Hybrid Encryption Algorithm for Data Transmission over public network

Salini Dev P V[1], Ann Preetha Jose[2], Jesline Joseph[3]

[1] *Salini Dev P V A.P,Information Technology, Viswajyothi College Of Engg. & Technology, Kerala, India*
[2] *Ann Preetha Jose A.P,Information Technology, Viswajyothi College Of Engg. & Technology, Kerala, India*

[3] *Jesline Joseph A.P,Information Technology, Viswajyothi College Of Engg. & Technology, Kerala, India*

ABSTRACT

Abstract—To improve the data transmission over the public network is very essential aspect. Cryptography provides some methods for securing the data. For that Encryption Algorithms are used to protect the confidentiality of data. Hybrid encryption is a method used for securing the data. Hybrid encryption is a process by which combines two or more algorithms together and provides more security than a single encryption can do. This provides safe mechanism for data transmission over the network. This mechanism includes confidentiality, integrity, authentication of identity, and non-repudiation. This mechanism also provides dual protection by taking the advantages of the algorithms used, so the data transmission in the network will be more secure. Here, some hybrid encryption mechanisms are discussed; that are based on combination of 3DES and RSA algorithms and combination of AES and ABE algorithms. Encryption speed of 3DES algorithm is faster than RSA algorithm distribute key safely and easily . RSA algorithm AES overcomes the disadvantages of 3DES. It is an effective method to resolve the problem of safe transmission in Internet.

Keyword *–AES, ABE ,RSA, Safe transmission,3 DES.*

1. INTRODUCTION

To improve the data transmission over the public network is very essential aspect. Cryptography provides some methods for securing the data. For that Encryption Algorithms are used to protect the confidentiality of data. Hybrid encryption is a method used for securing the data. Hybrid encryption is a process by which combines two or more algorithms together and provides more security than a single encryption can do [8]. This provides safe mechanism for data transmission over the network. This mechanism includes confidentiality, integrity, authentication of identity, and non-repudiation [9]. This mechanism also provides dual protection by taking the advantages of the algorithms used, so the data transmission in the network will be more secure. Here, some hybrid encryption mechanisms are discussed; that are based on combination of 3DES and RSA algorithms and combination of AES and ABE algorithms. Encryption speed of 3DES algorithm is faster than RSA algorithm distribute key safely and easily. RSA algorithm AES overcomes the disadvantages of 3DES. It is an effective method to resolve the problem of safe transmission in Internet.

Internet is an open system to public, it must face 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. Cryptography is used f or safe data transmission over the network. Cryptography is the process by which the original message is converted into some other form. This conversion of original message to cipher text is called encryption and the encrypted message is called cipher text. This process is shown in Figure1. And the reverse process is called Decryption; that is, creating the original message from the cipher text. There are different cryptographic algorithms. Cryptographic algorithms are mainly classified into

- Symmetric Encryption(Secret Key Cryptography)
- Asymmetric Encryption(Public Key Cryptography):Uses one key for encryption and another one for decryption.
- Hash Functions: Mathematical transformation is used for encryption.

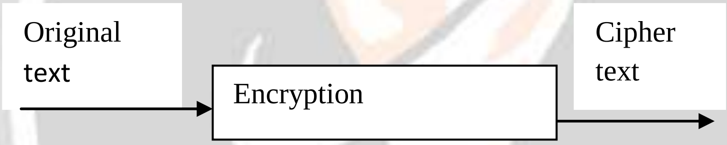


Figure1. Encryption

2. SYMMETRIC ENCRYPTION(SECRET KEY CRYPTOGRAPHY)

Single key is used for both encryption and decryption. Different algorithms are used for encryption by single key. Some of them are:

2.1 DES (Data Encryption Standard) Algorithm

It is a traditional encryption algorithm adopted by American government in 1976. DES algorithm uses many cryptographic technologies. It is defined that DES algorithm includes replacement, alternation and data input. And also plaintext is divided into many blocks. Each block has 64 bits and the key length is 64 bits. Only 56 bits are valid bits and the rest of 8 bits are used for parity checking. After 16 round replacements, a new 64bits data generated. At last, this 64 bits need an inverse replacement for generating the cipher text [3].

- ***Disadvantages of DES:***

Length of DES key is too short.

Distribution of key is difficult, if key lose system become worthless.

Calculation of DES is linear.

2.2 Triple-DES (3DES):

3DES is three times secure than DES. The process of 3DES is same as DES, but the operations are performed three times. It provides 112 bits for keys. This method performs three times encryption by using two different keys. Suppose two different keys are used K1, K2. K1 is used for encryption and then decrypt this with K2 and again encrypt this with K1.This process is shown in Figure2.

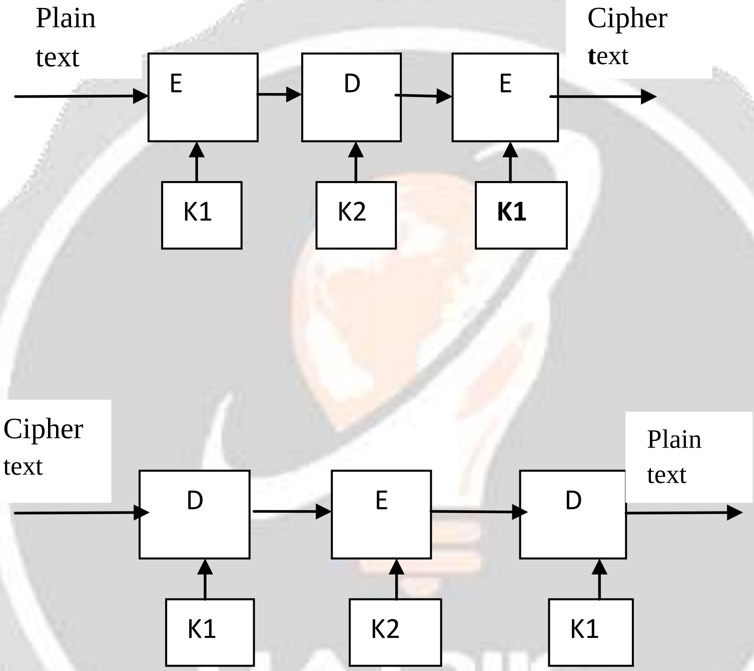


Figure2: Process of 3DES

- ***Disadvantages of 3DES:***

Computation (Encryption and Decryption) is performed 3 times than DES.

2.3 AES

Advanced Encryption Standard (AES) was adopted by US government. AES has 3 blocks 128,192,256 respectively. AES has 10 rounds for 128 bit keys,12 rounds for 192 bit keys and 14 rounds for 256 keys.

3. PUBLIC KEY ALGORITHM (ASYMMETRIC CRYPTOGRAPHY) -RSA ALGORITHM

Public key algorithm is also known as Asymmetric key algorithm. In Public key algorithm, for encryption it uses one key and for decryption it uses another key. And also Public key is open and Private key is secret. There are two uses for public key cryptography, Public key encryption and Digital signature. In public key encryption, message is encrypted with a recipient's public key. In digital signature, a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key [2].

3.1 RSA Algorithm: Key distribution in RSA is easy. 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 and decryption key [4]. 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 [4].

3.2 Diffie-Hellman: After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

3.3 Digital Signature Algorithm (DSA): The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.

3.4 ElGamal: Designed by Taher Elgamal, a PKC system similar to Diffie-Hellman and used for key exchange.

3.5 Elliptic Curve Cryptography (ECC): A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

The public key algorithms are relatively computationally costly compared with most symmetric key algorithms. The difference factor is the use of typically quite large keys [2].

4. THE IDEAS AND PROCESSES OF HYBRID ENCRYPTION ALGORITHM

DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher [1]. DES and RSA represent symmetrical and asymmetrical encryption algorithm respectively. Because the mechanism is different, they have their own merit and short coming [1][5][8]. The comparison is showed as below:

1) In aspect of security, DES and RSA algorithm have strong security.

2) In aspect of encryption speed, the velocity of DES is faster than RSA algorithm [5]. Because the length of DES has 56 bits, software can enhance the speed. The calculation process of RSA algorithm has many steps such as power and mod of big integer with many bits. The speed of RSA is slower than DES. In crowed network, it is not suitable to encrypt long plaintext.

3) In aspect of key management, RSA algorithm is better than DES algorithm. Because public key is opened to outside and private key is kept by holders. The update of key is easily. However, DES needs to allocate key pair. The update of key is hard[1]. DES generates and keeps different key[5].

RSA algorithm can realize data signature and authentication. It is better than DES. RSA achieve the reliability, completeness, and non-repudiation of data transmission.

5. MODEL OF DATA SAFE TRANSMISSION BASED ON RSA AND TRIPLE DES

1) Key pair of triple DES is generated in receiver. Then it encrypts the plaintext. Using public key of receiver encrypt symmetrical key pair [5].

2) Symmetrical key and plaintext which are encrypted by dispatcher are sent to receiver through open network. Encrypted digital abstract is dispatched too.

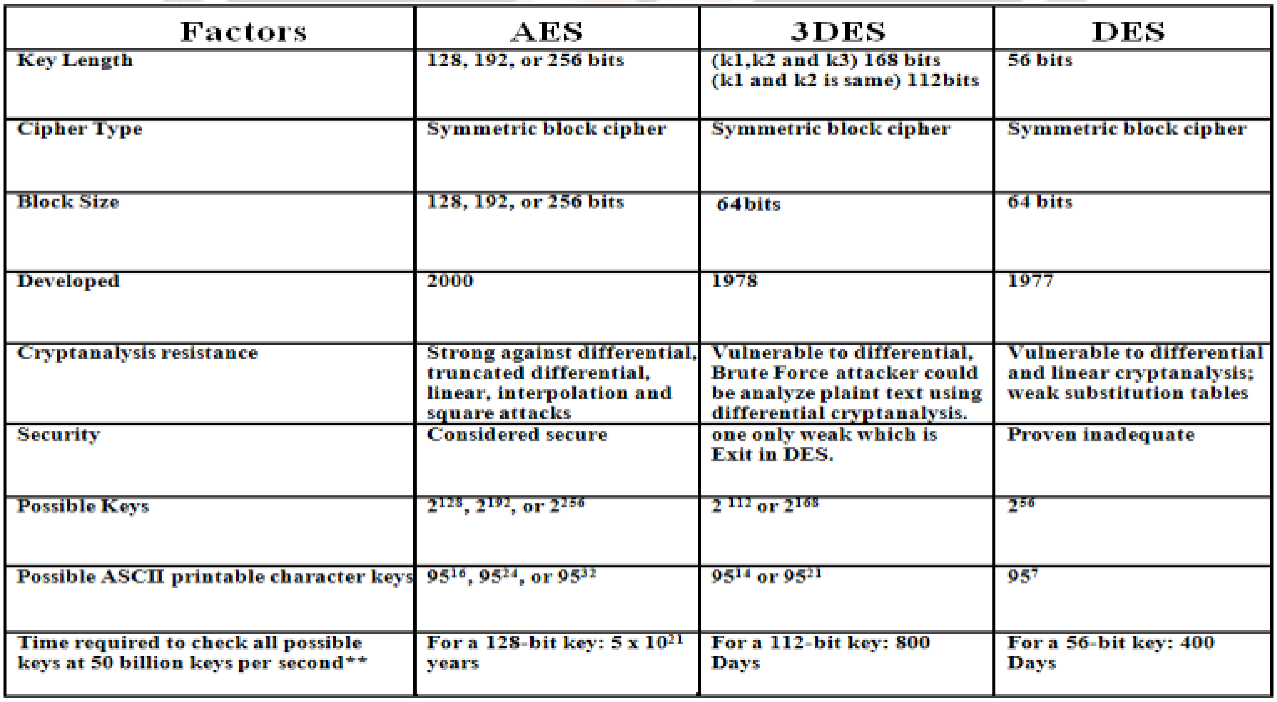
3) Receiver uses their own private key to encrypt symmetrical key pair, after getting the information from dispatcher. Then receiver uses symmetrical key decrypt message which is encrypted by dispatcher. At the same time, plaintext is copied [5].

4) Public key of dispatcher encrypts digital abstract. MD5 algorithm calculates digital abstract for plaintext. The digital abstract which is from dispatcher and calculated abstract which is from plaintext are compared. If the results are same, the transmission is safe. If the results are different, the message is tampered [6].

6. COMPARISON CHART

Comparative study between DES, 3DES and AES were presented in to nine factors is shown in table1 [10].

Table 1
Comparison between AES , 3DES and 3DES.



Factors	AES	3DES	DES
Key Length	128, 192, or 256 bits	(k1,k2 and k3) 168 bits (k1 and k2 is same) 112bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192, or 256 bits	64bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, Brute Force attacker could be analyze plaint text using differential cryptanalysis.	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	one only weak which is Exit in DES.	Proven inadequate
Possible Keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5 x 10^{21} years	For a 112-bit key: 800 Days	For a 56-bit key: 400 Days

7. AES (ADVANCED ENCRYPTION STANDARD) & ABE.

By using AES large amount of data can be encrypted. And under the dual protection with the ABE and AES algorithm the data transmission will be more secure.

This system provides high security and also faster than the existing system. This system uses ABE (Attribute Based Encryption) and AES (Advanced Encryption Standard) and provides high security and faster than RSA & DES. AES is much faster than triple DES and provide more security. It provides resistance against all known attacks and ABE encryption to provide confidentiality to the data [4]. ABE is more efficient, flexible and suitable than other cryptographic techniques and may be a lightweight security solution for web services.

7.1 AES

AES the block cipher ratified as a standard by National Institute of Standards and Technology (NIST) [4] .AES is a symmetric key encryption standard adopted by U S government. The standard comprises three block ciphers, AES-128, AES-192,and AES-256 adopted from a larger collection originally published as Rijndael. Each of these block ciphers has 128 bit block size with key size of 128,192,256 respectively [4],[7]. The AES ciphers have been analyzed extensively and are used worldwide.

AES has 10 rounds for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. AES is based on a principle known as Substitution Permutation network. It is fast in both software and hardware.

7.2 ABE

ABE provides normal encryption using AES, and extra access control function. ABE is more efficient, flexible and suitable than other cryptographic techniques and may be a lightweight security solution for web services.

8. JUSTIFICATION

When login, there is a provision to generate a key for each data. The key is generated from the attributes by using ABE algorithm. And also, there is a secret key for encryption and decryption process. Using the secret key user can encrypt the secret messages using AES algorithm. Secret key is same for both sender and receiver. This system is used for encrypting the plaintext using a random AES key and then using ABE to encrypt the AES key which is included in the cipher text. SHA256, algorithm is implemented in managing code. The algorithm has been added just to support the key generation requirements of AES. Main functions are,

- Security Key Generation:
- Security Implementation using ABE
- Data conformation

9. CONCLUSION

Data safe transmission bases on triple DES and RSA algorithm and with ABE & AES. It makes use of the advantage of triple DES which has the high encryption speed for plaintext. It also develops the merit of RSA which manages the key easily. ABE provides normal encryption using AES, and extra access control function. These mechanisms realize the confidentiality, completeness, authentication and nonrepudiation. It is an effective method to resolve the problem of safe transmission in Internet.

ACKNOWLEDGMENT

This paper is supported by the science and technology research program of Hebei province (042135117).

REFERENCES

[1] Wuling Ren, Zhiqian Miao,(2010),'A Hybrid Encryption Algorithm Based on DES And RSA in Bluetooth Communication', Proceedings IEEE Conference on Modeling, Simulation and Visualization Methods,Vol.5,pp.221225.

[2] IEEE 1363: Standard Specifications for Public-Key Cryptography .

[3] H. G. Zhang, Y. Z. Liu, "Evolution password and DES evolution research," Chinese Journal of Computer, vol 12, no. 2, pp. 1678-1684, September 2003.

[4] B. Yang, Modern Cryptography[M], Beijing: Tsinghua University Press, 2006

[5] Kui-He Yang, Shi-Jin Niu,(2009), 'Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm', International Conference on Computational Intelligence and Software Engineering,Vol.7, pp.1 – 4.

[6] S. P. Wang, Y. M. Wang, "Digital signature scheme based on DES and RSA," Journal of Software, vol 14, no. 1, pp. 146-150, June 2003.

[7] Douglas R. Stinson, Cryptography Theory and Practice[M], Beijing: Publishing House of Electronics Industry, 2002.

[8] Weber, S.G.: A Hybrid Attribute-Based Encryption Technique Supporting ExpressivePolicies and Dynamic Attributes. Information Security Journal: A GlobalPerspective 21(6), 297{305 (2012).

[9] K. C. Lu, Computer Cryptography-data Confidentiality and Security in Computer Network, Beijing: Tsinghua University Press, 2000.

[10] New Comparative Study Between DES, 3DES and AES within Nine Factors Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani.