Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review Paper on Security in Diffie-Hellman Algorithm

Preeti*, Bandana Sharma
CSE& Kurukshetra University
India

Abstract— The main aim of this research is to study and analyze the different techniques used to provide better security in Diffie-Hellman Algorithm and how the hardness of key can be enhanced in Diffie-Hellman encryption Algorithm by adding some mathematical operations in current algorithm.

Keywords— Diffie-Hellman Algorithm, Diffie-Hellman Key Exchange, Classical DH,Gaussian DH, Key Size

I. 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)[15]

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.[15]

A. *How 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.

B. *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.[8]

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.[4]The symmetric key for the session is K which is same for both alice and bob.[15]

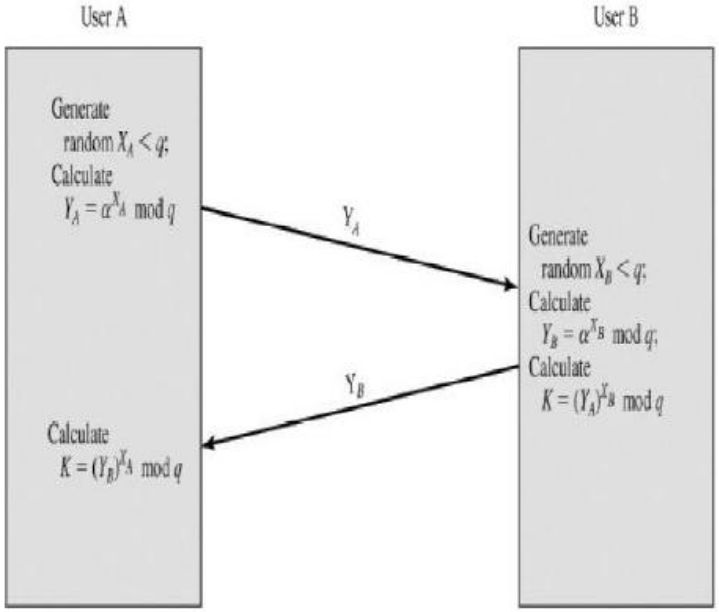

Fig.1 Diffie-Hellman Algorithm

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.[8]

II. 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 [4], 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 [5] , 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 [7], 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.

In [8], Vishal Garg, in 2012, provided harder encryption with enhanced public key encryption protocol for security & proposed work can be implemented into any of the network in order to provide better security. It enhanced the hardness in security by improving the Diffie-Hellman encryption algorithm by adding some more security codes in current algorithm.

III. COMPARISON OF EXISTING TECHNIQUES

Table1

ALGORITHM	KEY SIZE(in Bits)	TIME NEEDED To COMPUTE SECRET KEY (in msec)
Classical DH	12	20
Gaussian DH	28	40

IV. CONCLUSION

Modifying the security of Diffie-Hellman means increasing the key size. To ensure the security of various Algorithms computation of value of same symmetric key by different methods and then by applying some attack method shows the time needed to compute the symmetric key for different techniques.

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 COMMUNICATIONS LETTERS, VOLUME. 11, NO. 5, MAY 2007.

[3] Zhen Cheng, Yufang Huang, Jin Xu," *Algorithm for Elliptic Curve Diffie-Hellman Key Exchange Based on DNA Tile Self-assembly*",in 2008.

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

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

[6] Dongfang Zhang," *A New Authentication & Key Agreement Protocol of 3G based on Diffie-Hellman Algorithm*,"in 2010.

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

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

[9] Emmanuel Bresson, Olivier Chevassut, David Pointcheva & Jean-Jacques Quisquater, "*Provably Authenticated Group Diffie-Hellman Key Exchange*", in Proc. Of ACM CCS '01, ACM Press 2001.

[10] Michel Abdalla, Mihir Bellare, & Phillip Rogaway, " *DHIES: An encryption scheme based on the Diffie-Hellman Problem*", In Proc.of ACM CCS '01, ACM Press September18,2001.

[11] Jonathan C.Herzog, "*The Diffie-Hellman Key-Agreement Scheme in the Strand-Space Model*", 16th IEEE Computer Security Foundations Workshop (CSFW'03), 1063-6900/03 ,2003.

[12] Lein Harn, Manish Mehta & Wen-Jung Hsin, "*Integrating Diffie–Hellman Key Exchange into the Digital Signature Algorithm (DSA)*", IEEE COMMUNICATIONS LETTERS, VOL. 8, NO. 3, MARCH 2004

[13] Mario Cagaljm, Srdjan Capkun & Jean-Pierre Hubaux, "*Key agreement in peer-to-peer wireless networks*", Laboratory for Computer Communications & Applications (LCA) Ecole Polytechnique F´ed´erale de Lausanne (EPFL), CH-1015 Lausanne Networked & Embedded Systems Laboratory (NESL), University of California, Los Angeles (UCLA), November 2004.

[14] Raphael C.-W. Phan, "*Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol*" , IEEE COMMUNICATIONS LETTERS, VOL. 9, NO. 6, JUNE 2005.

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

[16] L. Harn, W.-J. Hsin & M. Mehta," *Authenticated Diffie–Hellman key agreement protocol using a single cryptographic assumption*", IEEE Proc.-Commun., Vol. 152, No. 4, August 2005.

