ISSN:0975-9646



# Hybrid cryptography technique using modified Diffie-Hellman and RSA

Shyam Deshmukh[#1], Prof.Rahul Patil[*2]

[#1] *ME Computer Department of Computer Engineering PCCOE, Savitribai Phule Pune University Pune 411044 Pune,India*

[#2] *Assistant Professor,Department of Computer Engineering PCCOE, Savitribai Phule Pune University Pune 411044 Pune,India*

***Abstract*— Diffie-Hellman is public key based symmetric key algorithm used for secret key sharing between two parties over public communication channel. Diffie-Hellman is weak when there is man in middle attack done by eavesdropper. Diffie-Hellman algorithm is not provide authentication. Security of Diffie-Hellman cryptography system completely depends upon random prime number selected by user. Finding private key after accessing public key and prime number p is logarithmic problem to solve. Diffie-Hellman is modified to provide authentication and avoid primitive root generation step to achieve speed and authentication to avoid key exchange with unauthenticated user.RSA is cryptography system based on asymmetric key cryptography concept. Security of RSA is depend upon prime factorization of integer value n which globally known to everyone in system. In this paper hybrid cryptography system is proposed to achieve secret message exchange. RSA uses random prime numbers P and Q which after multiplication , value N is shared to other side of communication.**

**Security of RSA is depend upon prime factorization of N. Newly proposed algorithm secretly generate value of N so that security level is increased in new RSA based cryptography system.**

*Keywords*— **Diffie-Hellman Key exchange, RSA algorithm, Symmetric key cryptography, secret key.**

## I. INTRODUCTION

In history of cryptography science, initially there was symmetric key cryptography concept invented. Later on asymmetric key cryptography came into existent, which work on basis of public and private keys. In symmetric key cryptography ,only one key used at both side while in asymmetric cryptography, public and private keys are used for encryption and decryption of message respectively. Diffie-Hellman is used while symmetric key cryptography for sharing secret key which is used for encryption of message for that particular session.RSA is asymmetric key cryptography system which uses public key and private key for encryption and decryption process respectively. In this work, hybrid cryptography method is proposed to deploy the cryptography system properly. Once In RSA cryptographers panel on TED channel, Whitefield Diffie, Ronald Raviset, Adi Shamir and Dan Boneh discussed that security of algorithm is depends upon proper deployment of algorithm with keeping the security of algorithm new approach is proposed which improve the deployment of algorithm and uses hybrid cryptography technique. This paper contains, section 2 is about related work. Section 3 includes original Diffie-Hellman and RSA algorithm. Section 4 contains proposed algorithm and section 5 is discussion about proposed technique which is conclusive remark of the paper.

## II. RELATED WORK

In literature survey, Diffie-Hellman algorithm is further modified by Xun Yi, San Ling, and Huaxiong Wang for password based authentication and key exchange protocol[1].This protocol is work in three phases. Initialization ,Registration and Authentication. Bruno Blanchet proposed one key exchange protocol which is based on password authentication. In this paper CryptoVerif tool is used to proof of password based authentication.[2]. The public key remains constant for large period of time and is used by everyone wishing to set up a shared secret key with other. Note that the public key should be authenticated in some way (e.g. by Bob's signature [3] . There is contradiction that The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms means calculating primitive root is difficult logarithmic process [4] .In this work, Proposed algorithm is modified Diffie-Hellman key exchange method without using primitive root of prime number. New algorithm is complete package of encryption. In which secret key generated by modified Diffie-Hellman algorithm is not used for encryption but using this secret key two new prime numbers are generated. This new generated prime numbers are used for RSA method as it is. Dr. Vuda Sreenivasarao and Amare Anagaw Ayele proposed new algorithm based on RSA using two public keys instead of one public key pair [5] and they have found that new algorithm is more hard to break and will provide security. After selecting fixed point rather than random selection of P,Q ,and e are given in paper "Fixed points of the RSA encryption algorithm" by Andrzej Chmielowiec [6] .This paper result shows that if n is of length 1024 bit then value of fixed point is less than $4.2 \times 10^5$ . Prof Prashant Sharma, Sonal Sharma and Jitendra Yadav modified RSA scheme with help of Short Range of Natural Numbers. Author claimed that security is increased with short range of natural number in RSA cryptography[7]. In this paper, initially two large prime number P and Q also selected and two additional short range numbers selected after that. Results shows that due to short range natural number selection and applying in algorithm security level is increased. Assad Ibraheem Khyoon published his modified scheme with RSA

algorithm . Assad proposed new algorithm which uses P ,Q and one more prime number Z for calculation of phi(n) function. Assad claimed that his algorithm is provide security against eavesdroppers attacks. In this paper , [8] various possible attacks are mentioned such as relation to factoring, small encryption exponent b, small decryption exponent a, forward search attack. New proposed algorithm is to change the method of selection of initial prime numbers p and q in RSA. Which are secretly generated at both side so that further risk of sharing values of keys on channel is reduced. Both the user secretly generate public, private key pair which can be used for encryption and decryption respectively. This newly generated algorithm is completely hybrid because which uses symmetric as well as asymmetric key approach.

## III. Diffie-Hellman Key Exchange Algorithm and RSA algorithm

Following section describe Original Diffie-Hellman key Exchange algorithm and RSA algorithm.

### *A. Diffie Hellman algorithm*

If user A and user B are communicating each other on public communication channel using Diffie-Hellman secret key exchange.

1. Global Public Elements
   $P$ prime number.
   g such that $g < P$ and g , a primitive root of $P$
2. User A Key Generation process
   Select private $XA$ , such that $XA < P$
   Calculate public YA as
   $YA = g^{XA} \bmod P$ .. (1)
3. User B Key Generation process
   Select private XB such that $XB < P$
   Calculate public $YB$ as
   $YB = g^{XB} \bmod P$ ..... .....(2)
4. Generation of Secret Key by User A using private key
   $Ka = YB^{XA} \bmod P$ ..... (3)
5. Generation of Secret Key by User B using private key
   $Kb = YA^{XB} \bmod P$ ..... (4)

Where Ka and Kb at user A and user B are same. In this way secret key is shared between user. Which is secret key valid only for that particular session? If user wants to communication after this session then new prime number, primitive root required and in this way security is achieved.

### *B. RSA algorithm*

Steps of RSA algorithm as follows.

1. Choose P and Q any random prime numbers.
2. Compute $N = P \times Q$ . .....(5)
3. Compute
   $\varphi(N) = (P - 1) \times (Q - 1)$ .....(6)
4. Choose e such that $1 < e < \varphi(N)$ and e and n are co prime.
5. Compute a value for d such that $(d \times e) mod\ \varphi(N) = 1$
6. Public key is $(e, N)$
   Private key is $(d, N)$
7. The encryption of m is
   $c = m^e mod\ N$ .....(7)
8. The decryption of
   $c$ is $m = c^d\ mod\ N$ .....(8)

In short , RSA selects two random prime which are used for calculation of N and public key e that is pair and private key pair. Here public keys are used to encrypt message and private keys are used to decrypt the message.

## IV. Proposed Hybrid Algorithm

New proposed hybrid algorithm divided into two parts. First part is based on modified Diffie-Hellman key exchange. Second part uses RSA approach to encrypt and decrypt the message but both side two keys are generated with RSA approach and keys are called as sender key for encryption of message and receive key to decrypt incoming message.

### A. *Secret key generation*

Secret key generation is modified Diffie-Hellman algorithm.

Steps are as follows

1. User A Generates Random Prime Number P
   P prime number generated at user A
   User A make P as $P1 = P + P$ (that is twice P)
   And send to user B.
2. User B Generates Random Prime Number
   User B receives Number P1 and calculates
   $P = P1/2$
   Q prime number generated at user B
   User B make Q as $Q1 = P + Q$ (that is add with P)
   And send to user A.
3. User A
   Receive number from user B
   and subtract P from Q1
   User A get $Q = O1 - P$
   User A send this value of Q1 back to Q
4. User B Authenticate and Send Public key to user
   A receive value of Q1
   Q' = Q1-P
   Compare value with Q
   If Q==Q' then go ahead.
   Select Radom Private Prime Number Pb.
   If above value Q matches then User B generate this public key
   $PubB = P^{Pb} mod\ Q$
   PubB is sent to User A
5. User A Receive Public key of User B and generate own public key
   PubB is received.
   Select random prime number as private key Pa
   $PubA = P^{Pa} mod\ Q$
   pubA is sent to user B

6. User B Receive Public key of User A and Secret Key Generation Process
   $SecKb = PubB^{Pa} \ mod \ Q$.....(9)
7. User A Secret Key Generation Process
   $SecKa = PubA^{Pb} \ mod \ Q$ (10)

Equation 9 and 10 are same as equation 3 and 4 but generated with modified Diffie-Hellman algorithm.

B. Sender key and Receiver key generation
   Sender key : Key will be used for encryption.
   Receive key: Key will be used for decrypt received messages.
   8. Calculate new P
      For user A
      $Pnew = P \times SecKa$….[ P is value of P from step 1 in part A and secKa is from eq 10 ]
      Find next prime of Pnew and which is new value of P at user A P = nextPrime(Pnew) ……(11.a)
      For user B
      $Pnew = P \times SecKb$ … ( secKb is from eq 9)
      Find next prime of Pnew and which is new value of P at user B P = nextPrime(Pnew) ……(11.b)
      Here both equation 11.a and 11.b will be same value because secret values are same.
   9. Calculate new Q
      For user A
      $Qnew = Q \times SecKa$…. [Q is value of Q from step 2 in part A and secKa is from eq 10 ]
      Find next prime of Qnew and which is new value of Q at user A Q = nextPrime(Qnew) ……(12.a)
      For user B
      $Qnew = Q \times SecKb$ (SecKb is from eq 9)
      Find next prime of Qnew and which is new value of Q at user B Q = nextPrime(Qnew) ……(12.b)
   10. Calculate value of N and φ(N)
       N = P * Q ……..(13)
       φ(N) = (P - 1) * (Q- 1) .. (14)
   11. Choose e such that 1 < e < φ(N) and e and N are co prime
   12. Compute a value for d such that $(d \times emod \ \varphi N = 1$
   13. Sender key is $(e, N)$
       Receive key is $(d, N)$
   14. The encryption of m is
       $c = m^e mod \ N$ .....(15)
   15. The decryption of *c is*
       $m = c^d \ mod \ N$ .....(16)

This is complete process of hybrid cryptosystem. In this process equation 15 and equation 16 are encryption and decryption process using sender key and receiver key respectively.

NextPrime(n) is a algorithm which calculate next prime number of n.

## V. DISCUSSION

The proposed algorithm is secure and detail process of cryptosystem. It is easy to understand and more secure as complexity of algorithm is logarithmic problem to solve. Security of RSA is depend on prime factorization of N. If eavesdropper successfully prime factor of N then security is compromised. Again value of generated public keys needs to know at sender how to get it to sender? For that public key distributor is needed. Proposed algorithm authenticate user as shown is First part of algorithm by exchange value of random P and Q. Then generate secret key at both side. Secret keys not known or not sent over communication channel so eavesdropper has no chance to get value of secret key. Secret key is multiplied to P and hence new P will be not identifiable to attacker though value of P get compromised. This value of P and Q are generated secretly at user side and this valued are not shared through communication channel so we claim that proposed method is more secret than original RSA. Cons of Proposed algorithm have extra steps which mix symmetric key and asymmetric key cryptography. Time required for this integration steps is disadvantageous of this proposed method. But we can achieve better security

## VI. CONCLUSION

Proposed algorithm is secure because which encrypt and decrypt message with secretly generated sender key and receiver key which is known to sender and receiver. Two level of security is implemented. Algorithm is based on hybrid cryptography as it uses asymmetric that is sender and receiver key and symmetric key that is both the user A and use B uses same key pair for encryption and decryption.

## REFERENCES


[1] Xun Yi, Ling, Hoaxing Wang, *Effiecient two-server password-only authenticated key exchange*, IEEE transactions on Parallel and Distributed systems, 1973-1982, Sept 2013.

[2] Bruno Blanchet, *Automatically verified mechanized proof of one encryption key exchange/ .CNRS ,Paris France* IEEE, 25th Computer Security Foundations Symposium,327-339,2012.

[3] Raphael C.-W. Phan, *Fixing the integrated Diffie-Hellman-DSA key exchange protocol."* VOL. 9, NO. 6, IEEE JUNE

[4] William Stallings, "*Cryptography and Network Security principals and practices*".

[5] Amare Anagaw Ayele1 Dr. Vuda Sreenivasarao, "*A Modified RSA Encryption Technique Based on Multiple public keys*" ,IJIRCCE 2013

[6] Andrzej Chmielowiec, "*Fixed points of the RSA encryption algorithm",* Elsevier 2009.

[7] Sonal Sharma,Prashant Sharma,Jitendra Yadav, "*Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm"* IJARCSSE2012.

[8] Assad Ibraheem Khyoon,*"Modification on the Algorithm of RSA Cryptography System"* 2006.