Implementation of Secure Data Transfer Using Hybrid Cryptosystem

Cherry Kyaw Win, Tin Zar Zar
Computer University (Dawei)
cherrykyaw.w@gmail.com

Abstract

Nowadays, Internet and network applications are growing very fast. Thus, people need to protect the information and to thwart the hackers. People interconnect their secret data by using cryptographic algorithms. But, the hackers can try to get the key, and therefore, the key security is the most important role in the cryptographic system. This paper intends to transfer data with high security by using hybrid cryptosystem. Hybrid Cryptosystem uses the secrete-key cryptography to encrypt the data and use the public-key cryptography to encrypt the secrete-key. It uses combination of the AES (Advance Encryption Standard) and RSA (River-Shamir-Adleman) algorithm. The system is based on the peer-to-peer architecture. In this system, the design of the cryptography technique is based on the digital envelope. The system can support user Authentication portion and data integrity.

1. Introduction

The expansion of the internet has caused an increase in the communication and storage of data, which has prompted to use more secure forms of protection information. Cryptography becomes the most important role while transferring the data over insecure communication channels.

Cryptography provides the basics for authentication of messages as well as their security and integrity. The various types of cryptographic algorithms provide high security in information, computer and network related activities and also protect the data integrity from various attacks. They include symmetric and asymmetric encryption technique [6].

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 makes it easy to distribute the cryptographic keys but its performance is inadequate for the encryption of bulk data. Secrete-key cryptography is more suitable for bulk encryption task. The architecture of each individual algorithm has advantages and disadvantages.

Therefore, in this thesis, hybrid cryptosystem uses the combination of AES (Advanced Encryption Standard) and RSA (River - Shamir – Adleman) algorithm. AES algorithm is used for file encryption and RSA algorithm is used for key encryption .Any file is encrypted with AES algorithm by using symmetric key. And then, this symmetric key is encrypted with RSA algorithm by using the receiver's public key. This system implements for a secure data transfer between two parties so that they can securely transmit and access critical information.

2. Symmetric Secret-key Cryptography

The Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. The modern study of symmetric –key ciphers relates mainly to the study of block cipher and stream ciphers and to their applications [7]. In any symmetric-key encryption technique, both the encryption and decryption process are carried out by using a single key. These algorithms are efficient, secure, execute at high speeds, and consume less computer resources of memory and processing time. However, symmetric key cryptographic techniques suffer from the disadvantages of Key distribution problem and Key management problem.

2.1. AES Algorithm

AES (Advance Encryption Standard) is a symmetric key system, which uses 128-bit data blocks and supports 128-bit, 192-bit and 256-bit key sizes. AES is a block cipher, which produces the encrypted data (cipher text) from 128-bit data blocks and the encryption key. The data to be encrypted (plaintext) is processed in 128-bit blocks. The encryption algorithm consists of four states.

SubBytes
ShiftRows
MixColumns
AddRoundKey.

2.1.1. SubBytes () Transformation

The SubBytes( ) transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table (s-box). The S-box used in the SubBytes( ) transformation is presented in hexadecimal form.

2.1.2. ShiftRows () Transformation

In the ShiftRows ( ) transformation ,the bytes in the last three rows of the state are cyclically shifted over different numbers of bytes. The first row is not shifted. Shift for the second row, 1-bytes circular left is shift for the second row, 2-bytes circular left shift for the third row, 3- byte circular left shift is for the fourth row.

2.1.3. MixColumns() Transformation

The MixColumns ( ) transformation operates on the state column by column, treating each column as a four-term polynomial.

2.1.4. AddRoundKey( ) Transformation

In the AddRoundKey() transformation, a Round Key is added to the State by a simple bitwise XOR operation.. Each Round Key consists of Nb words from the key schedule.

In add round key stage makes use of the key. Any other stage applied at the beginning or end is reversible without knowledge of the key, this scheme is more efficient and secure.

2.2. AES decryption

In the decryption algorithm, the sub bytes, shift row, mix columns stages are used as inverse function. In add round key stage, the inverse is achieved by XOR the same round key to the block. The decryption algorithm is not identical for the encryption algorithm. This is a consequence of the particular structure of the AES [6].

AES encryption and decryption flow is shown in figure 1.

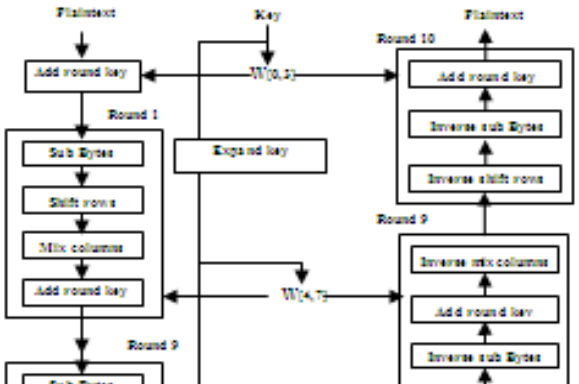

Figure 1. AES Encryption and Decryption

3. Asymmetric Secret Key Cryptography

The Asymmetric Secret-Key cryptography, also known as public key cryptography, is encryption that uses two different keys for encryption and decryption. One key is a public key that can be distributed to anyone. The other is a mathematically related key called a private key or secret key. This is a key that should be kept secret from the world. Only the owner should have access to the private key [9]. A primary advantage of such system is that providing authentic public-keys which is generally easier than distributing secret keys securely.

Public- Key encryption schemes are typically substantially slower than symmetric key encryption algorithms such as DES. For this reason, public-key encryption is most commonly used in practice for the transport of keys. Asymmetric ciphers are more mathematically complex than symmetric ciphers. They are based on the difficulties involved in solving certain mathematical problems.

3.1. RSA algorithm

The Rivest-Shamir-Adleman (RSA) algorithm was the first realization of a public key system. It has also become the most widely used public-key system. The security of algorithm is conjectured to be as hard as factoring large integers.

3.1.1. RSA Key Generation

RSA Key generation includes the following steps.

1. Generate two large random primes, p and q, of approximately equal size such that their product n = p q is of the required bit length, e.g.: 1024 bits.
2. Compute n= p q and $\Phi = (p-1)(q-1)$.
3. Choose an integer e, $1 < e < \Phi$, such that gcd (e, Φ) =1.
4. Compute the secret exponent d, $1<d<\Phi$, such that e d =1 (mod Φ).
5. The public key is (n, e) and the private key is (n, d).
   n is known as the modulus.
   e is known as the public exponent or encryption exponent.
   d is known as the secret exponent or decryption exponent.

3.1.2. RSA Encryption

Sender does the following:

1. Obtains the recipient's public key (n, e).
2. Represents the plaintext message as a positive integer m.
3. Computes the cipher text $C= m^e \bmod n$.
4. Sends the cipher text c to B.

3.1.3. RSA Decryption

Recipient does the following:

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the integer representative m.

3.2. Hybrid Cryptosystem

It uses both symmetric key and asymmetric key algorithms to achieve secure communication. Symmetric algorithms are much faster than public key algorithms. The public key cryptographic algorithms are more secure than symmetric algorithms, because it has two keys, one for encryption and another for decryption. Public key encryption solves the key exchange problem. In this hybrid encryption technique, symmetric algorithm is for encryption /decryption and public key cryptosystems for authentication [6].

4. The System Design

In this system, design of the cryptography technique is based on the digital envelope. The system includes the two encryption and two decryption components. The two encryption components are AES file encryption and RSA key encryption. The two decryption components are RSA key decryption and AES file decryption component. It's shown in the figure 2.

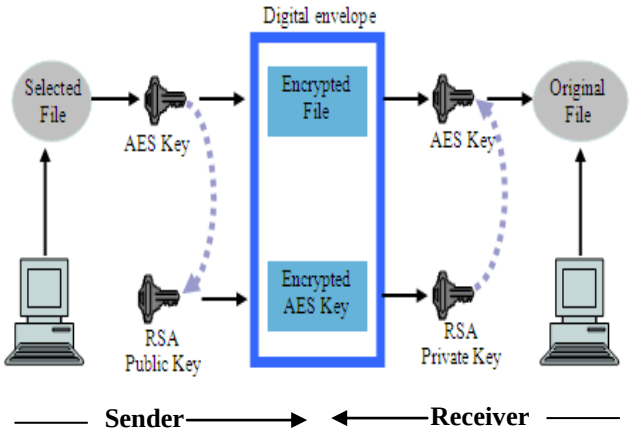

Figure 2. The System Design

4.1. Sender Side

The sender needs to perform the file encryption and key encryption.

To encrypt the file, the sender side needs to perform the following three steps:

1. Encrypt the user's text file by using AES (symmetric) algorithm.
2. Encrypt the AES (symmetric) key with RSA (Asymmetric) algorithm.
3. Send the encrypted file and key pass through the insecure channel.

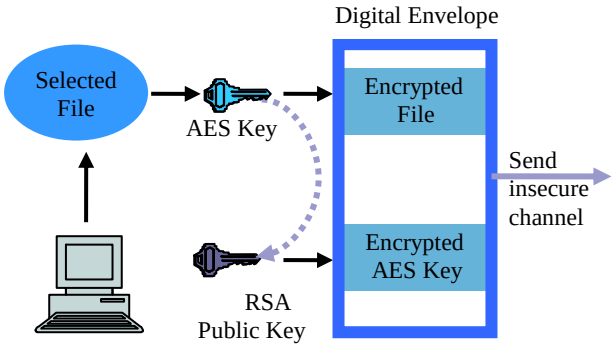

Figure 3. Encryption Process for Hybrid Cryptosystem

4.2. Receiver Side

The receiver needs to perform the key decryption and file decryption.

To decrypt the file, the receiver needs to perform the following two steps.

1. Decrypt the AES secrete key with RSA private key.
2. Decrypt the file with recover AES key.

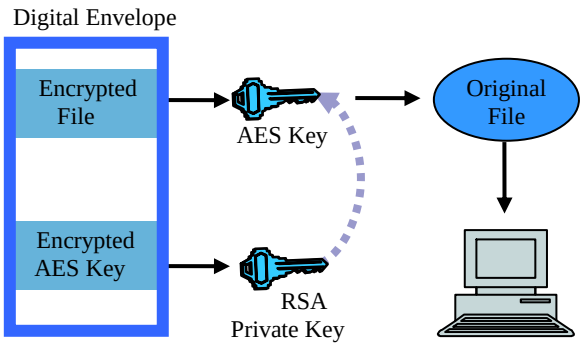

Figure 4. Decryption Process for Hybrid Cryptosystem

5. Time Evaluation

5.1. File size evaluation

The system is implemented the proposed hybrid cryptosystem using the combination of RSA and AES algorithm as well as we analysis to evaluate for each algorithm based on file sizes. The evaluation results are shown in table 1 and 2.

Table 1. File size after encryption of AES

Before encryption	After encryption
5 kb	no change
13 kb	no change
307 kb	no change

Table 2. File size after encryption of RSA

Before encryption	After encryption
5 kb	13 kb
96 kb	191 kb
307 kb	799 kb

In this table, the file size after encryption of AES is no change and RSA is larger than the original file.

5.2. Message Transmission Time

The time needed to transfer the data between the sender and receiver is very important in distributed system.

The time required for a network to transfer the message between two computers is as follows:

Message Transmission Time = latency + length/data transfer rate

In this equation, if the data size increased transmission time will be increased. The file size after encryption of RSA is greater than AES. Therefore, RSA will take more transmission time than AES.

5.3. Processing Time

AES key is short (128 bit) and encryption process is simple.

RSA key is very lone (1024 bit) and factorizing of the large prime numbers is time consuming.

So, encrypt and decrypt processing speed of AES is faster than RSA.

5.4. Key security evaluation

In AES algorithm, the key length is short and it needs to pass the key through the insecure channel. The two parties share the same key and if anyone receives the key can hack the encrypted file.

In RSA algorithm, the key length is long and no need to pass the key through the insecure channel. The two parties use the different key and difficult to hack the key.

Therefore, key security of RSA is more efficient than AES algorithm.

5.5. Experimental result

Hybrid cryptosystem uses a combination of both symmetric and asymmetric algorithms to encrypt the plaintext and symmetric key. The system is faster and carries less overhead than asymmetric algorithms .It solves the key distribution problem of symmetric encryption. Because Hybrid system encrypts both the plaintext and symmetric key, it decreases the probability of hacking the key and cipher text by un-authorized person. However, by making comparison between two algorithms, both the speed and efficiency are greatly improved. The experimental result of the system is shown in figure 5.

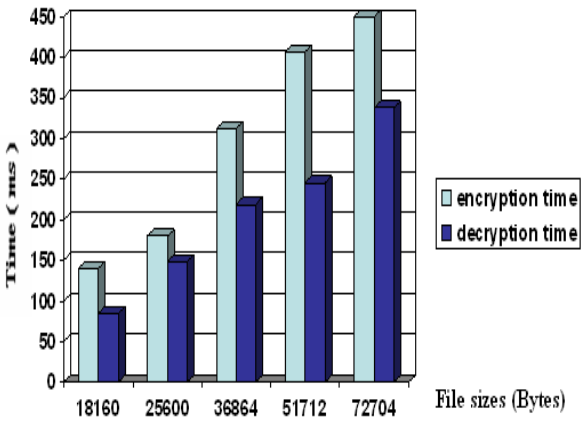

Figure 5. Encryption and Decryption time of the system.

6. Conclusion

Security is one of the most important parts in commercial applications. The selection of the cryptographic algorithm and the management of the key are critical to the effectiveness, performance and usability of security mechanisms. By using the hybrid algorithm, the system can take their advantages and can support effective encryption technique and key management for distributed system. Therefore, this system can achieve fast and secure way for communication of sensitive data in hybrid Cryptosystem. This system can be applied in critical applications, such as Banking systems, credit card and so on. C# programming language is used to develop this system.

7. References

[1] An Introduction to Cryptography.
ftp://ftp.pgpi.org/pub/pgp/7.0/docs/
english/IntroToCrypto.pdf (June27, 2001)

[2] Atreya , Mohan. Introduction to Cryptography.
http://www.rsa.com/solutions/developers/whitepapers
/IntrotoCrypto.pdf (June 27, 2001)

[3] Behrouz A.Forouzan
"Computer and Network Security". International Edition 2008.

[4] W.Stallings, *Cryptography and Network Security Principles and Practices, Fourth Edition 2007*

[5] Dr. Brian Gladman, v3.1, 3rd March 2001
"A Specification for The AES Algorithm" Rijndael (by Joan Daemen & Vincent Rijmen)

[6] Dr.E.Ramaraj[1],S.Karthikeyan[2] and M.Hemalatha[3]
"A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)" International Journal of The Computer, the Internet and Management Vol. 17.No.1 (January-April, 2009) p p 78-86.
.

[7] http://en.wikipedia.org/wiki/Cryptography

[8]http://vurooz.blogspot.com/2009/12/cryptography-history-of-cryptography.html.

[9] Jessica J. Benz
PGP: A Hybrid Solution
GIAC Certification Vers ion1. 2e

[10] KarLie, .Radia, S.Mike,
Network Security Private Communication in a Public World". Second Edition.