A Survey of Integrated Algorithm for Secure Transmission of Data

Jyoti Sahu
CS Final Year, Sanghvi Institute of Mangement & Science, Indore
RGPV, Bhopal
jyotisahu27@gmail.com

Priyanka Kaushal
CS Final Year, Sanghvi Institute of Mangement & Science, Indore
RGPV, Bhopal
priyankakshl2410@gmail.com

Ankita Soni
CS Final Year, Sanghvi Institute of Mangement & Science, Indore
RGPV, Bhopal
rakhisoni481990@gmail.com

***Abstract* – Organizations in both public and private sectors have become increasingly dependent on electronic data processing. Protecting these important data is of utmost concern to the organizations and cryptography is one of the primary ways to do the job. This causes a major concern for privacy, identity theft, electronic payments, corporate security, military communications and many others. In the internet for safely data transmission a combinational approach using RSA and Diffie Hellman key exchange is implementing because RSA distribute key safely and privately and Diffie Hellman provide fast transmission. Through comparing the digital signature which is transmitted by dispatcher and digital signature result of plaintext which is got by receiver through MD5 algorithm, data security can be guaranteed. This mechanism realizes the confidentiality, completeness, authentication and non repudiation. It is an effective method to resolve the problem of safe transmission in Internet.**

***Keywords* – Public Key, Message Digest, Confidentiality, Authentication.**

I. Introduction

The encryption algorithm is the core of database encryption, the scrambled text produced from a good encryption algorithm should be the frequency balanced, the stochastic not heavy code rule, the cycle very long and also not impossible to have the redundant phenomenon. Secrets Stealer will be very difficultly for success through analyses the characteristic of scrambled text frequency and heavy code. At the same time, the algorithm must adapt the database system characteristic, the response of encryption and deciphering, especially the deciphering, should be rapid in particular. Selecting suitable encryption algorithm for the database encryption should satisfy following several requests: [1] because the data preservation time is relative long, the request of algorithm intensity for database encryption is first. [2] because the data quantity is big in the database, and the most massive use way of data is the stochastic visit, therefore the request of encryption and decipher efficiency is high, cannot cause the large scale drop of database system perfonnance. [3], the definite orders and the scrambled text length should be as far as possible equal or at least quite, because the database organizational structure cannot have big change for the database management system after encryption. [4], the database encryption granularity should be each record field data. It will lead the key repeatedly used if the document or lists used as the unit to carry on the encryption, thus the cryptographic system the reliability will reduces or unable to use for the excessively long time of encryption and deciphering. [5] encryption algorithm ought to be able directly to carry on the encryption to the record field, regardless of the database is the relations, level. [6] the key management mechanism should be more flexible and finn because the time limit is long and key complex.

II. Classification of the Secure Transaction Methods

Diffie Hellman key exchange algorithm:

Diffie-Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature: A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Message digest: The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivets in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a hexadecimal number, 32 digits long.

Pseudo random number generator: A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRNG's state, which includes a truly random seed.

RSA algorithm: A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

For implementing the data safe transmission in Internet, a safe transmission mechanism which base on RSA and Deffie Hellman key exchange algorithm is put forward The mechanism makes full use of advantage of Deffie Hellman and RSA. RSA algorithm distribute key safely and easily. Digital abstract algorithm MD5 is adopted in this mechanism. Through comparing the digital signature which is transmitted by dispatcher and digital signature result of plaintext which is got by receiver through MD5 algorithm, data security can be guaranteed. This mechanism realizes the confidentiality, completeness, authentication and non repudiation. It is an effective method to resolve the problem of safe transmission in Internet.

III. Proposed System

In the Integrated security algorithm we use existing algorithms and combine them to create a more powerful security algorithm.

The working of integrated security algorithm defined as:

- The sender and receiver for data transmission first exchange key with the help of Diffie Hellmen key exchange algorithm
- To encrypt the message RSA algorithm is used. This algorithm is in use PRNG for generating random number.
- The MD5 is used to provide more security to encrypted data.
- Now output of MD5 is added with encrypted data and sent to the receiver.
- Receiver decrypts the message and gets the actual data which is send by sender.

Algorithm:-

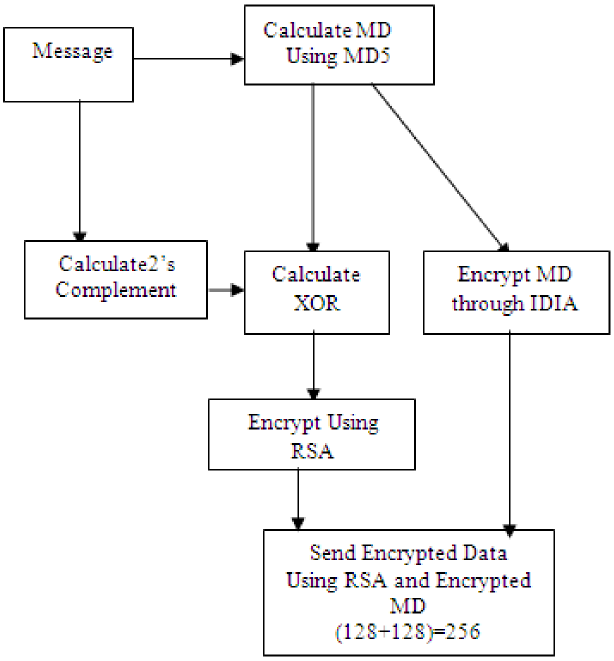
At Sending Side:

Steps

1: Find MD of 128 bit of data which you want to send
2: Calculate 2's complement of data which you want to send
3: Calculate XOR of 2's complement of data and MD
4: Encrypt the resultant data of the above step through 128 RSA
5: Apply IDIA to Encrypt the MD of the data
6: Use Deffie Hellman to exchange IDIA Key
7: Send 256 bit (send encrypted data using RSA [128] and encrypted MD [128] using MD5).

(Only 256 bit for every 128 bit data or send encrypted MD only ones for a session)

Block Diagram of System
Sending Side



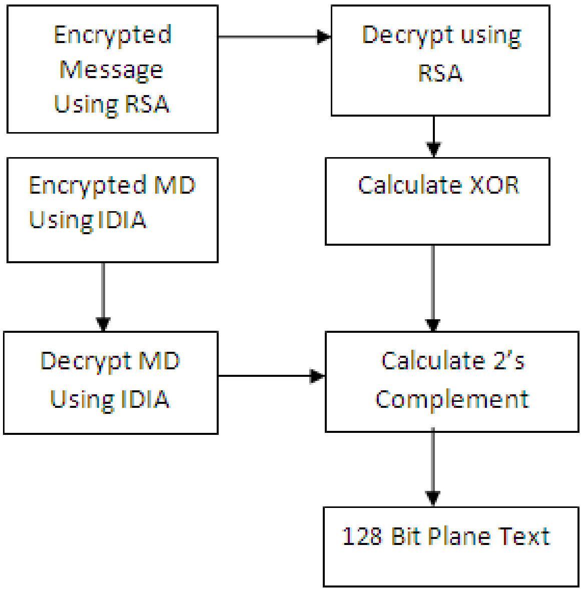
At Receiving Side:

Steps

1: Get IDEA Key Through diffie Hellman
2: Decrypt MD using IDEA
3: Decrypt data through RSA
4: Take XOR with decrypted data and decrypted MD
5: Take 2's Complement of resultant

This algorithm applied on the both sending and the receiving side and then we get the efficient method for the encryption and decryption.

Block Diagram of System
Receiving Side



IV. CONCLUSION

The conclusion is that many methods are applied for the encryption of the data and decryption of the data. But this paper defines the efficient approach for the data encryption and decryption with the use of the privately protected public key cryptography. When RSA and the Diffie Hellman approach is generally used but this method given in this paper is also have

REFERENCES

[1] Zheng Hu. Network and Information Security [M]. Peking: Tsinghua University Pres, 2006.

[2] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007 more complex and more valuable. The security ofithm suggested in this paper is more than other methods.

[3] Suri, P. R.; Rani, S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon, 2008.

[4] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos[J]. Microelectronics and Computer, 2005, 7: 25-28.

[5] Falk A. The IETF, the IRTF and the networking research community[C].Computer Communication Review, v35, n5, Oct. 2005:6970.

[6] Yaniv Shaked, Avishai Wool. Cracking the Bluetooth P[C]. 3rd USEN IX/ ACM Conf. Mobile Systems, Application and Services (MobiSys). Seattle , WA , J une 2005 :39250.

[7] 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.

[8] Y. Z. Wang, X. F. Liao, "Cipher system implement and intrusion tolerance mechanism," Computer Science, vol 7, no. 2, pp. 167-171, August 2007.

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

[10] Y. X. Xu, Java Security Program Example, Beijing: Tsinghua University Press, 2003.

AUTHOR'S PROFILE

Jyoti Sahu

belongs to Indore her date of birth is 27th Feb 1992 and pursuing B.E. degree in Computer Science Engineering from Sanghvi Institute Of Management & Science, Indore (M.P.) India from Rajiv Gandhi Prodhyougiki Vishwavidhyalaya, Bhopal(M.P.) India. Author's passing Year is June 2013. Her research interest includes computer networking and network & web security.

Priyanka Kaushal

belongs to Indore and her date of birth is 24th Oct 1991. Author is pursuing Bachelor of Engineering in Computer Science &Engineering from Sanghvi Institute of Management & Science, Indore (M..P.) from Rajiv Gandhi Prodhyougiki Vishwavidhyalaya, Bhopal (M.P.) India. Her research interest includes computer network & web security. Author's passing out year is 2013.

Ankita Soni

belongs to Indore and her date of birth is 4th Aug 1990. Author is pursuing Bachelor of Engineering in Computer Science &Engineering from Sanghvi Institute of Management & Science, Indore (M..P.) from Rajiv Gandhi Prodhyougiki Vishwavidhyalaya, Bhopal(M.P.) India .She takes interest for research in network & web security. Her passing year of B.E. is 2013.