Reliable Office Communication Using RSA and SHA-1

San Kyaw Zaw, Khin Kyu Kyu, May Phyo Oo
Computer University (Pathein)
whitetulip2020@gmail.com, khinkyu28@gmail.com, mayphyooo@gmail.com

Abstract

In data and telecommunication, cryptography is necessary when communicating over untrusted medium. With the development of network and software technology, digital signature becomes more and more important for the e-communication .The data transferred on e-communication system must have the characteristic of anti-deniability, integrity and confidentiality. In cryptography, RSA is widely used algorithm for the public key cryptography. The SHA hash functions are a set of cryptographic secure hash functions .This paper proposes a reliable office communication based on RSA and SHA-1. This system is implemented by C#.Net programming language.

1. Introduction

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt the encrypted data. This method is known as symmetric key cryptography [3]. Asymmetric cryptography uses different keys for encryption and decryption. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption [9]. These keys are labeled or known as a public and a private key; in this instance the private key cannot be derived from the public key [1]. In cryptography, RSA is an algorithm for the public key cryptography. RSA is widely used in e-communication and is believed to be secure given sufficiently long keys and the use of up-to-date implementations [5]. The SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology, NIST [5]. SHA stands for Secure Hash Algorithm. The three SHA Algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. The SHA-2 family uses an identical algorithm with a variable digest size which is distinguished as SHA-224, SHA-256, SHA-384, and SHA-512. SHA-1 is the best established of the existing SHA hash functions, and is employed in several widely used security applications and protocols. A cryptographically strong hash must be non reversible, meaning that by looking at the hash result there is no way to derive any part of the original message. It must also change significantly with any small change, even a single bit, in the input message. This is called the avalanche effect [1]. The hash should also be collision-resistant, meaning that it is impractical to find two messages with the same hash. A hash with these properties can be used as digital signature in this system.

This paper is organized as follows: In section 2, related works and problem issues about security requirements of communication in current day are described. The background theories of this proposed system are explained in section 3. In section 4, the overview of system is explained. Then, the implementation of reliable office communication system is described in section 5. Finally, this paper concludes with the benefits of proposed system.

2. Related Works and Problem Issues

Today, most of users use mail not only for private communication but also for office communication. Using mail account, users can protect their data with user name and password. However, users can face some problem due to masquerading attackers. Hence their secret data can be theft. Moreover their important data can be edited by tampering attacker. So, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity.

• Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

• Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

• Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions [7].In this system, using RSA only can provides the message confidentiality. Combining SHA-1 properties and RSA encryption can solve the needs of anti-deniability. This system uses RSA algorithms (PKCS) and SHA-1 for reliable communication in office use. In fact, the purpose of using RSA and SHA-1 plays a vital role for office communication.

3. RSA algorithms

The RSA algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir, Leonard Adleman at "Massachusetts Institute of Technology" MIT; the letters RSA are the initials of their surnames [4]. The RSA algorithm involves three steps: key generation, encryption and decryption. RSA involves a public key and a private key. RSA typically uses keys of size 1024 to 2048 [5][10]. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n [3][11]. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is 2^k bits, where $2^k < n <= 2^{k+1}$. Encryption and Decryption are of the following form, for some plain text M and cipher text $C = M^e \bmod n$; $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$.

Both the sender and the receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public key encryption algorithm [11]. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret [1].The keys for the RSA algorithm are generated by the following ways [2]:

1. Choose two large prime numbers p, q such that p is not equal to q, randomly and independently of each other.
2. Compute n = p * q
3. Compute the quotient Ø (n) = (p-1) (q-1)
4. Choose an integer e such that 1< e <Ø (n) which is co prime to Ø (n)
5. Compute d such that de = 1 (mod Ø (n))

Public key PU = { e , n }
Private key PR = {d , n }

Encryption: $C = M^e \bmod n$.
Decryption: $M = C^d \bmod n$.

3.1. A Simple Example of RSA Algorithms

Suppose M=88
Select two prime numbers; p=17 and q=11, and so n=p*q=187
Calculate Ø (n) = (p-1)*(q-1) =16*10 =160 and then Choose e=7
Determine d such that de=1(mod 160) and d<160, so d=23 because 23*7 =161= 1*160+1
Public key PU = {7,187}
Private key PR = {23,187}
Encryption: Cipher text $C=88^7 \bmod 187 = 11$
Decryption: Plaintext $M=11^{23} \bmod 187 = 88$

3.2. Hash Algorithm

Hash algorithm is an algorithm which is used to compute a data fingerprint of a data block [7]. 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. cannot 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 [8]. The popular hash algorithms are MD5, Secure Hash Algorithm (SHA, having all kinds of security level.) and so on. In this paper SHA-1 is support for sender's signature.

3.2.1 SHA-1. The Secure Hash Algorithm SHA is a family of cryptographic hash functions designed by the NSA and published as a U.S. government standard [NIST, 1994]. The first version published in 1993 is often referred to as SHA-0. SHA-l is the most commonly used hash function in the family of application protocols including the Transport Layer Security (TLS), Secure Socket Layer (SSL), Pretty

Good Privacy (PGP), Secure Shell (SSH), and the Internet Protocol Security (IPSec) [5].When a message of any length < 2^{64} bits is input, the SHA-1 produces a 160-bit output called a message digest [7][8].

3.2.2 .Example of SHA-1 Digest. The following is an example of SHA-1 digests. ASCII encoding is assumed for all messages.

SHA-1 ("The quick brown fox jumps over the lazy dog") = 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

Even a small change in the message will, with overwhelming probability, result in a completely different hash due to the avalanche effect. For example, changing dog to cog:

SHA-1 ("The quick brown fox jumps over the lazy cog") = de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

The hash of the zero-length message is:

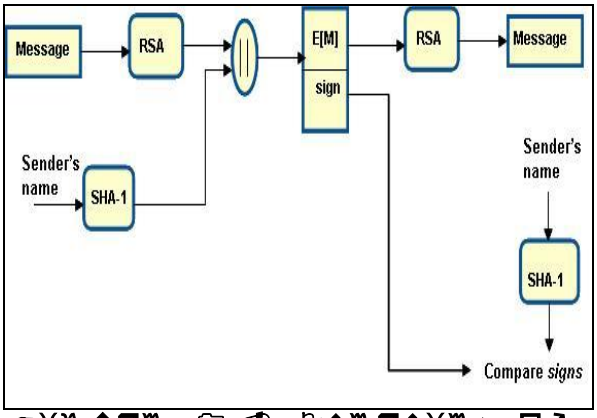
SHA-1 ("") = da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709

SHA-1 can process messages with the maximum length up to(2^{64}-1) bits, have a message block size of 512 bits, and have internal structure based on processing 32-bit words [8][9].

4. Overview of System

The Sender generates a message (M) and encrypts that original message with RSA algorithms by using the recipient's public key to produce an encrypted message. The sender's name is feed into the SHA-1 algorithms and generate 160 bit message digest, sender's signature. The Sender concatenates his signature and an encrypted message E [M] and sends to the recipient through the internet.

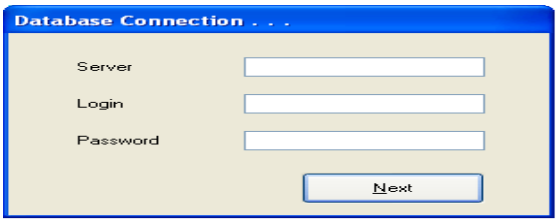
At the Receiver Site, the receiver decrypts the encrypted message "Cipher text" by using receiver's private key to reproduce the original message. And generate a 160 -bit message digest, sender's sign, by using SHA-1 on the sender's name. The Receiver compares these two message digest or signs. If signs are equal, then the signature is verified. In this ways; this system provides complete confidence between participants.



5. Implementation of the system

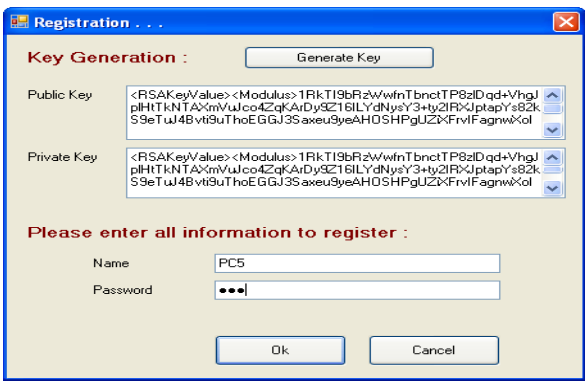
Implementation of the system is described as follows:

According to the figure 2, to enter the system, the user must connect to the server firstly.



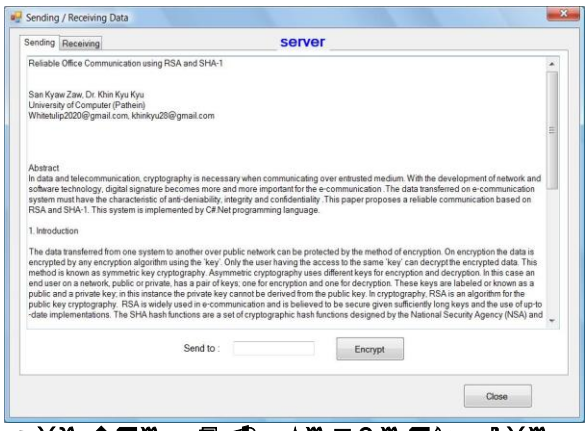
After connecting to server; he must fill the user login form for authorized access in the system. If his login is success; he can start the communication with other participants within the system. If the new one want to join and communicate with system for the first time; he must register to the system by the following process as shown in figure 3.

1. Generate his key pair (private and public) by key generator for the encryption and decryption.
2. Choose his name and password for login to the system.

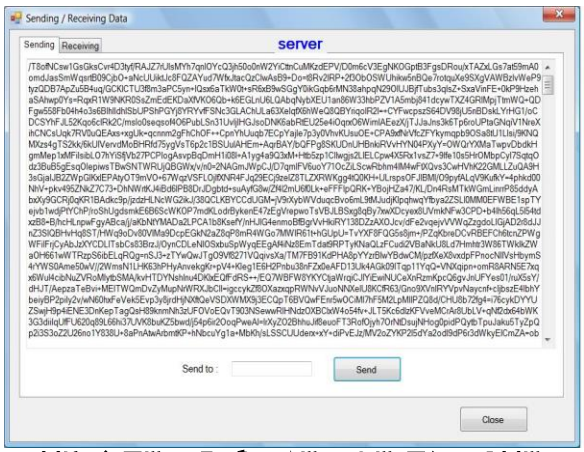


If the register is successful, he becomes the one of members and can communicate with others in this system .The system's key store saves the keys pairs and accounts of all users for control this communication.

5.1. Sender Site

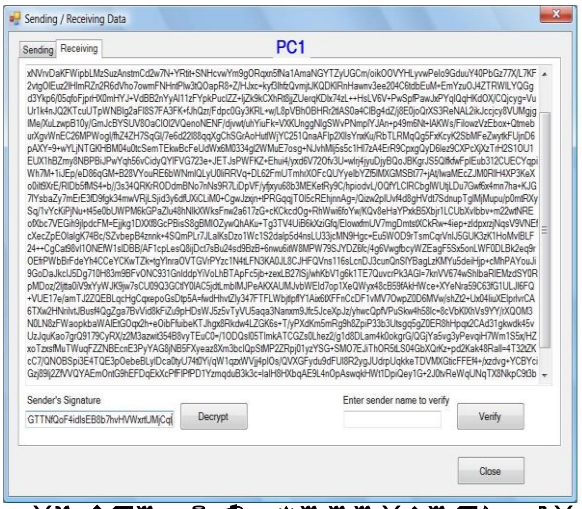


The sender's view can be seen in figure 4 and 5.The sender generates a message (M) and encrypts it. Then send to the intended recipient. The sending function involves 3 steps; one _ produces the 160-bit hash value or sign by SHA-1 on sender's log-in name, second_ concatenates this signature and "Cipher text" and three_ send to the receiver through the internet.



5.1.1. Sending order or announcement. When the head office sends the announcement or public order to all branch office, he uses the global encryption key to produce the "Cipher text". At the receiver site, all branch office, uses the global decryption key for recover the original message from the received "Cipher text".

5.2. Receiver Site



According to figure 6, the receiver decrypts this "Cipher text" by using his private key to reproduce the original message. And to verify the received sign; generate a 160 -bit message digest by using SHA-1 on the sender's name. The Receiver compares these two message digest or signs. If signs are equal, then the signature is valid.

6. Conclusion

A reliable office communication system has been implemented using RSA, SHA-1 and C#.Net programming language. This system provides the message communication to reliable by confidentiality, integrity and digital signature. A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The use of RSA and SHA-1 provide complete confidence between participants.

7. References

[1] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth) ", *John Wiley & Sons, Inc* .ISBN: 0471128457 Publication Date: 01/01/96

[2] C. Narasimham, J. Pradhan, "Evaluation of Performance Characteristics of Cryptosystem using Text Files"

[3] Anoop MS, "Public Key Cryptography, Applications algorithms and Mathematical Explanations", Tata Elxis Ltd, India

[4] B. Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem ",RSA Laboratories

[5] A.G. Konheim, "Computer Security and Cryptography", A John Wiley & Sons, INC., 2007

[6] Madrid, "Classic Cryptosystem", March, the first,2005

[7] A. Kaur, A. Verma , "Cryptography and its hash function's security" , U.I.E.T Panjab University, Chandigarh

[8] C.D. Canni`ere and C. Rechberger , "Finding SHA-1 Characteristics: General Results and Applications", Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Inffeldgasse 16a , A–8010 Graz, Austria

[9] S. Pongyupinpanich and S. Choomchuay , "An Architecture for a SHA-1 Applied for DSA", King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok 10520, Thailand

[10] N. Daswani, C. Kern, and A.Kesavan, "Foundations of Security ", Springer-Verlag New York, Inc.

[11] F.L. Bauer, "Decrypted Secrets ,Methods and Maxims of Cryptology ",Springer-Verlag Berlin Heidelberg, 1997-2007