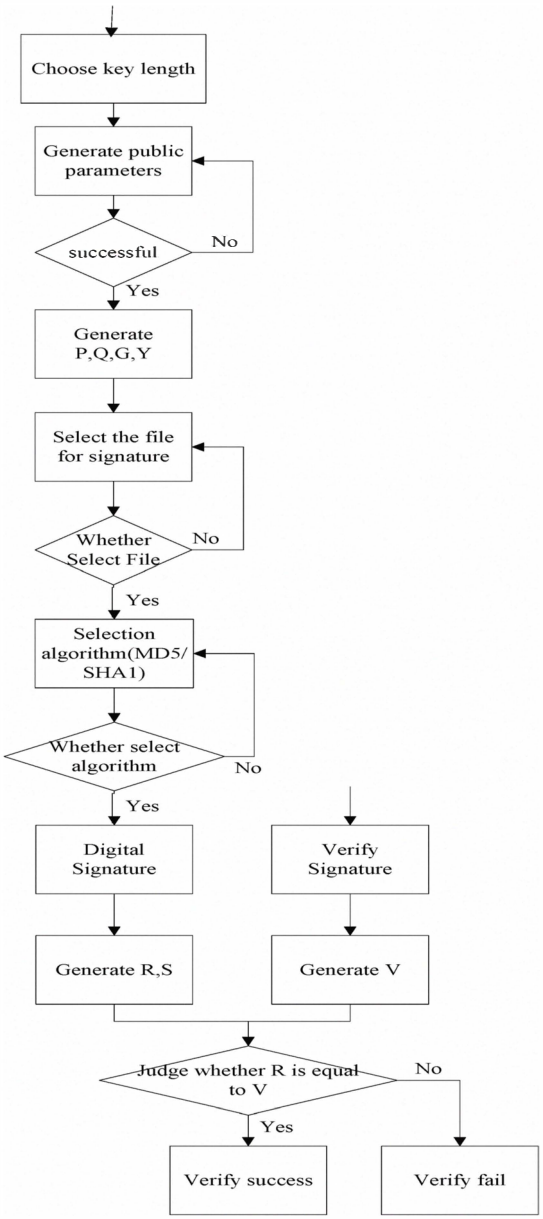

Figure 2. DSA Digital Signature Flowcharts

First, we need to select the key length according to our needs, and then generate the public parameters P, Q, G, Y (as previously mentioned a few parameters), and then select the file to be signed, select the MD5 algorithm to be used, or SHA1. After all these, digital signature is used to generate R, S and now signature is completed. The result is that the signature (R, S, M) is sent to your receiver (M for sending messages).

Authentication is that the recipient verifies the sender's signature (R, S, M) based on publicly available parameters P, Q, G, Y, theoretically gets the parameters of V. If R is equal to V, the signature is verified, otherwise the authentication fails.

3) Analysis of experimental results

a) Generate public parameters: as shown in Figure 3 to generate parameter P (128 * 4 = 512 of the large numbers), and expressed by 128-bit hexadecimal number, the parameter Q (40 * 4 = 160 bits large numbers) expressed by the 40-bit hexadecimal numbers, the parameter G (40 * 4 = 160 bits large numbers) expressed by the 40-bit hexadecimal numbers, the public key Y (128 * 4 = 512 bits large numbers) expressed by 128-bit 16 hexadecimal numbers. R indicates how many seconds it takes to generate the public parameters (Figure 3 shows 4 seconds).

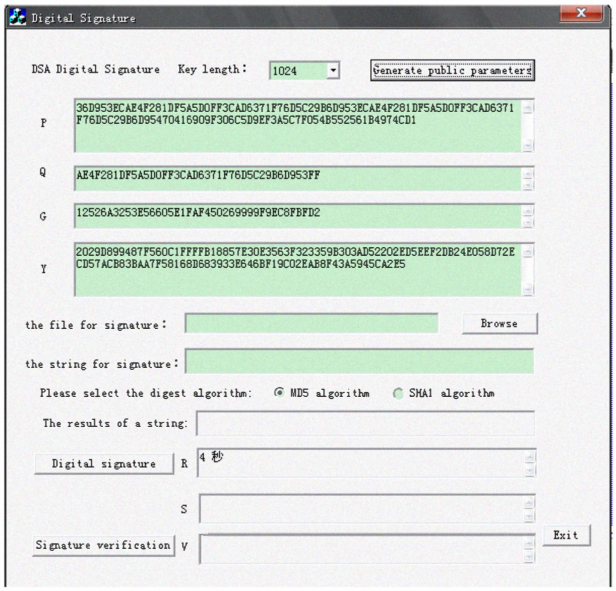

Figure 3. Figure of generated public parameters

b) Digital Signature: As shown in Figure 4, select the file, or a string for signature, then generate the summary of the results of the string, select the digest algorithm, digital signature after the completion of all, finally generated characters R, S. (R, S) shall be the results of the signature.

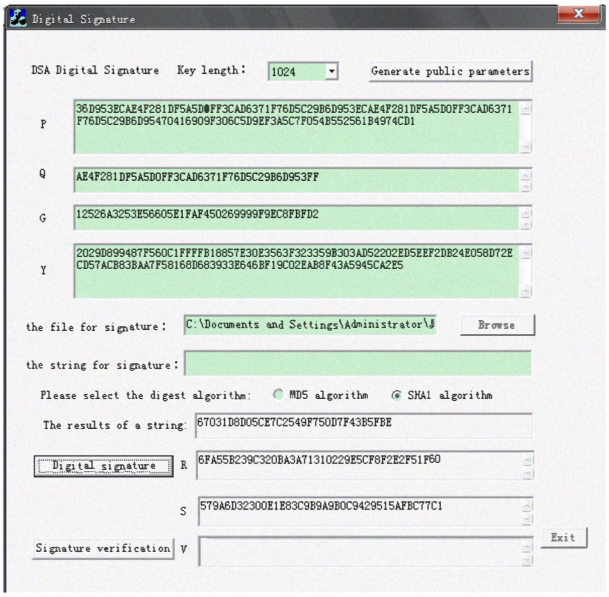

Figure 4. Simulation of digital signature effect

c) Signature verification: Figure 5 shows that when a signature is validated V is achieved by calculation. It can be observed that R is equal to V, which means that a certification numbers are signed.

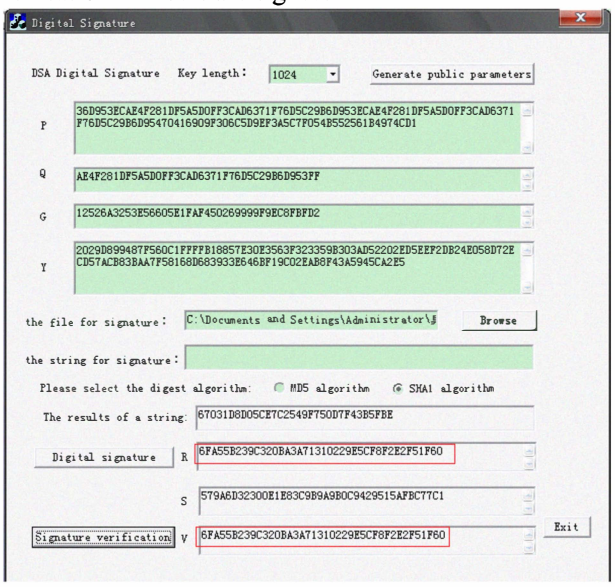

Figure 5. Simulation of Verified Digital Signature

Nevertheless, the experiment also reveals a few issues. First, public key algorithm is not efficient or convenient enough for long file encryption for which Hash function can be used instead. In the original document P, a one-way Hash function is used to generate a relatively short output of H, namely, Hash (P) = H, where P can be quickly generated by H while H is almost impossible to generate the P, then with public key algorithm acting on H generated "signature" S, denoted by Ek1 (H) = S, k1 for the A's public key, A sent (P, S) to B, B receive (P, S), then we need to verify that S is A's signature. If Hl = H2, which Dk2 (S) = Hash (P), then S is A's signature. Also, if we use a key Hash signature k, so that only people aware of key k can use hash, that is to use H (m, k) instead of H (m), we can enhance the security of cryptographic Hash, that is to use H (m, k) instead of H (m), we can enhance the Hash encryption security. The above method is actually transferring the signature process from the original file to very short hash values. This can greatly improve efficiency.

IV. CONCLUSION

The DSA algorithm adopted in this paper works well to solve problems of digital signatures based on simulation. This article discusses modern e-commerce security issues and the way to apply digital signature, a very powerful tool, to solve practical problems. Needless to say, there is much room for development for the digital signature in our country. Risks and crises are involved with security due to relatively late start of China's e-commerce, relatively backward development and the lack of security products with independent intellectual property rights. Therefore, it is necessary that we vigorously develop advanced information technologies with independent intellectual property rights and establish an integrated security system of information network. Digital signature technology needs further improvement and great efforts should be put to improve technology involved in the security of digital signatures. Undeniably, digital signature is the trend of the development of information security. Under such circumstances, it is essential to continuously improve the infrastructure of the digital signature environment and address the legal as well as technical issues in order to develop digital signatures.

REFERENCES

[1] The application of digital signatures. http://www.xici.net/b660239/d45154859.htm

[2] Zhang Xianhong.Principle and Technology of Digital Signature[M].Beijing: Machinery Industry Press, 2004 : 15-98

[3] Digital Signature Algorithm Analysis and Hash Signature. http://www.upsdn.net/html 2005, 10

[4] Lin KeZheng, Zhuang Qianyu.Combination of digital watermarking and digital signature authentication algorithm [J]. Chinese Academic Journal E-magazine, 2009:9-12

[5] Chen XiangLin. Digital signature technology and algorithm. Fujian PC, 2007, 6 : 58-59