A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman

Shilpi Gupta and Jaya Sharma
Department of Computer Science & Engineering
Amity School of Engineering & Technology
Amity University, India
sgupta5@amity.edu,
jsharma1@amity.edu

***Abstract* - Internet and Network applications have seen a tremendous growth in the last decade. As a result incidents of cyber attacks and compromised security are increasing. This requires more focus on strengthening and securing our communication. One way to achieve this is cryptography. Although a lot of work has been done in this area but this problem still has scope of improvement. In this paper we have focused on asymmetric cryptography and proposed a novel method by combining the two most popular algorithms RSA and Diffie-Hellman in order to achieve more security.**

Keywords- RSA, Diffie-Hellman, Encryption, Public Key, Data Encryption

I. INTRODUCTION

One of the most important techniques to secure communication in the presence of third party is cryptography. The 4 main requirements of cryptography are: to maintain confidentiality, data integrity, authentication and non-repudiation from unauthenticated users. Distributed Cryptography involves distribution of keys and encryption of data using this key. This encrypted data is sent over the public network. The secret key is shared among set of users so that the intended recipient can decrypt the data.

Encryption is the process of conversion of data (called plain text) into an unreadable form (called a cipher text), this cipher text cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the people who are authorized to read that data [3]. There exist many encryption algorithms that are widely used for information security. They can be categorized into symmetric (private) and asymmetric (public) key encryption. In practice, in order to achieve the optimal efficiency, the symmetric key algorithms and public key cryptography algorithms are generally combined together. Also Public-key cryptography can be used with secret-key cryptography to get the best of both worlds. Thus in this paper we have proposed a hybrid cryptographic algorithms by a combination of RSA and Diffie-Hellman. This combined approach is intended to get security advantage of public key system and speed advantage of secret key system.

II. ASYMMETRIC CRYPTOGRAPHY

In Asymmetric cryptography a pair of keys is used to encrypt and decrypt a message so that it is transmitted securely. Initially, a network user receives a public and private key pair from a Certificate Authority. The process of encryption using asymmetric cryptography can be explained by following steps -

- Use a key (public key) to encrypt a message.
- Another (private key) to decrypt a message.
- Private Key known to owner and used only by owner.

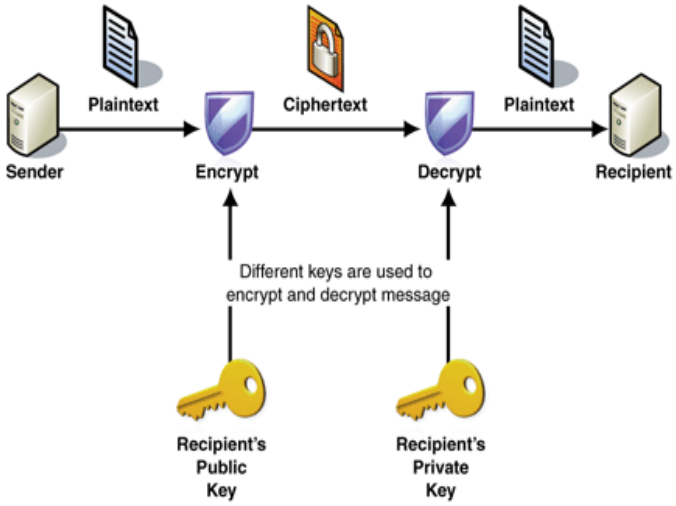

Figure 1: Asymmetric Key Encryption

The advantage of using asymmetric key encryption is that it provides better key distribution and scalability in comparison of symmetric systems. RSA, Elliptic Curve Cryptosystem (ECC), Diffie-Hellman, El Gamal, Digital Signature Algorithm (DSA), Knapsack are some of the standard Asymmetric Key Algorithms.

978-1-4673-1344-5/12/$31.00 ©2012 IEEE

III. RSA ALGORITHM

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs, including Pretty Good Privacy (PGP). RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It involves three steps: key generation, encryption and decryption It is still widely used in electronic commerce protocols, and is believed security depends on the difficulty of decomposition of large numbers [4].

Steps of Algorithm for Key Generation:

1. Choose two distinct prime numbers P and Q.
2. Calculate N = P x Q. (n is used as mod for both the public and private keys)
3. Select the public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q -1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1.
5. For encryption, calculate the cipher text CT from the plain text PT as follows: CT = PTE mod N.
6. Then send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows: PT = CTD mod N.

This algorithm is based on the theory of Prime Numbers and the fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large (100 or more digits) prime numbers. Real challenge in the case of RSA is the selection and generation of public and private keys.

Problems In RSA Algorithm

- If any one of p, q, e, d is known, then the other values can be calculated. So secrecy is important.
- It is important to make sure that message length should be less then bit length otherwise the algorithm will fail.
- Due to the usage of public key RSA is much slower than any other symmetric cryptosystems.
- The length of plain text that can be encrypted is limited to the size of n=p*q.
- Each time RSA initialization process requires the random selection of two very large prime numbers (p and q).

Advantages Of RSA Algorithm

- it uses Public Key encryption which means that the text will be encrypted with someone's Public Key (which everyone knows about) but only the person intended for can read it, by using their private key (which only they know about).
- Use of public key in RSA provides digital signatures that cannot be repudiated.
- Ciphering & deciphering algorithm are same.

IV. DIFFIE – HELLMAN ALGORITHM

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure Connectivity protocols on the Internet [8, 1]. In an era when the lifetime of “old” technology can sometimes be measured in months, this algorithm is now celebrating its 25th anniversary while it is still playing an active role in important Internet protocols.

DH is a method for securely exchanging a shared secret between two parties A and B over a public network and each holding public/private key to agree on a shared secret value [5] .This shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec). These protocols will be discussed in terms of the technical use of the DH algorithm and the status of the protocol standards established or still being defined.

Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network

Steps of this algorithm are as:

1. Taking two numbers “P” and “G” “P” is a large prime number “G” is called the base.
2. Picks a secret number “A” as first secret number = A, then picks another secret number “B” as second secret number = B.
3. Computes first public number X = GA mod P, and public number = X. Then computes second public number Y = GB mod P, and public number = Y.
4. Exchange their public numbers.
5. First knows P, G, A, X, Y, Second knows P, G, B, X, Y.
6. Computes First session key as KA = YA mod P OR KA = (GB mod P)A mod P OR KA = (GB) A mod P OR KA = GBA mod P.

7. Computes second session key as KB = XB mod P OR KB = (GA mod P)B mod P OR KB = (GA) B mod P OR KB = GAB mod P.
8. Fortunately for Both by the laws of algebra, First session key "KA" is the same as Second session key "KB", or KA = KB = K.
9. Know we have both the secret value as "K".

Advantages Of Diffie Hellmen Algorithm

- No known successful attack strategies until now, so it is secure.
- Diffie-Hellman protocol generates a "shared-secret"-an identical cryptographic key shared by each side of the communication.

Problems In Diffie Hellmen Algorithm

- It is easily susceptible to man-in-the-middle attacks.
- The algorithm cannot be used to encrypt messages.
- There is also a lack of authentication.
- The computational nature of the algorithm could be used in a denial-of-service attack very easily.

V. PROPOSED HYBRID ALGORITHM

RSA algorithm is used as Public key cryptography method. It is widely used in Electronic commerce protocol .It has a public key and private–key. Public key is known to everyone and used for encryption and Private Key is used for decryption. The RSA algorithm can be used for both public key encryption and digital signatures **[8**]. It is based on the theory of Prime Numbers. Its security is based on the difficulty of factoring large integers. The amount of time it takes to factor a number of x bits is asymptotically the same as the time it takes to solve a discrete log over a field of size x bits **[7].** It is the world's most popular Asymmetric Key Encryption algorithm.
Diffie Hellman algorithm is used as key exchange method that allows two parties that have no prior knowledge to each other to jointly share a secret key **[2].** DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network.

In our paper we use both RSA and Diffie- Hellman for providing more security.

Steps of this algorithm are as

1. Choose two large prime numbers P and Q.
   a. Calculate N = P x Q.
   b. Select public key (i.e encryption key) E such that it is not a factor of (P – 1) and (Q -1).
   c. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1
   d. Suppose R, S and G is automatic generated prime constants.
   e. And put the value of E and D from above as secret number such that A=E and B=D.
2. Now calculate following as public number
   $X = G^A \bmod R$
   $Y = G^B \bmod R$
3. Calculate session key with formula
   $K_A = Y^A \bmod R$ or $K_A = (G^B \bmod R)^A \bmod R$ or $K_A = (G^B)^A \bmod R$ or $K_A = G^{BA} \bmod P$.
   $K_B = X^B \bmod R$ or $K_B = (G^A \bmod R)^B \bmod R$ or $K_B = (G^A)^B \bmod R$ or $K_B = G^{AB} \bmod R$.
   Such that $K_A = K_B = K$.
4. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT

Firstly to use RSA each user must (privately) choose two large random numbers P and Q to create his own encryption and decryption keys. These numbers must be large so that it is not computationally feasible for anyone to factor N = P*Q **[6].** Next step (b & c) is to generate E and D. After this we put E and D as inputs A and B to Diffie-Hellman and compute XA and XB , through which we generate session key KA and KB such that KA = KB = K. Then we XOR our input Plain text with the session key (K) for Encryption or to produce Cipher text and for Decryption again XOR Cipher text with session key (K) to produce original Plain text.

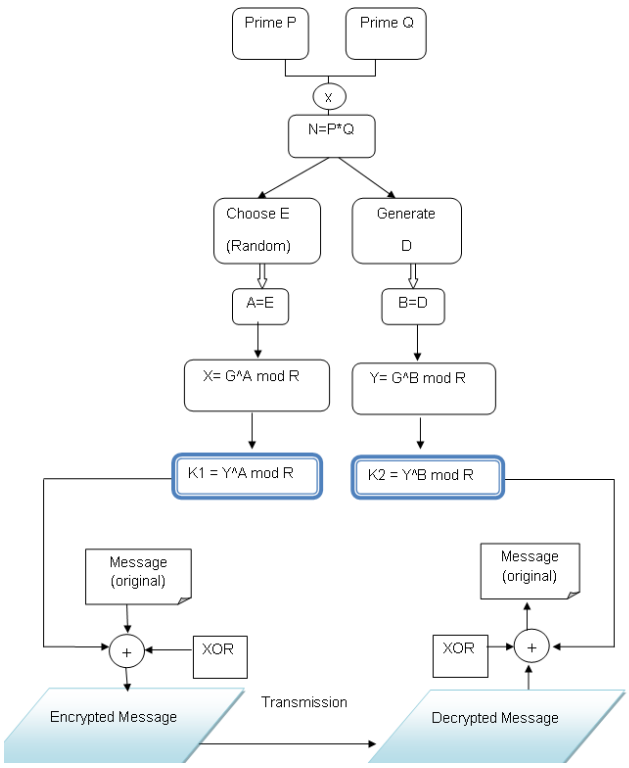

Figure 2: A Hybrid RSA & Diffie-Hellman

VI. RESULTS

The RSA keys were taken as input to Diffie Hellmen in this Implementation. The required keys are generated by the main program. A GUI was developed using java Applet. It provides options to input a user message and to upload a file.

In this approach the Diffie Hellman is not only used for the key generation but also for the generation of more secure cipher text. Generation of prime number for both RSA and Diffie is not all easy, so to guess that number and find out the key is impossible.

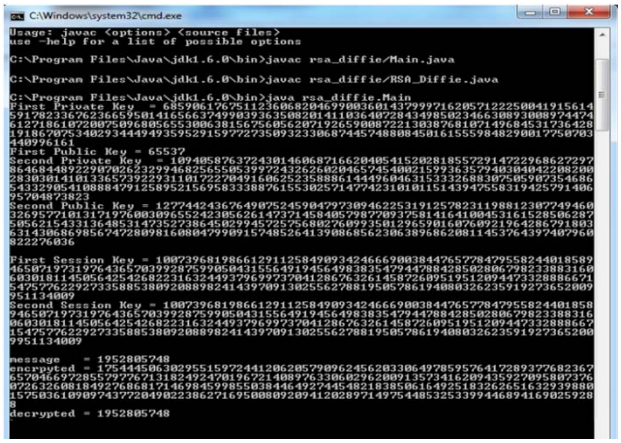

Figure 3: Key Generation

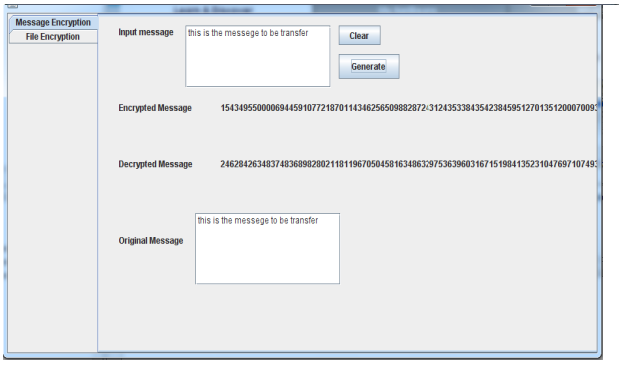

Figure 4: Encrypted & Decrypted Message

VII. CONCLUSION AND FUTURE SCOPE

The proposed approach will be of great use for the secure communication. It will be easy for user to send and receive messages and files which are the most confidential to them. On a long run, this will prove to be of immense help in security services and encryption technique. Presently, the usability of proposed Algorithm is demonstrated with very few concept and ideas which in future can be expand. The efficiency in terms of time complexity can be revised for better working of algorithm. The key size for encryption and decryption purpose can be reduces further. Currently the Algorithm is used for encryption and decryption purpose only. Further it can be used for digital signature generation.

REFERENCES

[1]. Vishal Garg, Rishu, Improved Diffie-Hellman Algorithm for Network Security Enhancement, Int.J.Computer Technology & Applications, Vol 3 (4), 1327-1331

[2]. William Stallings, Cryptography and Network Security-Principles and Practice, fifth Edition, Pearson publication.

[3]. Atul Kahate, Cryptography and Network Security, fourth Edition, Tata McGraw-Hill.

[4]. Xin Zhou, Xiaofei Tang, Research and Implementation of RSA Algorithm for Encryption and Decryption, 2011 the 6th International Forum on Strategic Technology. DOI: 10.1109/IFOST.2011.6021216

[5]. Emmanual Bresson, Dynamic group Diffi-hellman key exchange under standard assumption, Proceeding of EUROCRYPT, LNSC 2332, page no. 321-336, 2002.

[6]. R.L. Rivest, A. Shamir, and L. Adleman , A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 1978, Volume 21, Page no.120—126

[7]. Mykola Karpinskyy, Yaroslav Kinakh, Reliability of RSA Algorithm and its Computational Complexity, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 8-10 September 2003, Lviv, Ukraine

[8]. David A. Carts, A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols SANS Institute Reading Room Site http://www.sans.org/reading_room /whitepapers/vpns/review- Diffie-hellman-algorithm-secure-internet-protocols_751