International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Editorial Board

Editorial Advisory Board

Title

SECURE FILE TRANSMISSION SCHEME BASED ON HYBRID ENCRYPTION TECHNIQUE

Author(s)

Gaurav Shrivastava

Assistant Professor & Head,

Department of Information Technology,

Mathura Devi Institute of Technology & Management,

Indore, Madhya Pradesh, INDIA

ABSTRACT:

To enhance the security level of data transmission in Open Network, a hybrid encryption Technique based on AES, RSA and MD5 is proposed. The mechanism makes full use of advantage of AES RSA, MD5 because encryption speed of AES algorithm is faster than RSA algorithm for long Encrypting Plain Texts, and RSA algorithm Key distribute is very safely and easily. Under the dual protection with the AES algorithm and the RSA algorithm, the data transmission in the Open Network will be more secure. Mean while, it is clear that the procedure of the entire encryption is still simple and efficient as ever. Digital abstract Algorithm MD5 is adopted in this technique. It is an effective technique to overcome the problem of safe data transmission in network. This Technique maintained the confidentiality, Authentication and Integrity.

Keywords: Double DES, RSA, Digital Abstract. Hybrid Encryption Technique

1. INTRODUCTION:

In the Internet, global information tide expends the application of information network technology. It also brings about great economical and social benefit along with the extensive use of this technology. However, because Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet. Information security becomes a hot problem which is concerned by our society. This paper puts forward a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. Than we required some technique to solve a problem in internet and over technique includes many properties are confidentiality, completeness, authentication of identity, and non-repudiation. [1]

For implementing the secure file transmission in Internet, a Hybrid Encryption Technique which base on Double DES, RSA and MD5 Digital Abstract. The mechanism makes full use of advantage of DES and RSA. Because encryption speed of Double DES algorithm is faster than RSA algorithm for large size File, and RSA algorithm distribute key safely and easily. File

encryption security of Double DES algorithm is far higher than DES algorithm. Digital abstract algorithm MD5 is adopted in this Technique. Which is got by receiver through MD5 algorithm, data security can be guaranteed. This Technique is maintained the confidentiality, authentication and integrity. It is an effective method to resolve the problem of secure file transmission in Internet

2. SYMMETRIC KEY ALGORITHM – II DES:

The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key. DES is a block cipher. It encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bit of cipher text the same algorithm and key are used for encryption and decryption. The key length is 56 bits. Consequently the two main variation of DES have emerged, which are Double DES and Triple DES.

Double DES uses two keys, says k1and k2. It first performs DES on the original plain text using k1 to get the encrypted text. It again performs DES on the encrypted text, but this time with the other key k2. The final output is the encryption of encrypted text.

$$p \rightarrow E(k_1, \quad p) \rightarrow E(k_2, \quad E(k_1, \quad p)) = C$$

Double DES has a 112-bit key (the key is actually 128 bits, but every 8^{th} bit is a parity check; so, only 112 or the 128 bits are meaningful) and enciphers blocks of 64 bits.

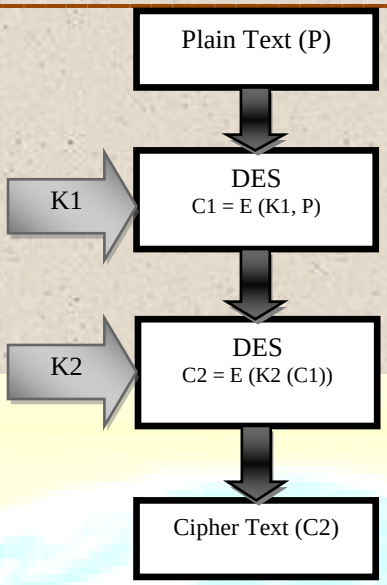

Fig: 1 Double DES

3. ASYMMETRIC KEY ALGORITHM – RSA:

Asymmetric key algorithm is also called Public key algorithm. The basic thought of public key algorithm is that the key is divided into two parts. One is encryption key and the other is decryption key. Encryption key cannot be got from decryption key and vice versa. Because public key is open and private key keep secret, RSA algorithm overcomes difficult of key distribution. RSA encryption process is showed as figure 2.

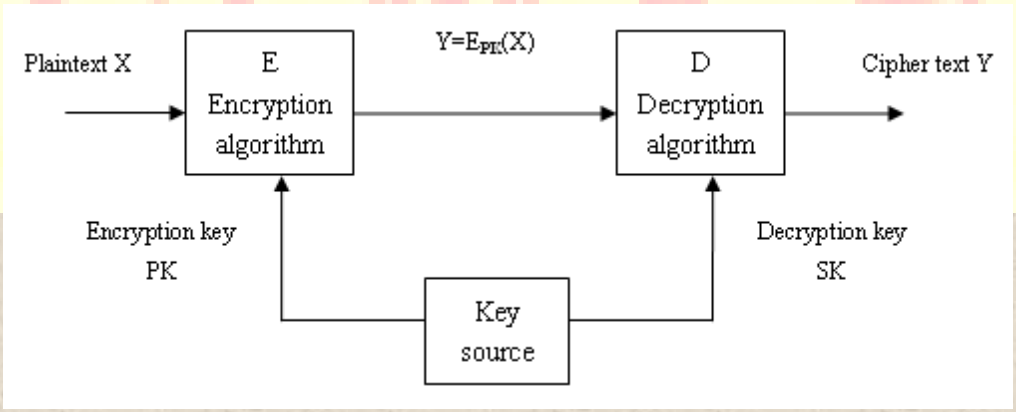

Fig: 2 The process of RSA

The principle of RSA algorithm is that: according to number theory, it is easy to finds two big prime number, but the factorization of the two prime numbers is hard. In this theory, every customer has two keys. They are encryption key PK = (e, n) and decryption key SK = (d, n). Customer opens public key. Each person who wants to transmit information can use the key. However, customer keeps private key to decrypt the information. Here, n is the product of two big prime number p and q (the bits of p and q which are decimal number extend 100). e and d satisfy certain relation. When e and n are known, d cannot be got. The specific content of algorithm is showed as below. [1]

A. Encryption and Decryption Algorithm

Assuming integer X expresses plaintext and integer Y expresses cipher text. The operation of encryption is that Encryption:

$$Y = X^e \bmod n$$

The operation of decryption is that

$$\text{Decryption: } X = Y^d \bmod n$$

B. Key Generation and Calculation of Relevant Parameter

1) Calculating n. Customer selects two big prime number p and q. The value of n can be got by the equation n = p * q. n is the mode number of RSA algorithm. Plaintext must be expressed by a number which is smaller than n. In practice, n is long number which includes a few hundreds of bits.
2) Calculating φ (n). Customer calculates the Euler function
   a. $\varphi(n) = (p-1) * (q-1)$
   b. φ (n) is defined as the number which is smaller than n and primes to n.
3) Choosing e. Customer chooses a number e which prime to φ (n) from [0,φ (n) − 1] as open encryption index.
4) Calculating d. Customer calculates the d which satisfies the follow equation.
5) $e * d = 1 \bmod \varphi(n)$

6) Public key PK = (e, n) and private key SK = (d , n) are got through calculating.[1]

4. SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY TOGETHER:

If would be very effective, if we could combine the two cryptography algorithm mechanism, so as to achieve the better of the two and yet do not compromise on any of the features? More specifically, we need to ensure that the following objectives are met:

1) The solution should be complexity
2) The encryption and decryption processes must not take long time.
3) The generated cipher text should be compact in size
4) The solution should scale to a large number of users easily, without introducing any additional complications.
5) The key distribution problem must be solved by the solution.

Indeed, in practice; symmetric key cryptography and asymmetric key cryptography are combined to have a very effective security solution. [3]

5. MESSAGE DIGEST ALGORITHM:

Message Digest Algorithm (MD5) was designed by Ron Rivest in 1991 to replace an earlier hash function, The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

6. PROCESS OF HYBRID ENCRYPTION TECHNIQUE:

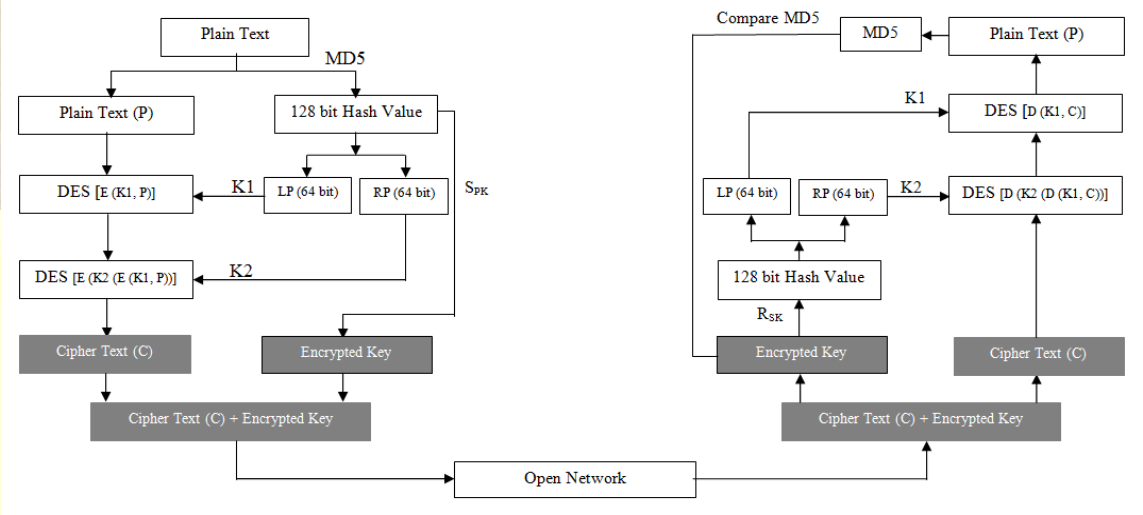

Fig: 3 The Process of Hybrid Encryption Technique

In The Double DES Algorithm is a symmetric, block-oriented cryptographic algorithm. It operates on 64-bit plaintext blocks and uses 112-bit (originally 128 bits) keys, what makes it practically immune to brute force attacks. IDEA is build upon a basic function, which is iterated eight times. The first iteration operates on the input 64-bit plaintext block and the successive iterations operate on the 64-bit block from the previous iteration. After the last iteration, a final transform step produces the 64-bit cipher text block. [3]

Public key algorithm is also called asymmetric key algorithm. The basic thought of public key algorithm is that the key is divided into two parts. One is encryption key and the other is decryption key. Encryption key cannot be got from decryption key and vice versa. Because public key is open and private key keep secret, RSA algorithm overcomes difficult of key distribution. The principle of RSA algorithm is that: according to number theory, it is easy to finds two big prime number, but the factorization of the two prime numbers is hard. In this theory, every customer has two keys. They are encryption key PK = (e, n) and decryption key SK = (d, n). Customer opens public key. Each person who wants to transmit information can use the key. However, customer keeps private key to decrypt the information. Here, n is the product of two big prime number p and q (the bits of p and q which are decimal number extend 100). e and d satisfy certain relation. When e and n are known, d cannot be got. [3]

Message-Digest refers to hash transformation of message. MD5 algorithm gets the remainder (64 bits) of the primitive plaintext through mod 2^{64}. The result is added to the end of Message. The MD5 code includes the length information of the message. Some message whose range of bits from 1 to 512 is added into the place which is between message and remainder. After filling, the total length is several times of entire 512. Then the whole message is divided into some data blocks. Each of them includes 512 bits. The data block is further divided into four small data blocks which include 128 bits. The small data block is input into hash function to perform four round calculations. In the end, MD5 message abstract is got. [1]

A. ENCYPTION PROCESS

The Encryption of Hybrid Encryption Technique as follows.

- The first, calculate MD5 of plain text (P) than generate 128 bit hash Value.
- The second 128 bit hash value divided in to two equal part LP (Left Part) & RP (Right Part) both are 64 bit.
- The third, consider LP as a key K1 and RP as a key K2.
- Fourth DES algorithm encrypt the plain text with the help of key K1, and produce cipher text C1 (C1 = E (K1, P)). Then again DES algorithm encrypt cipher text C1 with the help of key K2, and produce cipher text C2 (C2 = (E (K2 (C1))).
- Fifth 128 bit MD5 encrypted by RSA algorithm with receiver public key R_{PK} and produce encrypted key (EK).
- Six combine a cipher text (C2) and encrypted key (EK), produces a complex message (CM). CM is send to the receiver.

B. DECRYPTION PROCESS

The decryption of Hybrid Encryption Technique as follows.

- The first, the receiver received complex message CM into two parts; one is cipher text (C2) and other encrypted key EK.

- The second encrypted key (EK) decrypted by RSA algorithm with receiver secret key R_{SK} and produce 128 bit key.
- The third, 128 bit key divided in to two equal part LP (Left Part) & RP (Right Part) both are 64 bit.
- The fourth, consider LP as a key K1 and RP as a key K2.
- Fifth DES algorithm decrypt cipher text (C2) with the help of key K2, and produce cipher text C1 (C1 = D (K2, C2)). Then again DES algorithm decrypts cipher text (C1) with the help of key K1, and produce plain text P.

C. COMPARE DIGITAL ABSTRACT

- The first, Calculate MD5 of plain text (P).
- The second encrypted key (EK) decrypt by RSA Algorithm with help of Receiver Secrete Key R_{SK} and produce a key and it's also a MD5.
- Then third compare Both MD5s.

7. ADVANTAGE OF HYBRID ENCRYPTION TECHNIQUE:

- Using DES Algorithm MD5 Algorithm maintain a Integrity.
- Using MD5 Algorithm maintain a Integrity.
- Using RSA algorithm and the IDEA key for data transmission, so it is no need to transfer IDEA key secretly before communication;
- Management of RSA key is the same as RSA situation, only keep one decryption key secret;

8. CONCLUSION:

Secure File Transmission Scheme Based on Hybrid Encryption Technique, Hybrid Encryption Technique is based on Double DES, RSA and MD5 algorithm. It makes use of the full advantage

of Double DES which has the high encryption speed for long plaintext and RSA algorithm is manages the key easily. The receiver can verify whether the information is tampered in network through using MD5 algorithm. It is an effective method to resolve the problem of secure File transmission in Internet. We should develop improved cryptosystems to provide greater security. In this scheme increase a time complexity and space complexity against the exhaustive attack and the time complexity trade off attack. This Technique realizes the confidentiality, completeness, authentication and non repudiation.

9. REFRENCES:

- KUI-HE YANG and SHI-JIN NIU, Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm, IEEE 978-1-4244-4507-3/2009
- Wuling Ren and Zhiqian Miao, A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication IEEE 978-0-7695-4046-7/ 2010
- Atul Kahate, Cryptography and Network Security, Second Edition, the McGraw-Hill Companies.
- William Stallings, Cryptography and Network Security, Prentice Hall of India Private Limited, New Delhi.