SECURE E-MAIL SYSTEM USING HYBRID APPROACH OF TRIPLE-DES AND RSA ENCRYPTION ALGORITHMS

Khin Lay Mon, Thiri Naing
Computer University (Meiktila), Myanmar
khinlaymon.tk@gmail.com, thuthiri@gmail.com

ABSTRACT

Security challenges are evolved by the explosive growth of digital communications as e-mail and Internet, and also millions of electronic transactions need protection, by the rapid growth of commerce. Thus, this made security a vital issue for every consumer. In order to attain the security of information, unauthorized access to information must be prevented, privacy must be established. These processes are imperative for the success of secure information security technology (cryptography) is to keep the content of information secret among all authorized entities. i.e. confidentiality. This system implements two encryption and two decryption as hybrid approach by using the combination of a symmetric encryption algorithm, Triple-DES and an asymmetric encryption algorithm, RSA encryption algorithm. One of the two components is key encryption with RSA public key algorithm and another is data encryption by using the Triple-DES encryption algorithm.

1. INTRODUCTION

Cryptography provides the basics for authentication of messages as well as their security and integrity; carefully designed security protocols are required to exploit it. There are different types of encryption algorithms used to protect sensitive data including; symmetric, asymmetric encryption techniques.

The selection of the cryptographic algorithms and the management of the key are critical to the effectiveness, performance and usability of security mechanisms. Public-key cryptography make it easy to distribute the cryptographic keys but its performance is inadequate for the encryption of bulk data. Secret-key cryptography is more suitable for bulk encryption task. Each individual algorithm's architecture has advantages and disadvantages.

As such, in this thesis we develop the Combining Information Secure System. These system uses the secret-key cryptography to encrypt the data and use the public-key cryptography to encrypt the secret-key. To implement the proposed system, we used the combination of RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), public-key algorithm and Triple-DES (Triple Data Encryption Standard), secret-key algorithm.

2. MOTIVATION

Symmetric cipher uses the same key for encryption and decryption If the sender encrypt a message and send this encrypted message to the receiver, both the sender and receiver must use the same key. The advantages of the symmetric cipher are speed due to its relatively low computational requirements. The problem of symmetric cipher is how the two parties exchange the symmetric key securely.

In asymmetric cipher, the sender and receiver must have a key pair that consists of public and private key. The sender uses the public key for encryption message. The private key used to decrypt the message. The public key algorithms are much slower than symmetric key algorithms but they can solve the key distribution problem. One disadvantage of public-key algorithms is that the public-key algorithms would not be suitable for encryption large amounts of data [2]. This system would be to get secure communication between two entities. This system implements the high speed and high performance by using the symmetric and to avoid the key management problem by using the asymmetric encryption algorithm.

3. RELATED WORK

Security plays a vital role for all systems that uses network to send message especially in distributed system. For this reason, several approaches are explored for developing a secure communication

system. The ancient people began to use substitution ciphers and transposition ciphers. Which means encryption was usually based on alphabetic letters of message. Many problems related to substitution cipher and transposition ciphers had occurred such as security relied with sender/ receiver to know the encryption algorithm and keep it secret; method not feasible to implement among large group.

In secret-key cryptography, the sender and receiver use the same key for both encryption and decryption. Firstly, the sender and receiver must agree the secret-key before the sender sends her message to the receiver. The weak point of symmetric cryptosystem is the key distribution. To solve the problem public key cryptography have developed. One of the disadvantages on asymmetric (public-key) cipher is that it can not operate large data encryption.

The attractive solution for above problems is to implement the hybrid approach. First is data encryption by using Triple-DES algorithm, a symmetric algorithm. Second function is key encryption by using RSA algorithm, public key algorithm. This system can provide the secure way for peer-to-peer data transfer. By using this system, we can obtain the security of text data. The system applies the hybrid method. Therefore, we can achieve fast encryption speed and can solve the key management problem.

4. SYMMETRIC ENCRYPTION

Symmetric algorithm sometimes called conventional algorithms is algorithms where the encryption key can be calculated from the decryption key and vice versa. The symmetric algorithms, also called secret-key algorithms require that the sender and receiver agree on a key before they can communicate securely.

The security of a symmetric algorithm is completely depending on how well the key is protected. Decryption is thus simply the inverse of the encryption algorithm.

4.1 Triple-DES block cipher

The Data Encryption Standard (DES) was published by the National Bureau of Standards in 1977 [5] and reaffirmed in its final form by the Federal Information Processing Standards Publication (FIPS) in 1994 [6]. DES is a block cipher with Feistel [7] networks, which operates on data blocks of 64-bit length. Triple- DES variant was developed after it became clear that DES by itself was too easy to crack. Triple-DES is symmetric cryptosystem. Triple-DES is designed to operate on 192 bit blocks of data. . A block is transformed into an encrypted (192 bit) block of output in 48-rounds. Triple-DES is built on three DES block cipher in order to support a higher security level. It operates on the Encryption-Decryption-Encryption (EDE) mode, which uses sequentially first DES encryption, then DES decryption and last DES encryption, with the support of three different keys. The total keys length therefore is 3x64 = 192 bits. The required key length of Triple-DES is 192 bits. The decryption operation of the Triple – DES is performed such as DED mode.

Triple- DES applies the DES algorithm three times as EDE sequence. Each DES encryption begins with initial permutation IP that rearranges the bit to produce the permuted input. This is followed by a phase consisting of 16 rounds of the same functions which involves both permutation and substitution functions. The output of the last (sixteenth) rounds consists of 64 bits that are a function of the input plain text and the key. The left and right halves of the output are swapped to produce the pre-output. Finally, the pre- output is passed through a permutation (IP^{-1}) that is the inverse of initial permutation function, to produce the 64 bit cipher text. DES decryption uses the same algorithm as encryption except that the application of the sub keys is reversed.

In this system, Triple-DES encryption algorithm is used for encryption and decryption a sensitive data.

5. ASYMMETRIC ENCRYPTION

The concept of public-key cryptography was introduced in 1976 by white field Diffi and Martin Hellman in order to solve the key management problem. In their concept, each person gets a pair of keys, one called the public-key and the other called the private key. Each person's public-key is published while the private-key is kept secret. The need for the sender the receiver to share secret

information is eliminated: all communications involve only
public-keys and no private-key is ever transmitted or shared.

Furthermore, public-key cryptography can be used not only for privacy encryption; but also for authentication (digital signatures).

5.1 RSA algorithm

Ron Rivest, Adi Shamir, and Leonard Adleman invented the RSA algorithm in 1978 in response to the ideas proposed by Hellman, Diffie, and Merkel. This algorithm was the first publicly available public-key cryptosystem in the world and despite its security being unproven; confidence in it has risen over years of cryptanalysis. Because of this, it has subsequently become the most widely used cryptosystem in the world.

The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. RSA uses two separate keys for encryption and decryption. One key is made public, enabling anyone to send the message to the holder of the corresponding private key and allow the holder to decrypt the message with this 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. A typical key length of RSA for a secure transmission is 1024 bit or 309 decimal digits.

Here are RSA algorithm.

For encryption the Plain text message M,

$$C = M^{e} \bmod n$$

For decryption the Cipher text C,

$$M = C^{d} \bmod n = (M^{e})^{d} \bmod n$$

Key generation algorithm

- Choose two distinct prime numbers p and q and compute $n = p * q$
- Compute $\Phi = (p-1)(q-1)$
- Choose an integer e, $1 < e < \Phi$, such that $\gcd(e, \Phi) = 1$
- Compute the secret exponent d, $1 < d < \Phi$ such that $ed = 1 \pmod{\Phi}$
- The public key is (n, e) and the private key is (n, d).

The values of p, q and Φ should also be kept secret. Both sender and 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 with a public key of KU = { e,n } and a private key of KR ={d, n }.

In this system, RSA algorithm is used for encryption secret-key.

6. HYBRID CRYPTOSYSTEM

The implementation of hybrid algorithms has helped expel some of the flaws of using individual symmetric and asymmetric algorithms. The system is faster and carriers less overhead. than asymmetric algorithms and it solves the key-distribution problem of symmetric encryption.

The security of hybrid cryptosystems does rely on the security of the asymmetric algorithm, as obtaining the asymmetric private key and subsequently discover the plain text. This is however, a more secure method (as opposed to purely using an asymmetric algorithm) because pattern recognition and statistical analysis can be used on encrypted plain text whereas it can't be used on encrypted random values (of the symmetric key). Also a further level of complexity has been added by encrypting the key for the plain text and this appends to the level of difficulty of cryptanalysis.

7. OVERALL SYSTEM DESIGN

The system consists of two encryption and decryption components. The sender needs to perform the data encryption and key encryption. The receiver needs to perform the key decryption and data encryption.

To work with the system, the sender does the following steps-

1. Encrypt the message with the Triple-DES key.

2. Encrypt the Triple-DES key with RSA public key.

3. Send the encrypted file and key.

The receiver needs to perform the following steps-
1.Recover the Triple-DES key by decrypting with RSA private key.

2. Obtain the original message by decrypting the encrypted message with recover symmetric key

8. USER ACTIVITY OF THE PROPOSED SYSTEM

In this system, the sender and receiver must perform two encryption and decryption process. If sender sends an encrypted message; he would encrypted his plaintext using his symmetric-secret key, then encrypt his symmetric-secret-key using receiver's asymmetric-public-key, then send both the cipher text and the encrypted key to receiver. Receiver would then decrypt sender's encrypted key by using asymmetric-private-key and then use that to decrypt cipher text, this can be see in the figure:

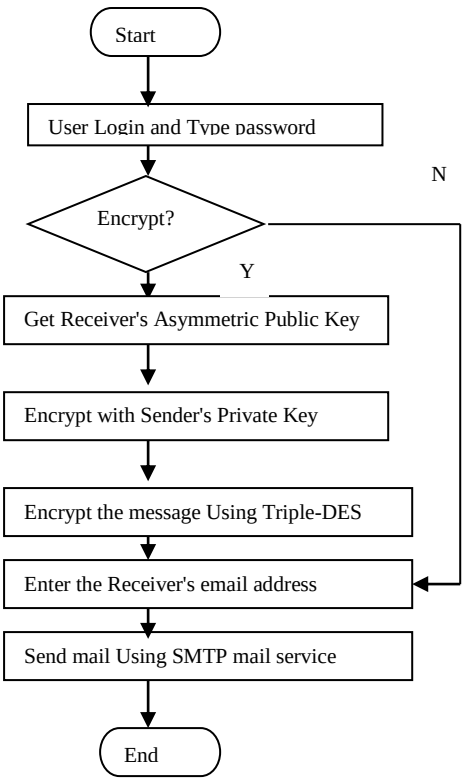
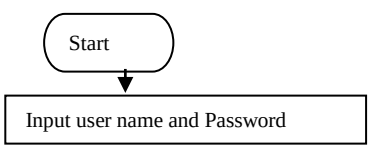


Figure 1. System flow diagram for Sender



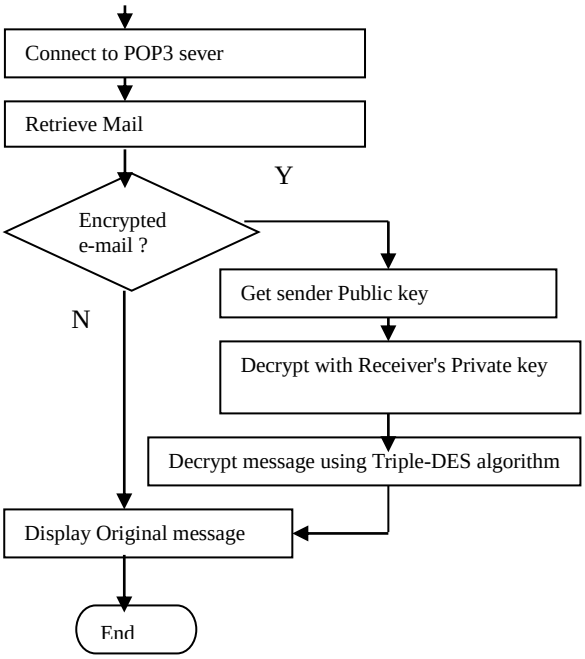


Figure 2. System flow diagram for Receiver

9. IMPLEMETATION OF THE SYSTEM

This system splits a hybrid encryption scheme into two distinct components: an asymmetric key encapsulation mechanism and a symmetric data encapsulation mechanism. It does have the advantages of allowing the security requirements of asymmetric and symmetric parts of the scheme to be completely separated. It can be used for data communication and electronic commerce in open networks. Public key cryptography is used to protect digital data going through an insecure channel from one place to another. RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures.

Using symmetric cryptography, it is safe to send encrypted message without fear of interception; however, there always remain the difficult problem of how to securely transfer the key to the recipients of a message so that they can decrypt the message. Public-key encryption is used to solve the problem of delivering the symmetric encryption key to the receiver in a secure manner.

This system implements the hybrid system that includes two main components: key encryption and data encryption. The sender needs to perform the data encryption and key encryption. The receiver needs to perform the key decryption and data encryption. At first, the sender must login in sending message side. And then, encrypt the message with the Triple-DES key and encrypt the Triple-DES key with RSA public key. After that, send both the encrypted message and key by using the SMTP service. In receiver side, it has to recover encrypted key and encoded message. The receiver recover the Triple-DES key by decrypting with RSA private key as the first step. Then, he can get the original message by decrypting the encrypted message with recover symmetric key. Therefore, the system can support an effective encryption technique for the distributed system. The proposed system implements as shown in following figures-

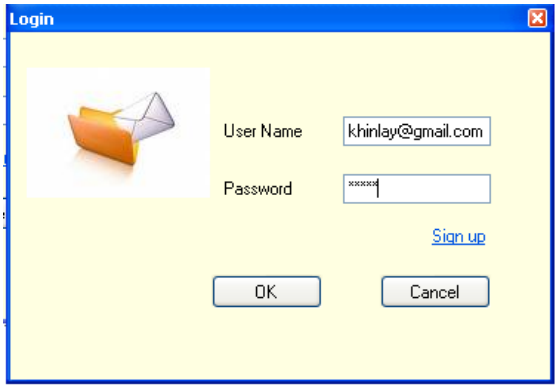


Figure 3. User Interface for Login Form

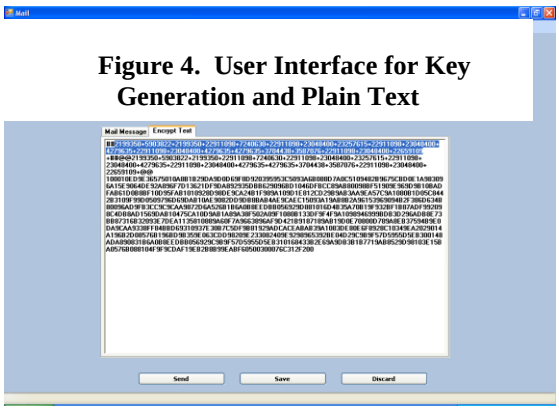


Figure 4. User Interface for Key Generation and Plain Text

Figure 5. User Interface for Cipher Text (Both Key and message)

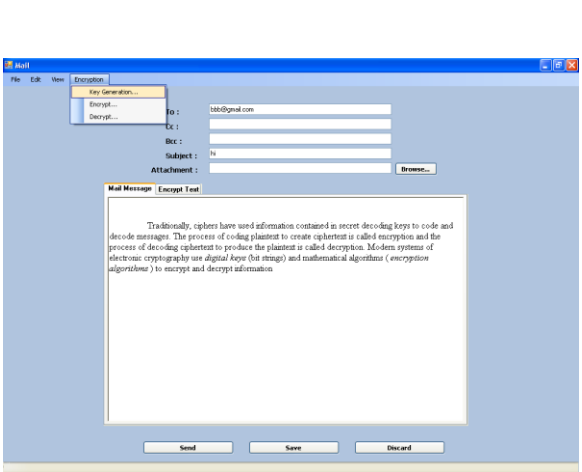


Figure 6. User Interface for Decryption Process Form

10. CONCLUSION

Symmetric cipher have key distribution problem because the symmetric encryption algorithm used the same key for encryption and decryption. Public key cryptography solves that problem. In a public key cipher, the sender has a key pair consisting of a public key and a matching private key. All known public key algorithms are much slower than symmetric key algorithms. It would not be practical to use a public key algorithm to encrypt large amount of information. However, that problem can easily be overcome by combining a public key cipher with a fast symmetric cipher.

The system decrypt e-mail message encrypted with the symmetric encryption algorithm, Triple-DES and the asymmetric encryption algorithm, RSA between two communications. It is necessary to add the compression algorithm to replace the common groups of text with single character. That can decrease the size of the cipher text, therefore increasing transfer speeds, decreasing storage needs and increasing the level of complexity for cryptanalysis. Therefore, the system can support an effective encryption technique for the distributed system.

References

[1] Brue Schneier

"E-mail Security", How to keep Your Electronic Message Private, John Wiley and Sons, Inc, 1995.

[2] D.Tom, "Cryptography," February 7, 2000.

[3] Simmons, R.J

"Symmetric and Asymmetric Encryption"

ACM Computing Surveys, December 1979.

[4] Date, C.J

"Security" Volume II

Reading Mass: Addition-Wesley (1983)

[5] Data Encryption Standard, Federal Information Processing Standard (FIPS) 46, National Bureau of Standard, 1977

[6] Federal Information Processing Standards Publishing 140-1, Security Requirements for Cryptographic Modules," U.S. Department of Commerce/NIST, Springfield, VA: NIST, 1994

[7] B. Schneier, "Applied Cryptography, Protocols, Algorithms, and Source Code in C" , John Wiley & Sons 1994.