News Media System Using RSA Algorithm

Aye Aye Khaing, Khin Thet Mar
Computer University, Maubin
ayeayekhaing046@gmail.com, moenaychikhin@gmail.com

Abstract

In data communication, cryptography is necessary when communication over insecure channel. In many business sectors, secure and efficient data transfer is essential. Cryptography provides the basics for authentication of messages as well as their security and integrity. To ensure the security to the applications of business, the business sectors use Public Key Cryptographic system. In cryptography, RSA is the most widely used public key cryptographic systems. Public Key Cryptography can be used for confidentiality and authentication. Digital signature can be used for message authentication and non-repudiation. To secure news media, this paper proposes the combination of public key cryptography (RSA) algorithm and secures hash algorithm (SHA-1).

1. Introduction

Data communication is an important aspect of our living. Therefore, to transmit new media from one site to other, protection of data from misues is essential. Media uses to store and deliver news information or data to the public (people).To secure news media, asymmetric cryptographic algorithm (also called public key algorithm) enables secure transmission of information. Cryptographic techniques are extremely critical to the development and use of defence information system and communication networks. In distributed environment, encryption is needed for authentication and guarding the secrecy of data in transit.

There are different types of encryption algorithms used to protect sensitive data including; symmetric and asymmetric encryption techniques. Symmetric encryption uses the same key for encryption and decryption. Asymmetric encryption also called public key algorithms uses a pair of related keys one for encryption and other for decryption [1]. Public key algorithm is a method for secret communication between two parties without requiring an initial exchange of secret keys [4]. Asymmetric cipher permits the encryption key to be public, allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. RSA (Rivest, Shamir and Adleman) is the most popular public key algorithm. Another type of applications in public-key cryptography is digital signature schemes [9].

Digital signature schemes can be used for sender authentication and non-repudiation. Authentication allows someone in the electronic world to confirm data and identities, and non-repudiation prevents people from going back on their electronic world. In this paper, secure News media system has been implemented with reporter site and media site by using public key authentication, RSA algorithm and secure Hash Algorithm (SHA-1) to secure the data and network of news media. This paper is organized as follows. Section 2 describes the related work. Section 3 explains background theory. Section 4 presents the system overview. Section 5 discusses the implementation of the system. Section 6 describes the experimental results. Finally, the last section is conclusion.

2. Related work

Roman Novak [10] implemented on the card used for secure Internet banking. Several weaknesses had been discovered, the sub-channel information leakage being the largest. Protection of the user's PC was still required because the SSL session keys were handled by the system and the implementations of the interfaces enable an ad-versary to gather security-related data about the card in the man-in-the-middle type of attack. Mr.P.Balakumar [7] developed under Graphical User Interface environment which was very easy to operate by the users. This system was developed using the Java language so that it could be executed on any platform. The design of this system supports both the Internet and Intranet environments. The System was developed to provide security for the file transfer process in distributed environment. So the system should ensure the security of the documents that were transferred. E.Inzunza-González [4] presented the development of software to encrypt messages with the RSA algorithm. This

system could be used in universities and research centres as a tool for studying public-key cryptography. The system was friendly and easy to operate for users. In this paper, the secure news media are transmitted from one site to another. News media security is needed to protect message during their transmission. We use RSA algorithm and SHA - 1 algorithm for new media security.

3. Background Theory

In this section, RSA public key cryptosystem, RSA algorithm and Secure Hash algorithm are presented as background theory.

3.1 RSA Public-Key Cryptosystem

Public- key cryptography is a fundamental and widely used technology around the world, and enables secure transmission of information on the internet and other communication systems [4]. In 1977 Rivest, Shamir and Aldeman invented the RSA algorithm for encryption and digital signatures which was the first public-key cryptosystem [3]. Public-key cryptography is a method for secret communication between two parties without requiring an initial exchange of secret keys. In public-key cryptography, the user generates different public keys from two prime numbers, and then selects a public-key to generate the corresponding private-key. The user uses a public key to encrypt the message and a private key to decrypt. The private-key is kept secret and the public key is distributed at will [8].

3.2 RSA Algorithm

The Rivest, Shamir, Adelman (RSA) scheme is a block cipher asymmetric cryptosystem, in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits. In RSA system all the users must generate their private key KR= {d, n} and kept it in secret and store their public key KU= {e, n} in Key Distribution Centre (KDC). The sender receives the receiver's public key from the KDC and encrypts the message using the receiver's public key. The receiver uses his private key to decrypt the coded message. The private key is known only to the receiver himself.

3.2.1 RSA Key generation

Key generation is the most important part of RSA; it is also the hardest part of RSA to implement correctly. A RSA public and private key pair can be generated using the algorithm below:

1. Choose two large random primes number p and *q*, *p* is not equal *q*
2. Compute n = *p*q*
3. Compute the quotient Ø (n) = (p-1) (q-1)
4. Choose a random encryption exponent e, e and Ø (n) are relative prime,1< e <Ø (n)
5. Derive the decryption exponent *d*, *ed =1 mod* Ø (n)

Public key: *K= (e, n)* the pair of e and n
Private key: *K = (d, n)*

3.2.2 RSA encryption and decryption

Suppose that person *A* wants to establish a secure communication with person *B* by using the RSA algorithm. Person *A* determines the numbers *n*, *e* and *d* . A pair of number (*e*, *n*) is publicly available (it is called "public key" and serves to person *B* for encrypted messages intended to person *A* or to verify digital signatures of messages sent by person *A*. Encryption**;** To encrypt the message *m*, the sender *B* uses public key exponent *e* by the following formula:

$$c = m^e \bmod n \quad \ldots\ldots \quad (1)$$

A pair (*d, n*) is called "private key" and it is only known by person *B* and serves for decryption or digital signing of the messages [6].
Decryption**;** To decrypt the cipher text *c*, the receiver *A* uses private key exponent *d* by the following formula:

$$m = c^d \bmod n \quad \ldots\ldots \quad (2)$$

3.2.3 Signature and Verification

RSA signature is one of digital signature types created by using RSA algorithm. Sender applies has function to the message or file to produce a message with fixed length. Then, sender signs the message or file by using RSA algorithm to produce the signature. The process of signing uses the equation as follow:

Signature; $S = m^d \bmod n \quad \ldots\ldots \quad (3)$

To verify the signature,

The sender sends this signature to the recipient. Receiver uses sender's public key to decrypt the signature as the following equation:

Verification; $V = s^e \bmod n \quad \ldots\ldots \quad (4)$

3.3 Secure Hash Algorithm

Hash functions are the primary mechanism to provide information integrity services. A hash function takes a message of arbitrary length and creates a message digest of fixed length. Families of well-known hash function are MD2, MD5 and SHA. MD2, MD4 and MD5 are MD stands for Message Digest. The Secure Hash Algorithm (SHA) is a standard that was developed by the National Institute of Standards and Technology (NIST). The SHA

family consists of SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. SHA-1 algorithm is secure because it is computationally infeasible to find a message which corresponds to a given digest [5]. The SHA algorithm is used by both the transmitter and intended receiver of a message in computing and verifying a digital signature. Any change to the message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA algorithm can be described in two stages: preprocessing and hash computation. Preprocessing involves padding a message and the purpose of message padding is to make the total length of a padded message a multiple of 512.The SHA-1 sequentially process block of 512 bits when computing the message digest. The hash computation generates a message schedule from the padded message. The final hash value generated by the hash computation is used to determine the message digest. This property is used in the creation and verification of digital signatures and message authentication codes.

4. Overview of the System

In this system, all of two (reporter, media) site generate the public and private key pairs by using RSA key generation algorithm and send public key to other site.

At the Reporter site, the reporter generates a message (M) and encrypts that original message with RSA algorithms by using the media's public key to produce an encrypted message. The reporter produces 64-bits message digest by using SHA-1 algorithms on that original message. The message digest is digitally signed by using the reporter's private key to produce a signature. The reporter concatenates a signature and an encrypted message and sends to the media through the internet. Reporter process is shown in Figure 1.

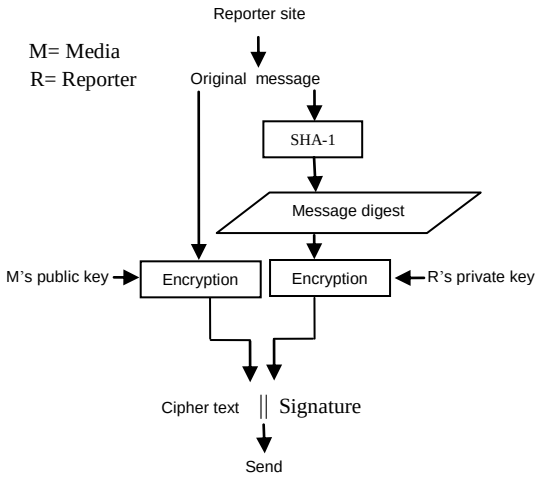

Figure 1. Reporter's Encryption process

At the Media Site, the media decrypts the encrypted message "Cipher text" by using media's private key to reproduce the original message and generate a 64 -bit message digest by using SHA-1.The media decrypts the signature with the reporter's public key. Then The Media verify these two messages digest. If the two messages digest are the same, verification complete and the message is accepted. In this ways; this system provides complete confidence between participants. That process is shown in Figure 2.

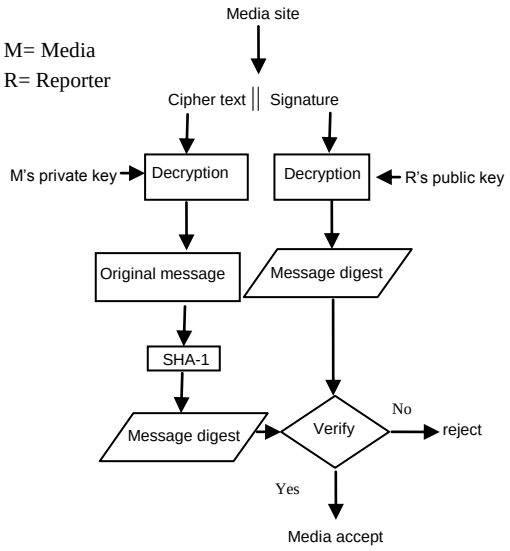

Figure 2. Media's decryption process

5. Implementation of the System

This paper has implemented the secure news media system to prevent information or data from access by unauthorized parties, while it is being transmitted. The system uses a 1024-bit of RSA key and secures hash algorithm (SHA-1) implementation, which is sufficient for news media system.

5.1. Reporter site

To connect the reporter to the media server, the reporter must fill the user login form for authorized access in the system. If his/her login is success; the reporter can start the communication with other participants within the system. For the first time, the new reporter must register with his/her name and password for login to the system.

If the register is successful, the reporter becomes the one of members and generates his/her key pair (private and public) by key generator for the encryption and decryption. And then the reporter's public key sends to the media and receives Media's public key. After the key generation and sending have finished, the reporter creates a message (M) and

encrypts it. The reporter produces the signature and the encrypt message when this message is encrypted finished. Then the reporter concatenates this signature and encrypted message and send to the media site through the internet. Reporter site's sending form is shown in Figure 3.

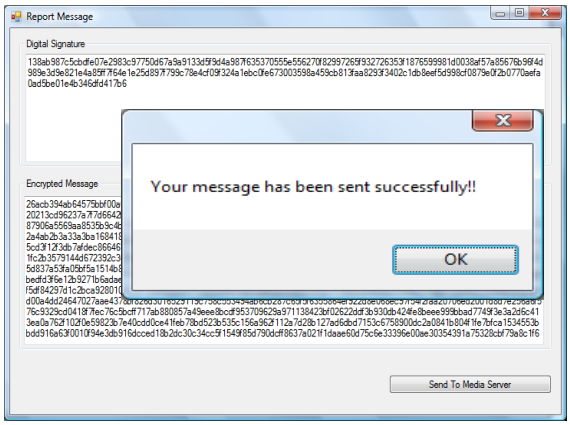

Figure 3. Reporter's signature and encrypted message sending form

5.2 Media site

The Media has received the message which contains cipher text and signature. After the media decrypts the cipher text and signature, produce two message digest. Then the Media verify these two messages digest. If two message digest are the same, the system is successful. This process is shown in Figure 4.

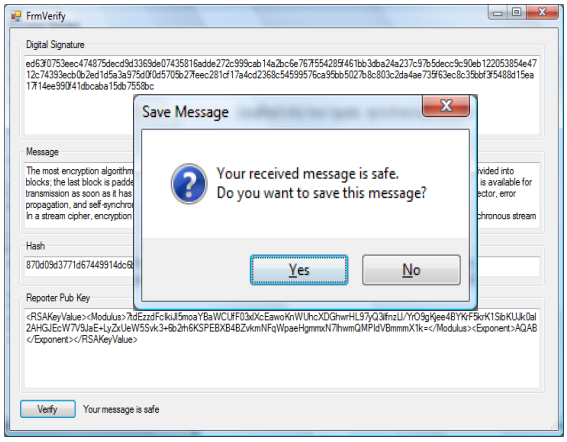

Figure 4. Media's verify form

6. Experimental Results

In this section are presented encryption time and decryption time of various types of input message. Any change to a input message in transit will, result is a different time. This system is tested with various types of input message. This paper is implemented using C#.Net programming language and the execution of the developed tool on a personal computer equipped with an Intel ® core™ 2 Duo 2.00 GHz CPU , 2G RAM. Window XP operating system.

In this Figure 5 shown in runtime of encryption at various file size.

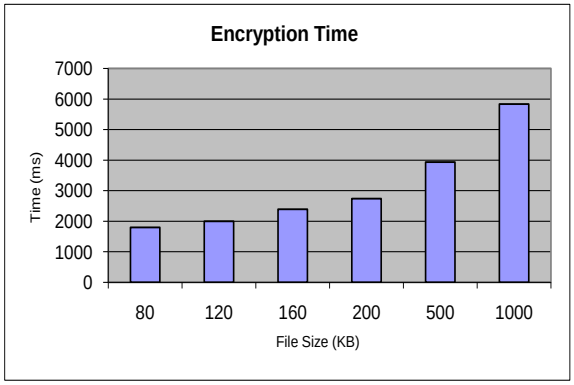

Figure 5. Encryption time of various file size

Decryption time is longer than the encryption time in the same file size. In this Figure 6 shown in runtime of decryption at various cipher size.

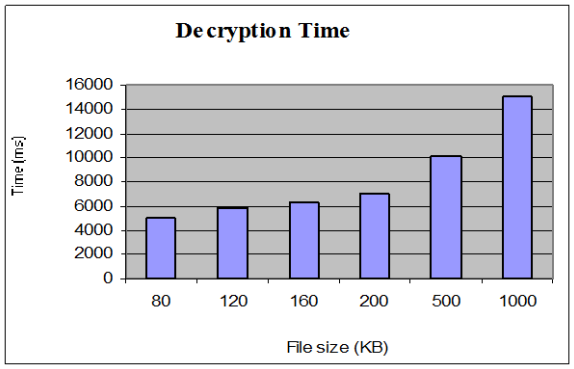

Figure 6. Decryption time of various cipher size

7. Conclusion

The secure news media system has been implemented using RSA algorithm and secure hash algorithm (SHA-1). SHA-1 is used for computing the hash value of the message. RSA is used for signing and verifying the signature. The private key of RSA is used for encrypting the hashed message. The public key of RSA is used for decrypting the signature to recover the hash value of the message. This system provides the message communication to secure by confidentiality, integrity and digital signature with two parties. The digital signature and hashing provides message integrity, non-repudiation and authentication for the reporter and media. The secure new media system supports protecting news

media for reporter and media by using RSA digital signature and SHA-1.

References

[1] Anoop MS, "Public Key Cryptography, Applications Media's verify form algorithms and Mathematical Explanations", Tata Elxis Ltd, India

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

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

[4] E.Inzunza-Gonzalez, C. Cruz-Hernandez, R. M. Lopez-Gutierrez, E.E. Garcia-Guerrero, L. Cardoza-Avendano, H. Serrano- Guerrero, " Software to Encrypt Message Using Public-Key Cryptography".

[5]Federal Information,"Secure Hash Standard", Processing Standards Publication 180-2, Aug 1, 2002

[6]M.Markovic, T.Unkasevic, G.Dordevic,"Institute of Applied Mathematics and Electronics", Kneza Milosa 37, 11000 Belgrade, Yugoslavia

[7]Mr.P.Balakumar "Biometrics Based File Transmission Using RSA Cryptosystem", Selvam College of Technology, Namakkal, Tamilnadu, India

[8]Pradosh Kumar Mohapatra, "Public Key Cryptography", ACM Student Magazine.

[9] R.L Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology.

[10] Roman Novak, "On the Security of RSA Capable Smart Cards" Jo·zef Stefan Institute Jamova 39, 1000 Ljubljana, Slovenia

[11] W.Stallings, "Cryptography and Network Security", Principles and Practices, Fourth Edition, 2006