ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Enhancement in Security by improving Diffie-Hellman Algorithm

Preeti[1], Bandana Sharma[2]

[1]Haryana Engineering College, Kurukshetra University
Jagadhri, Haryana, India
preeti.bhutani99@gmail.com
[2] Haryana Engineering College, Kurukshetra University,
Jagadhri, Haryana, India
bandanasharma1@gmail.com

Abstract: *Diffie Hellman permits two users to exchange a secret key through an insecure channel & without any prior secrets. So the security has become more important. So in our proposed work we provide harder encryption with enhanced public key encryption protocol for security. Proposed diffie hellman is based on Simple 2-step Method for Computing a Shared Secret and safe prime generation. It can generate new P and G values and ability to use Known Primes from RFC 2409, which defines the Internet Key exchange.*
Keywords: *Diffie-Hellman Algorithm, Entropy, Histogram, floating frequency*

1. INTRODUCTION

In 1976, Whitfield Diffie & Martin Hellman discovered Diffie-Hellman Algorithm & published in "New Directions in Cryptography." Various protocols are making use of this algorithm as given below:

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Secure Shell (SSH)
- Internet Protocol Security (IPSec)
- Public Key Infrastructure (PKI)[7]

Diffie Hellman permits two users to exchange a symmetric secret key through an insecure wired or wireless channel & without any prior secrets [1].

In Diffie-Hellman cryptosystem, two parties create a symmetric session key to exchange data without having to remember or store the key to use in future. They don't have to meet to agree on the key; it can be done through the internet. [7]

1.1How the protocol works:-

When Alice and Bob need a symmetric key to communicate. Both requires to choose two numbers, first number is a large prime no., and the second number is a random number. The numbers chosen need not be confidential. These numbers can be sent through the Internet; & they can be public.

1.2 Diffie-Hellman's Key Exchange Algorithm

1. Global Public Elements: Prime number q; $\alpha < q$ and α is a primitive root of q.
2. User A Key Generation: User B Key Generation:
3. Select private X_A $X_A < q$
   Select private X_B $X_B < q$
4. Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$
   Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$
5. Calculation of Secret Key by User A: $K = (Y_B)^{X_A} \bmod q$. Calculation of Secret Key by User B: $K = (Y_A)^{X_B} \bmod q$

The result is that the two sides have exchanged a secret value. In addition, because XA and XB are private, an intruder only has the following ingredients to work with: q, a, YA, and YB. Thus, the adversary is forced to take a discrete logarithm to determine the key. For example, to figure out the private key of user B, an adversary must compute XB = dloga, q(YB). The adversary can then calculate the key K in the same manner as user B does.The security of the DH key exchange lies in the fact that, rather it is quite easy to calculate exponentials modulo q prime, but it is very difficult to calculate discrete logarithms. For large prime numbers, the latter task is considered infeasible. [6]

Secure transmission is generally realized by encryption and authentication mechanisms; encryption protects all the data during transmission while authentication guarantees procedures to install permitted devices.[3]The symmetric key for the session is K which is same for both alice and bob.[7]

Figure 1 shows how the classical diffie-hellman algorithm works. The protocol portrayed is insecure against a man-in-the-middle attack. The key exchange protocol is unresisting to such an attack because it does not authenticate the participants. This weakness can be overcome with the use of digital signatures & public-key certificates.[6]

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

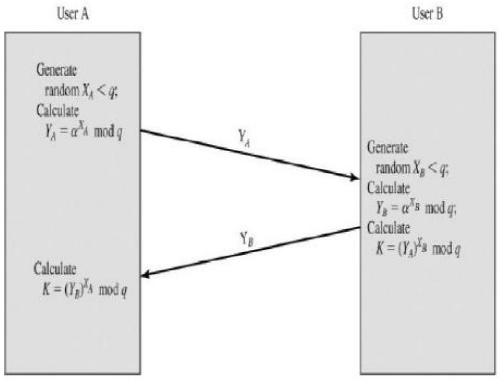

Figure1: Diffie-Hellman Algorithm

2. RELATED STUDY

In [1], P. Bhattacharya, in 2005 two modifications of DH. The very first modification is to change the domain to integer with n=2pt where Zn is still cyclic and the second modification is to change the domain to Gaussian arithmetic Z [i]. After implementing the three algorithms we found that the symmetric key size derived from the two modified algorithms is much greater than the classical one. Furthermore, attacking the two modified algorithms using Pohlig-Hellman algorithm & the same prime value p & private value a or b, needs more time than the classical one.

In [2], Ik Rae Jeong, in May 2007, provided an overview that a few integrated key exchange schemes which provide authentication using the DSA signature have been proposed in order to provide authentication to the Diffie-Hellman key exchange,. It identified that all of the previous Diffie-Hellman-DSA schemes do not provide security against session state reveal attacks. It also suggested a strong Diffie-Hellman-DSA scheme providing security against session state reveal attacks as well as forward secrecy & key independence.

In [3], Salvatore Cavalieri in 2009, deals with the problem of making secure data transmission inside Home and Building Automation environment; the data exchanged here may regard commands to actuators or private and secret information. This paper deals with this problem taking into account the KNX communication system, which at this moment, doesn't force any encryption and authentication mechanisms. A solution for data encryption & authentication will be presented & assessed, comparing it with the current state of the art.

In [4] , Eun-Jun Yoon, in 2009, proposed an efficient Diffie-Hellman-MAC key exchange scheme which provides security against session state reveal attacks as well as forward secrecy & key independence.

In [5], S. Anahita Mortazavi, in 2011,in this author proposed an efficient many-to-many group key management protocol in distributed group communication. In this protocol, members of group are managed in the hierarchical manner logically. Two type of keys are used, asymmetric & symmetric keys. In the key tree, the leaf nodes are the asymmetric keys of the corresponding group members and all the intermediate node keys are symmetric keys assigned to each intermediate node. For asymmetric key, DH key agreement is introduced. Members use codes assigned to each intermediate node of key tree in order to calculate intermediate node keys. Group members do calculate intermediate node keys rather than distributed by a sponsor member. This approach includes the features i.e. no keys are exchanged between existing members at join, and only one key, the group key, is given to rest of the members at leave.

3. PROPOSED WORK

3.1 Implementation:- I have added two functions to classical deffie-hellman and implementation in JAVA

- **Create e: -** The first step in deffie hellman key exchange to generate a shared secret key. The numBits should be twice the size of the shared secret to be generated.
- **Find K: -** The second step in deffie-hellman key exchange E is the key created by other party. Returns the shared secret (k) as an SSH1 format bignum encoded as a hexagonal string.

3.2 Proposed Algorithm

The proposed algorithm is implemented in Java JDK is 1.6. It overcomes the drawback of classical deffie-hellman algorithm.

Step1:- User select prime no. a (create two separate instance of diffie hellman object one for sender & one for receiver)

Step 2:- Enter a prime no. (sender)

Step 3:- Enter a prime no. (receiver)

Step 4:- Sender will now send p & g to receiver which are safe prime nos.

Step 5:- Receiver checks whether p is safe or not

Step 6:-Create 256 bit key at sender & reciever side using find k function

Step 7:- Perform encryption using key at sender side or decryption at receiver side

Step 8:-Write the generated key into file for analysis purpose.

4. RESULT ANALYSIS

These were the following parameter which was analyzed:-

1) ENTROPY

2) FLOATING FREQUENCY

Entropy: - Entropy is an expression of insecurity as the number of Yes/No questions which have to be answered in order to clarify a message or character. If character has a very high probability of occurrence, then its information

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

content is low. This parameter calculates the entropy of a document.

Floating Frequency: - The floating frequency of a document is a characteristic of its local information content at individual points in the document. This parameter calculates the floating frequency of a document.

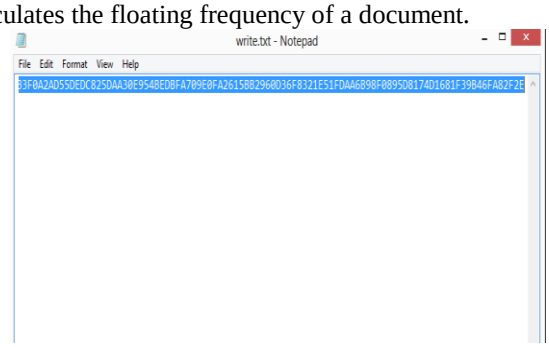

Figure 2: Secret key generated

Figure 2 shows the secret generated.

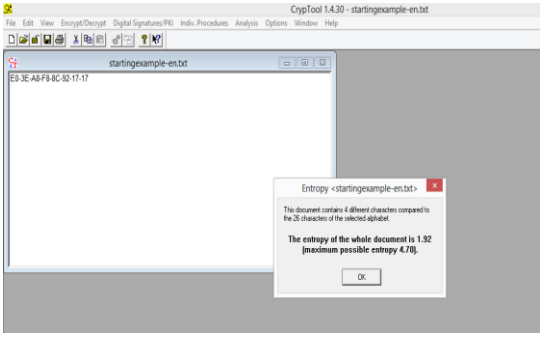

Figure 3: Entropy of classical deffie-hellman algorithm

Figure 3 shows the value of parameter entropy by classical diffie-hellman algorithm.

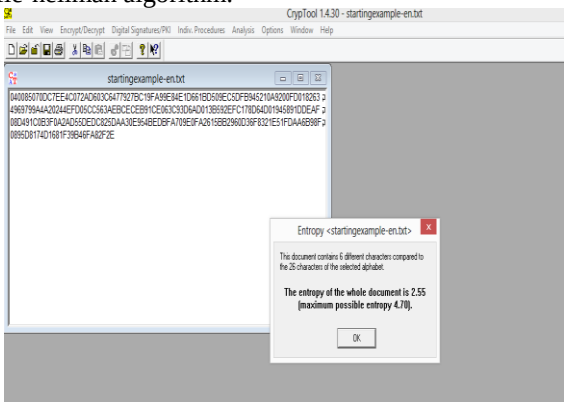

Figure 4: Entropy of proposed algorithm

Figure 4 shows the value of parameter entropy by proposed algorithm

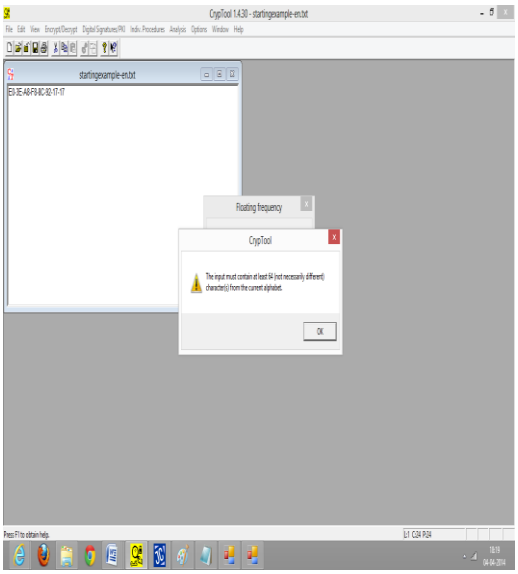

Figure 5: Floating frequency of classical deffie-hellman algorithm

Figure 5 shows the analysis result of parameter floating frequency by classical diffie-hellman algorithm.

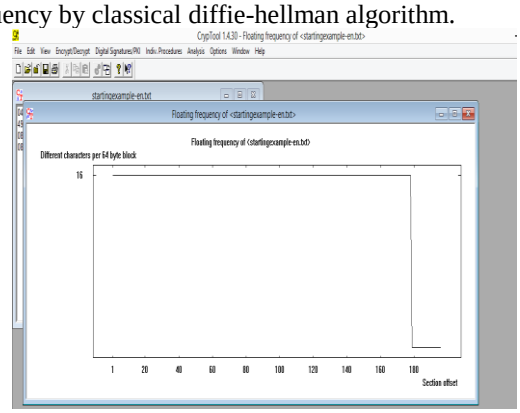

Figure 6: Floating frequency of proposed algorithm

Figure 6 shows the analysis result of parameter floating frequency by proposed algorithm

5. COMPARISON

TABLE 1: COMPARISON BETWEEN CLASSICAL & DIFFIE-HELLMAN ALGORITHM

	Classical diffie hellman	**Proposed algorithm**
Entropy	1.92	2.55
Histogram	Frequency distribution of 5 characters is shown	Frequency distribution of 100 characters is shown
Floating frequency	Input does not contain 64 characters	Different characters are found per 64 byte block

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Auto correlation	Characters does not match because input must contain at least 8 characters from the current alphabet	No. of characters matches
The N-Gram	4 common N-grams are shown	6 common N-grams are shown
Periodicity	Periodicity found	No Periodicity found

Value of Entropy in proposed algorithm increases. In proposed algorithm frequency distribution of 100 characters is shown & in classical diffie-hellman it is of 5 characters. Autocorrelation in classical diffie-hellman does not match characters whereas in proposed algorithm no.of characters matches. There are 4 common N-Grams in classical diffie-hellman and 6 in proposed algorithm. Periodicity is found in classical diffie-hellman and not found in proposed algorithm.

6. CONCLUSION

The main aim of the research is to provide better encryption algorithm and better security. Our proposed algorithm is compared with diffie hellman algorithm and the different parameters were analyzed In my work entropy increases, frequency distribution in histogram decreases, different characters are there in floating frequency, N-grams increases and periodicity is not found. This shows that our research made the key hard and enhanced the security.

REFERENCES

[1] P. Bhattacharya, M. Debbabi & H.Otrok, "Improving the Diffie-Hellman Secure Key Exchange", International Conference on Wireless Networks, Communications & Mobile Computing in 2005.

[2] I.R Jeong, Jeong ok kwon, & Dong Hoon Lee," Strong Diffie-Hellman-DSA Key Exchange", IEEE COMMUNI-CATIONS LETTERS, VOLUME. 11, NO. 5, MAY 2007.

[3] Salvatore Cavalieri & Giovanni Cutuli," Implementing Encryption & Authentication in KNX using Diffie-Hellman & AES Algorithms",in 2009.

[4] Eun-Jun Yoon, Kee-Young Yoo," An Efficient Diffie-Hellman-MAC Key Exchange Scheme, " Fourth Inter-national Conference on Innovative Computing, Information & control, in 2009.

[5] S. Anahita Mortazavi, Alireza Nemaney Pour," An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman & Symmetric Algorithm: DHSA", Inter-national symposium on computer networks & distributed systems, February 23-24, 2011.

[6] Vishal Garg, Rishu,"Improved Diffie-Hellman Algorithm for Network Security Enhancement", Int.J.Computer Tech-nology & Applications,Vol 3 (4), 1327-1331 IJCTA | July-August 2012 Avai-lable online @www.ijcta.com 1327

[7] Behrouz A. Forouzan, "Data Communi-cations & Networking", Fourth Edition, in 2008, New York:Tata McGraw-Hill