Implememtation of Digital Signature in Authentication for E-Trading System

Thiri Lwin
anomalous.000@gmail.com

Abstract

Applications of digital signature technology are on the rise because of legal and technological developments, along with the strong market demand for secured transactions on the Internet. The internet based on the network are become essential tools in today. Also based on the network, communications for the business or trading become wide information society. So, information security is needed to cover the most of threads over the network. Information security means not only for storing and communication data in secrete but also for ensuring that the source of message is valid and the message has not been altered. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. The proposed system is intended to implement the Digital signature in Authentication for E-trading System by using DSA algorithm. This system also covers for confidentiality by applying RC5 algorithm. This system provides not only for security infrastructure for online e-trading system but also for digital signature products and online security, it is important to understand the application development trends in digital signature technology.

1. Introduction

Simple encryption and decryption can fix the message or data without understanding it and the receiver can't know receive message is the original message or not. One of the fundamental tools used in information security is the digital signature.

Although messages may often include information about the entity sending a message, that information mats not accurate. Digital signatures can be used to authenticate the source of messages, when ownership of a digital signature secrete key is bound to a specific user, a valid signature shows that the message was sent by that user. The important of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of the account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

The methods of encryption have been adopted for thousands of years as a mean for communication secrete messages from one location to another. Encryption is one of the cryptography technologies. Encryption is used at the very foundation of data storage and communication to protect the information, such that: Confidentiality, Data Integrity and Authentication of the data is ensured.

Digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of parameters and authenticates the integrity of the signed data and the identity of the signatory. An algorithm provides the capability to generate and verify signature. Signature generation makes use of private key to generate a digital signature. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user public key. Only the processor of the user private key can perform signature generation.

2. Related Works

Information security algorithms using DSA for signature generation and verification are applied in real world system such as electronic mail, electronic funds transfer, electronic data interchanges, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication.

The author Steve Burnett & Stephen Paine write about the digital signature and secure data encryption by using RSA and DSA algorithm in the RSA Security's Official Guide to Cryptography book. The author Jim Minihan research about digital signature by most useful signature algorithm DSA, RSA and ECDSA.

Dr. Burt Kaliski proposed timing attacks policy. The concept of timing attacks has been known for years, but Kocher's results are new and significant in that they can recover complete key information given only the running time of an operation, previous attacks could only recover partial key information or required timing information on the

individual steps within a cryptographic operation [2].

Brian Bladman, Carl Ellison and Nicholas Bohm proposed digital signatures, certificates and electronic commerce. It also turns out that digital certificates are more effective as mechanisms for attaching permissions to digital signatures instead of names or identities. And these properties in combination lead to uses of digital signatures, not as vehicles for identity, but rather as mechanisms that can represent the closed trust relationships on which commerce depends [1].

3. Cryptography

Cryptography is the science of writing in secrete is an ancient art; the first documented use of cryptography is writing dates back to 1900 BC, when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some expert argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunication, cryptography is necessary when communication over any entrusted medium, which includes just about any network, particularly the internet.

3.1 Digital Signature (DSA) Algorithm

When a message is received, the recipients may desire to verify that the message has not been altered in transit. Furthermore, the recipients may wish to be certain of the originator's identity. Both of these service can be provided by DSA.DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature.

3.1.1. Main processes of DSA

There are two main processes in DSA.-Signature Generation-Signature Verification Each signatory has a public and private key. The private is used in the signature generation process and public key is used in the signature verification process .For both signature generation and verification, the data which is referred to a message M, is reduced by means of Secure Hash Algorithm (SHA-1).

3.1.2. Signature Generation

Signature Generation – The signature of a message M is the pair of numbers r and s computed according to the equations. Variable r is generated mainly based on a user per message secrete number k .r= $(g^{k} \bmod p) \bmod q$ and variable s is generated mainly based on the private or secrete key x. s = $(k^{-1}$ (SHA-1(M)+ xr)) mod q.

3.1.3. Signature Verification

To verify the signature, the verifier first checks to see that 0<r<q and 0<s<q ,if either condition is violated the signature shall be rejected. If these conditions are satisfied, the verifier computes "v" as:

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

u1= ((SHA-1(M))w)mod q

u2= ((r) w)mod q

$v = (((g)^{u1}(y)^{u2}) \bmod p) \bmod q$.

Then verifier check that v is equal to r (one of the variable of signature) .If v=r, then signature is verified and the verifier can have high confidence that the received message was sent by the party holding the secrete key x corresponding to public key y.

3.2. Secure Hash Algorithm (SHA-1)

When a message of any length < 264 bits is input, the SHA-1 produces a 160-bits output called a message digest. Signing the message digest rather than the message the message often improves the efficiency of the process because of the message digest is usually smaller in size than the original message.SHA-1 is called secure because it is computationally infeasible to find a message which correspond to a given message digest.SHA-1 is a technical revision of SHA-0.A circular left shift operation has been added to the specifications and is based on principles of the MD4 message digest algorithm and is closely modeled after that algorithm.

3.2.1. Main Processes of SHA-1

There are two main processes in SHA-1, Message Padding and Computing the Message Digest.

3.2.2. Message Padding

The purpose of message padding is to make the total length of a padded message a multiple of 512. SHA-1 is used to compute a message digest for a message or data file that is provided as input. The message or data file should be considered to be a bit string. The length of the message is the number of bits in the message (the empty message has length 0). If the number of bits in a message is a multiple of 8, for compactness we can represent the message

in hex.SHA-1 sequentially processes blocks of 512 bits when computing the message digest. The following specifies how this padding shall be performed. As a summary, a "1" followed by m "0"s followed by a 64- bit integer are appended to the end of the message to produce a padded message of length 512 * n. The 64-bit integer is the length of the original message. The padded message is then processed by the SHA-1 as n 512-bit blocks.

3.2.3. Computing the Message Digest

The computation uses two buffers, each consisting of five 32 bit words, and a sequence of eighty 32 bit words. The words of the first 5-word buffers are labeled A, B, C, D, and E. The words of the second-5 word buffered are labeled H0, H1,H2, H3, H4 .The words of the 80-word sequence are labeled W0,W1,….,W79.A Single word buffer TEMP is also employed. In this case, in hex let MASK = 0000000F.

Before processing, the {Hi} are initialized as follows: in hex,

H0 = 67452301
H1 = EFCDAB89
H2 = 98BADCFE
H3 = 10325476
H4 = C3D2E1F0
a. Divide Mi into 16 words W [0]… W [15], where W[0] is the left-most word.
b. Let A=H0, B=H1, C=H2, D=H3, E=H4.
c. For t=0 to 79 do
s=t ^ MASK;
If (t>=16) W[s] = S1 (W [(s+13) ^MASK] XOR W [(s+8) AND MASK] XOR W [(s+2) ^ MASK] XOR W[s]);
TEMP=S5 (A) +f1 (B, C, D) +E+W[S] +K1;
E=D; D=C; C=S30 (B) =A; A=TEMP;
d. Let H0=H0+A, H1=H1+B, H2=H2+C, H3=H3+D, H4=H4+E.

3.3. RC5 Algorithm

RC5 is a fast block cipher designed to be suitable for both software and hardware implementation .It is a algorithm with a variable block size , a variable number of rounds ,and a variable-length secrete key .This provides the opportunity for great flexibility in both the performance and the level of security.

There are common reasons for applying a RC5 algorithm to the communications: to provide secure way for communication of sensitive data in Network and other media communication. Ensure for confidentiality that no one can read the message except the intended receiver.

3.3.1. Main Process of RC5

There are three main processes in RC5, Key expansion, encryption and decryption.

3.3.2. Key Expansion

Step 1: copy the secret key K[0,…,b-1] into an array L[0,..,c-1] of $c=\lceil b/u \rceil$words , where u=w/8 is the number of bytes/word .Step 2 : initialize array S to a particular fixed (key independent) pseudo-random bit pattern, using an arithmetic progression modulo 2 w determined by the "magic constants" P w and Q w.

P w = Odd ((- 2) 2w)
Q w = Odd ((- 1) 2w)
S[0] = P w ;
For i = 1 to t-1 do
S[i] = S[i-1] + Q w ;

Step 3: i = j = 0;A = B = 0;
do 3 * max (t , c) times:
A = S[i] = (S [i] + A + B) <<<3 ;
B = L[j] = (L [j] + A + B) <<< (A+B);
i = (i+1) mod (t);
j = (j+1) mod (c);

The key-expansion function has a certain amount of" one-wayness": it is not so easy to determined K from S.

3.3.3. Encryption

The input block is given in two w-bits registers A and B .Key Expansion has been already performed, so that the array S[0,..,t-1] has been computed. Here is the encryption algorithm in pseudo-code:

A = A + S[0];
B = B + S[1];
For i=1 to r do
A=((A⊕B)) <<< B) + S[2 * i];
B=((B⊕A)) <<< A) +S[2 * i + 1] ;
The output is in the register A and B.

3.3.4. Decryption

The decryption routine is easily derived from the encryption routine.

For i = r down to 1 do
B = ((B - S[2 * i + 1]) >>> A)⊕ A;
A = ((A - S[2 * i]) >>> B)⊕ B;
B = B - S[1];
A = A - S[0];

4. System Design and Implementation

The inputs of proposed system are all necessary information of category that are category name, price, quantity etc. and transaction types for e-trading system. The proposed system is composed of

two main processes (1) encryption and signature generation process (2) signature verification and decryption process.

The proposed system design is implemented on e-Trading system. The proposed system includes two branches and one head office. This system is intended to hide information from access by unauthorized parties, while it is being transferred, which is when it is digital signature. The digital signature can show whether the document was truly signed by the purposed author, and it can also provide 'non-repudiation 'of transmitted information. This system also uses encryption to provide secure way for communication of sensitive data in Network.

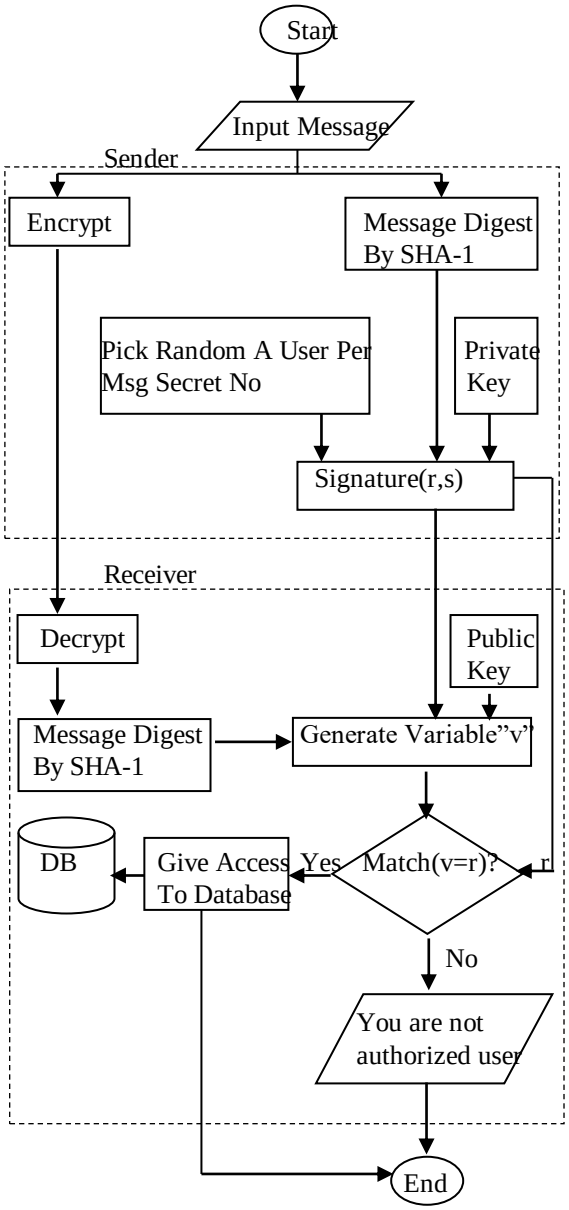


Figure 1. System Design

4.1. Encryption and Signature Generation

This process generate signature for input messages by means of DSA algorithm signature generated equation.DSA use SHA-1 hashing algorithm to improves the efficiency and to be computationally infeasible to find a original input messages at signature generation and verification .The original input message become 160 bits output called a message digest.

The signature of a message M is the pair of r and s computed according to the equations below:

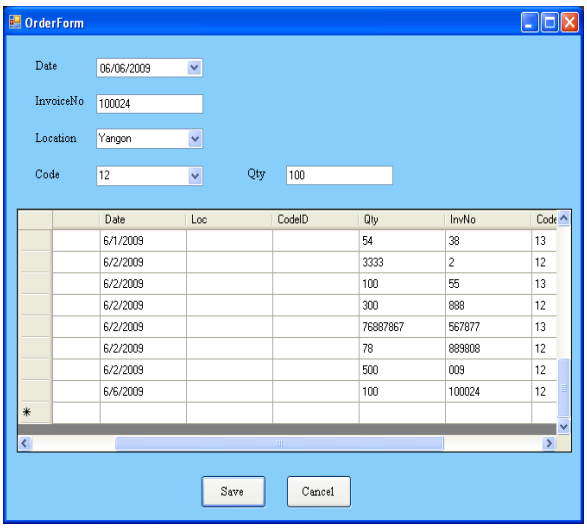
$$r = (g^{k} \bmod p) \bmod q$$

$$s = (k^{-1}(\text{SHA-1}(M) + xr)) \bmod q$$

r is generated mainly based on a use per message secrete number k and s is generated mainly based on the private or secrete key x. The private key x is a randomly generated integer with $0<x<q$. Variable q is a prime divisor of p-1, where $159<q<160$. Variable p is L bits prime modulus, where $512 <= L <= 1024$. The public key $y = g^{x} \bmod p$ is also generated for the verification case.

In our proposed system also encrypt the original input message by RC5 algorithm for communication of sensitive data in network and ensuring for confidentiality that no one can read the message except the intended receiver. The Figure 2 shows the signature generation and message encryption form in the system.

When the user request order, it is needed to fill all necessary information for order to head office. From this order request by the import/export data, the system generates signature and encrypt the original message by export function and then send this signature and encrypted message to head office. The export form is shown in Figure 3.



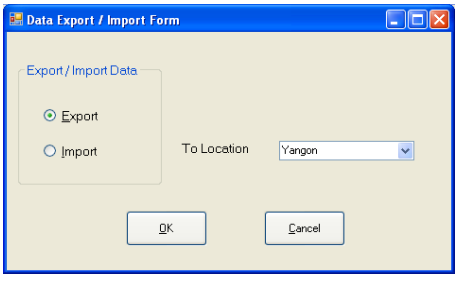


Figure 2. Order Form Entry

Figure 3. Generate Signature and Message Encryption

4.2. Signature Verification and Decryption

At the head office (receiver site), the system decrypt the cipher text by means of RC5 algorithm. After decrypt by RC5 the message becomes original message.

The decrypted message is verified by DSA signature verification equation.

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

$u1 = ((SHA\text{-}1(M))w) \bmod q$

$u2 = ((r)\ w\ ) \bmod q$

$v = (((g)^{u1}(y)^{u2}) \bmod p) \bmod q$.

Then verifier checks that v is equal to variable r that is one variable of signature sent from sender.

If the original message has not been altered, then the message is shown as Figure 5.This message has the integrity that the sender and receiver of a message may have a need for confidence that the message has not been altered in transit.

If the attacker takes the transactions of message when we send it .Then generate signature in their own way and send signed object again. When head office imports the transactions of the message by import/export data then the signature can't be validate and alert the message as shown in Figure 6.

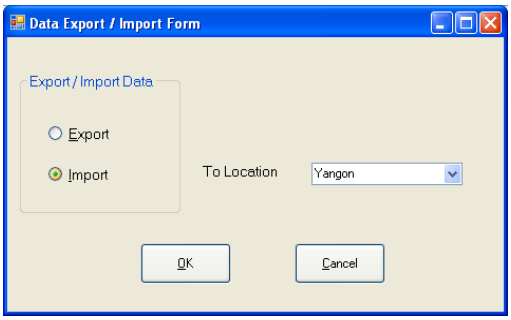


Figure 4. Message Decryption and Verify Signature

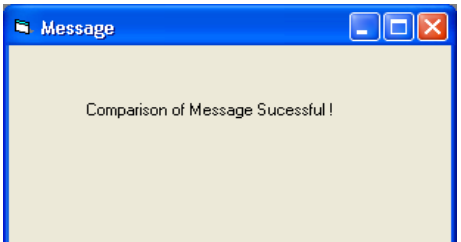


Figure 5. Message Alert for Verified Transactions

Figure 6. Message Alert for Unauthorized User

5. Conclusion

This paper is used to implement digital signature in authentication for e-Trading system by DSA. When a message is received, the recipients may desire to verify that the message has not been altered in transmit. Furthermore, the recipients may wish to be certain of the originator's identity. Both of these services can be provided by DSA.RC5 ensure for confidentiality that no one can read the message except the intended receiver. So, this system can provide not only for high confidence in sender authenticity, message integrity and confidentiality but also for security infrastructure for online e-trading system.

6. References

[1] Brian Gladman, Carl Ellison and Nicholas Bohm, "Digital Signatures, Certificates and Electronic Commerce" version 1,1, June 8, 1999.

[2] Burt Kaliski, "Timing Attacks on Cryptosystems", Volume 2, Journal , January 23, 1996.

[3] Jim Minihan , “Understanding Digital Signature And Public Key Infrastructure ”,Whitepaper
https://www.do.ks.gov/PKI/digsigwhitepapre.doc

[4] S.Kaliski jr, Burton and Yin, Yigun Lisa , “On the Secutiry of the RC5 Encryption Alogirthm”,Version 1.0,1998

[5] L.Leiss,Ernst , “Principle of Data Security” ,ISBN 0-306-41998-2, 1982

[6] National Institutes of Standards and Technology (NIST), ”Digital Signature Standard, FIPS PUB 186-1”.
https://csrc.nist.gov/publications/fips/fips 186-1/fips 186-1.pdf

[7] National Institute of Standards and Technology (NIST), “Secure Hash Standard, FIPS PUB 180-1”.
www.itl.nist.gov/fips pubs/fips 180-1.htm

[8] L.Rivest,Ronald, ”The RC5 Encryption Algorithm”, MIT Laboratory For Computer Science 545 Technology Square, Cambridge , Mass.02139, December 1994

[9] W. Stallings, “Cryptography and Network Security principles and practices” , fourth Edition.

[10] Santa Clara, CA 95054, “An Introduction to Cryptography”