Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing the Diffie-Hellman Algorithm

Rohini[*]
CSE & Kurukshetra University,
India

Er.Meenakshi Sharma
CSE & Kurukshetra University,
India

Abstract*— The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide. Network consists communication. Communication is the medium for sending and receiving the data between two parties i.e. Sender and receiver but communication needs the security from unauthorized people. Security covers a variety of computer networks that are used in everyday. It secures the network, as well as protecting and overseeing operations being done. For more security, we use Diffie – Hellman algorithm. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. The Diffie–Hellman key exchange method permits two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.In our proposed work, we provide harder encryption with extend public key encryption protocol for security. Our proposed work provides better security and implemented in any network. We have enhanced the hardness of security by DH algorithm. The DH algorithm is improved by adding codes to the algorithm.

***Keywords*—.Diffie-Hellman (DH), Bluetooth (BT), Secure Shell (SSH), Public Key(PK),Network(NW),Private(PRVK).**

I. INTRODUCTION

Network security is the authorization of access to data in the network and administrator is managed it. Users are given ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers different types of computer networks that are used in everyday jobs conducting transactions and communications among government agencies and businesses. Networks are private i.e. within a organization, and others which may be public access. Network security involved in organizations and variety of institutions. It explains: It secures network, protecting and overseeing operation being done. The most common and simple way of protecting the network resource by assigning it a different name and corresponding password

II. DIFFIE- HELLMAN ALGORITHM

Diffie Hellman (DH) allows two parties to exchange a symmetric secret private key through an insecure wired or wireless channel. Modifying the security of DH means improving the security of the protocols that use DH. DH works under the domain of integer Zn where n = p. P and a are the two parameters of DH where p is a large prime number and a is a generator selected from the cyclic group Zn. Two principals A and B can use the DH algorithm to exchange a symmetric key. The principal A chooses a private value a, then it chooses a large random prime P and a generator a. The PK of A is (p,a, a') and the private key is a. A sends its public key to B. After receiving A's public key, B chooses its own private key b and computes its public key (p,a, ab). B sends its public key to A. Now A and B computes their symmetric key [1].

Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A generates a private key XK, calculate *YK*, and send this to user B. User B sends the acknowledged by generating a private value *XL* calculating *YL*, and sending *YL* to user A. Both users can then calculate the key. The public values q and α ahead of time would need to be known. Alternatively, user A could pick values for q and α and include those in the first message.

III. DH ALGORITHM IN GROUP COMMUNICATION PROTOCOL

There are many approaches that are based on the Diffie Hellman key agreement protocols. The main issue in approach is: the group member’s needs synchronization to form parent keys from their two or more child keys. The cost of modular growing is higher than other approaches.. If calculation of a member is slow, the key agreement process will be delayed. There are two types of nodes leaf nodes and intermediate nodes. Leaf nodes are asymmetric key in the key tree and for this Diffie- Hellman key agreement protocol is introduced and intermediate node is calculated by assigning codes to it.

IV. DH ALGORITHM IN LAYER AND SECURE SHELL

DH algorithm involves the confidentiality and integrity. It flows secure data from users end to server side.SSH is program. it is a protocol also . It encrypts the sequence of the data that flows between the connections.

V. DH ALGORITHM IN BLUETOOTH

BT is a device and technology that transfer the data without any wire. It has a range in which it works. Bluetooth has two types: 1) piconet and 2)scatternet.In piconet, there is a group of devices in which one is master and others are slaves .this is based on master-slave theorem and scatter net is working with group of piconets.communication between these by mater of piconets .Using the Diffie-Hellman algorithm for authentication in Bluetooth devices. This algorithm establishes a shared key and a secure channel is setup between Bluetooth devices and in Bluetooth network.

VI. METHODOLOGY & ASSUMPTIONS

We have completed the research in following steps to get the set objectives.
Step 1: Deep study of the security flaws in network has been done and encryption prospective has taken in account.
Step 2: Study of Diffie-Hellman Algorithm to sense the security in key exchange process has be done.
Step 3: Study and proposed Algorithm with enhancement have come into shape in form of algorithm.
Step 4: After shaping up of proposed algorithm, implementation of proposed algorithm has been tested on C compiler with c language.
Step 5: Comparison of enhanced Diffie-Hellman algorithm with classical Diffie-Hellman algorithm using CrypTool.

VII. PROPOSED ALGORITHM

```
1)  inputs g, a and p
2) if argument are less than 3,then error and stop
3)if p is not prime, then stop
//DH algorithm with g^amod (p)//
4) Dhkey=0
//generate key at sender side//
5)Dhkey=dh1(g, a, p)
//generate key at receiver side//
6)Dhkey=dh2 (g, a, p)
```

Algorithm for Dh1

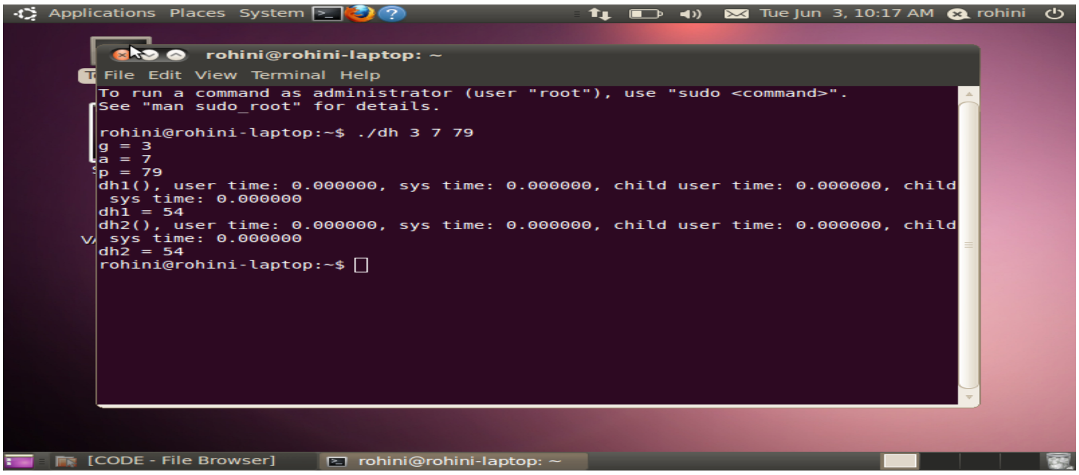
```
  1)If a is zero, then stop
2)If a is one, then return g%p
3)Applying (a*b)%c == ((a%c)*(b%c))%c
return ((g%p)*(dh1( g, a-1, p)))%p
```

Algorithm for dh2

```
1)if a is zero, then stop
2)if a is one, return  g mod p
3)repeat steps4 two to eight times
4)tmp = (tmp*z)%p
    return tmp
```

We have compared the proposed and classical Diffie-Hellman algorithm by using the CrypTool. We analyse the secret key generated by both classical and proposed Diffie-Hellman algorithm by using various parameters of this tool like entropy, autocorrelation etc. We observe that entropy has been increased and autocorrelation decreases which means we have generated the much more secure key which is difficult to break. As a result we enhance the security in NW and it becomes more difficult to decrypt the PRVK generated by the enhanced Diffie-Hellman algorithm.

VIII. RESULTS &.DISCUSSION

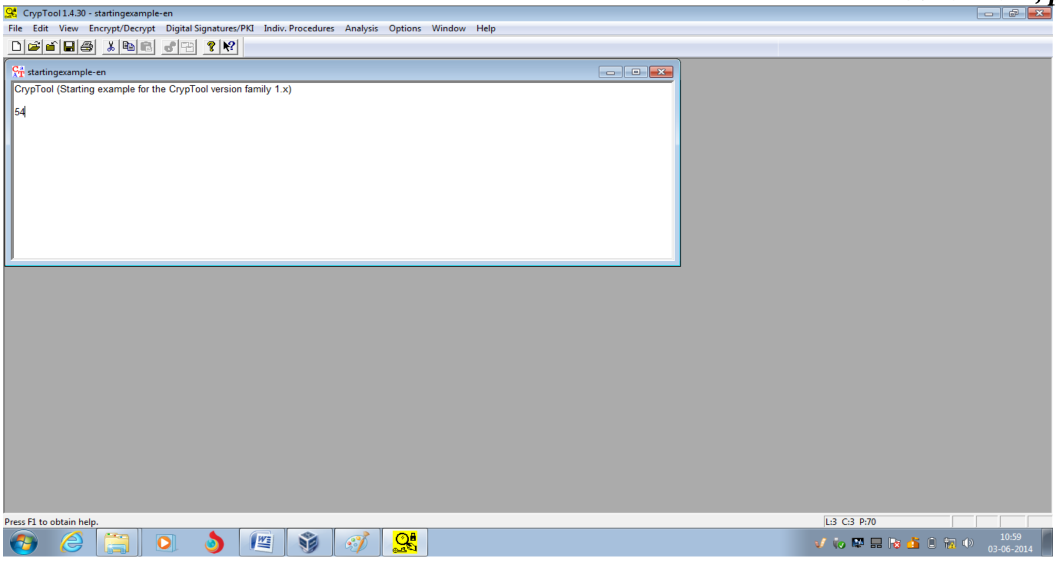


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

rohini@rohini-laptop:~$ ./dh 3 7 79
g = 3
a = 7
p = 79
dh1(), user time: 0.000000, sys time: 0.000000, child user time: 0.000000, child
 sys time: 0.000000
dh1 = 54
dh2(), user time: 0.000000, sys time: 0.000000, child user time: 0.000000, child
 sys time: 0.000000
dh2 = 54
rohini@rohini-laptop:~$ 
```

Fig 1.1. Output screen of Proposed Algorithm

The command prompt shown in the Figure 5.2.1.1 generate secret key which is same for both the sender and the receiver. The receiver can decrypt the encrypted cipher text to the plain text with the help of generated key. As we have increased the range of the secret key it becomes very difficult to decrypt the encrypted text.

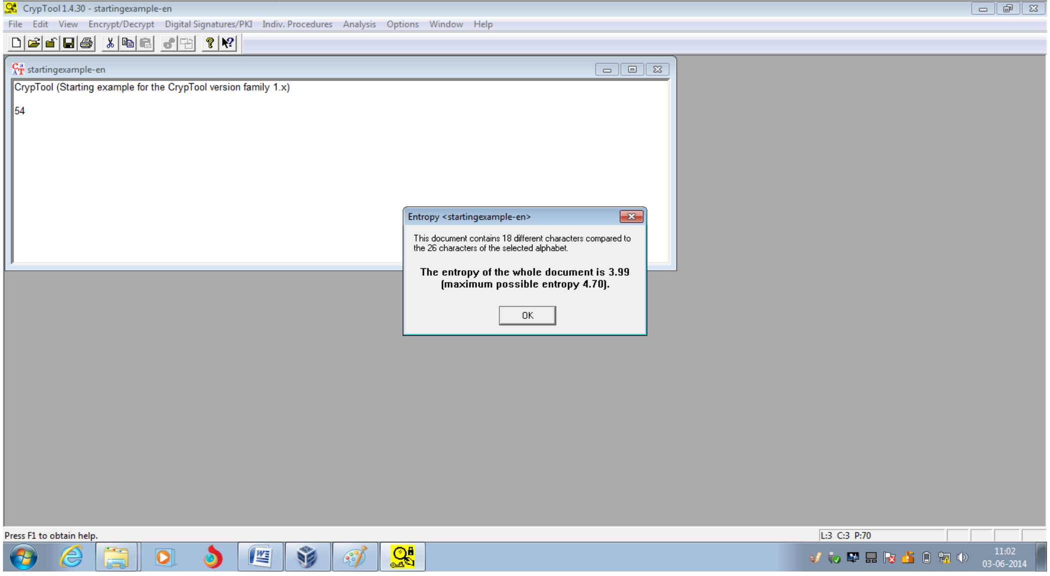

CrypTool 1.4.30 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Press F1 to obtain help.
L:3 C:3 P:70
10:59
03-06-2014

CrypTool (Starting example for the CrypTool version family 1.x)

54

Figure 1.2 Key Generated is pasted in CrypTool for analysis of different Parameters

The generated key in the previous figure is pasted in the CrypTool as shown in figure 1.2 for the analysis of various parameters. Using this tool, user can get its own parameters.


CrypTool 1.4.30 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Entropy <startingexample-en>
OK
Press F1 to obtain help.
L:3 C:3 P:70
11:02
03-06-2014

CrypTool (Starting example for the CrypTool version family 1.x)

54

This document contains 18 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 3.99 (maximum possible entropy 4.70).

Figure 1.3 Calculated Entropy for given sample for Proposed System

The entropy is calculated by using CrypTool for the secret key of proposed algorithm. The result comes out to be 3.99. This calculated entropy result is higher than the classical Diffie-Hellman algorithm entropy result.

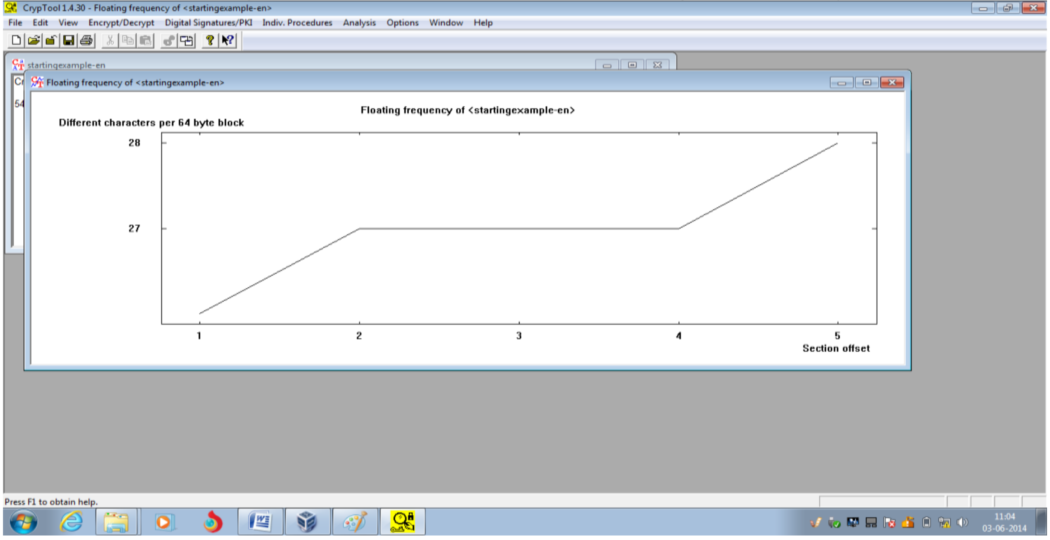

CrypTool 1.4.30 - Floating frequency of <startingexample-en>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Floating frequency of <startingexample-en>
Floating frequency of <startingexample-en>
Different characters per 64 byte block
28
27
1
2
3
4
5
Section offset
Press F1 to obtain help.
11:04
03-06-2014

Fig 1.4: Calculated Floating frequency for Proposed System

As sown in figure 1.4 above the floating frequency of a document is a characteristic of its local information content at individual points in the document.

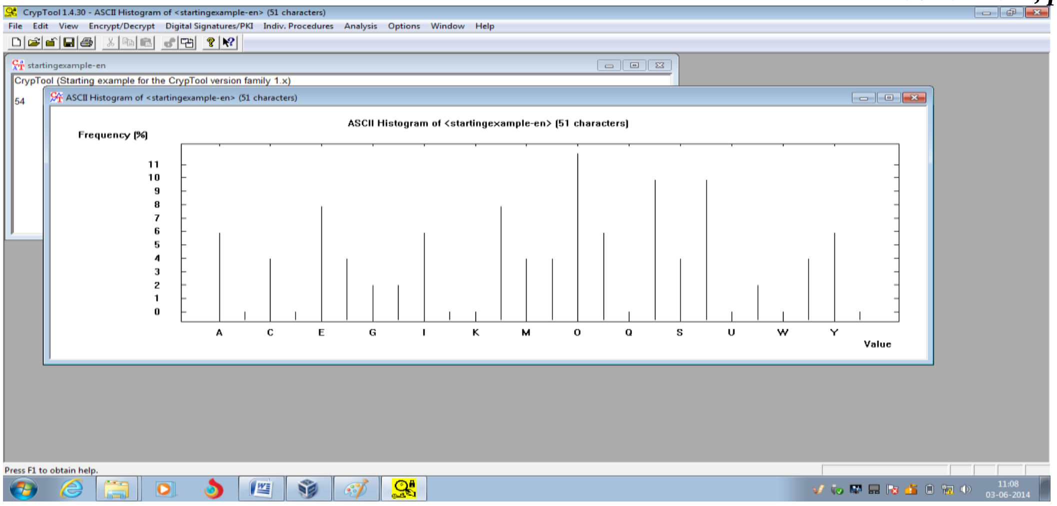
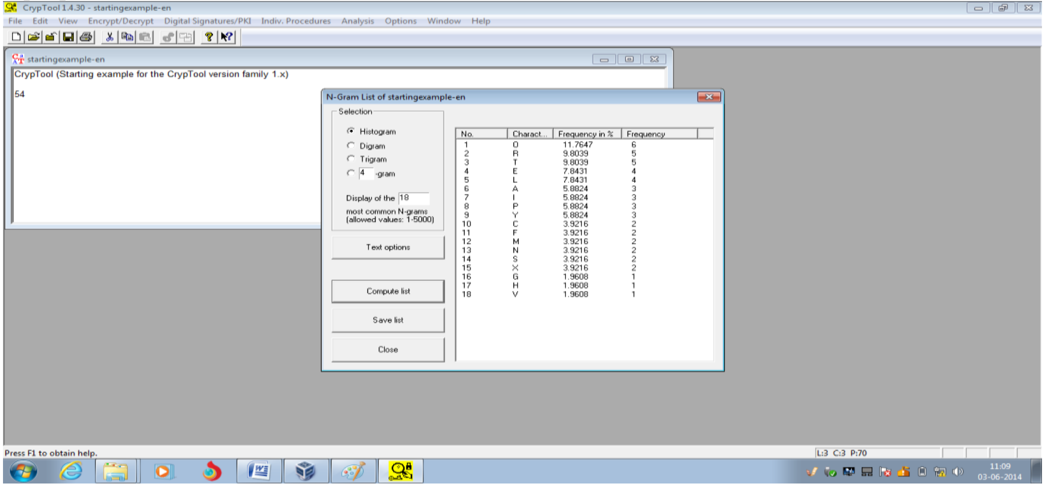

CrypTool 1.4.30 - ASCII Histogram of <startingexample-en> (51 characters)
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
CrypTool (Starting example for the CrypTool version family 1.x)
54
ASCII Histogram of <startingexample-en> (51 characters)
ASCII Histogram of <startingexample-en> (51 characters)
Frequency (%)
11
10
9
8
7
6
5
4
3
2
1
0
A
C
E
G
I
K
M
O
Q
S
U
W
Y
Value
Press F1 to obtain help.
11:08
03-06-2014

Fig 1.5: Calculated Histogram for Proposed System

Histogram is a graphical representation showing a visual impression of the distribution of data.The figure 1.5.shows histogram for proposed work


CrypTool 1.4.30 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
CrypTool (Starting example for the CrypTool version family 1.x)
54
N-Gram List of startingexample-en
Text options
Compute list
Save list
Close
Press F1 to obtain help.
L:3 C:3 P:70
11:09
03-06-2014

Selection

● Histogram
○ Digram
○ Trigram
○ 4 -gram

Display of the 18 most common N-grams (allowed values: 1-5000)

No.	Charact...	Frequency in %	Frequency
1	O	11.7647	6
2	R	9.8039	5
3	T	9.8039	5
4	E	7.8431	4
5	L	7.8431	4
6	A	5.8824	3
7	I	5.8824	3
8	P	5.8824	3
9	Y	5.8824	3
10	C	3.9216	2
11	F	3.9216	2
12	M	3.9216	2
13	N	3.9216	2
14	S	3.9216	2
15	X	3.9216	2
16	G	1.9608	1
17	H	1.9608	1
18	V	1.9608	1

Figure 1.6:Calculated N-Gram for Proposed System

The Figure 1.6 shows N-gram for proposed systems. N-gram calculates the every character generated in the key. The gaps between equal N-grams can be very helpful for breaking a cipher

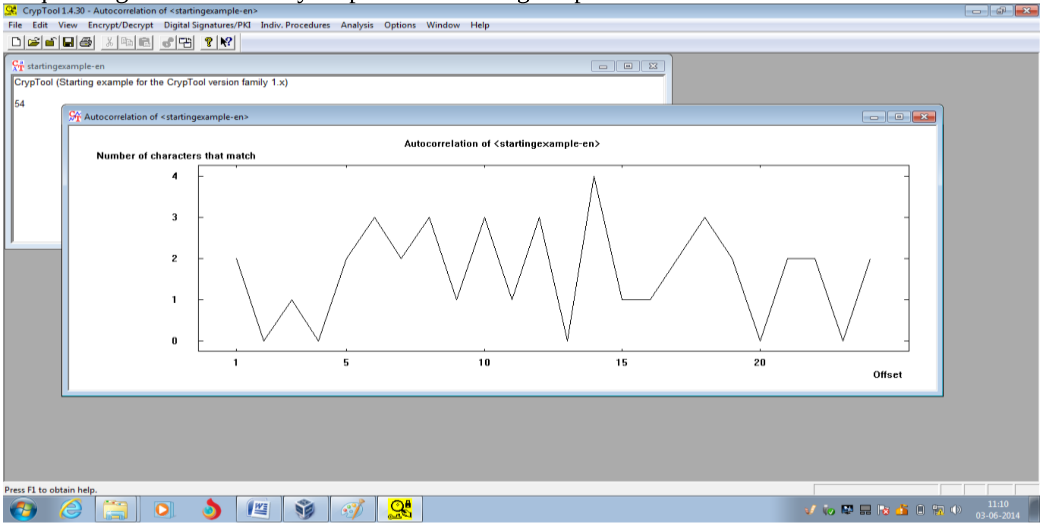

CrypTool 1.4.30 - Autocorrelation of <startingexample-en>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
CrypTool (Starting example for the CrypTool version family 1.x)
54
Autocorrelation of <startingexample-en>
Autocorrelation of <startingexample-en>
Number of characters that match
4
3
2
1
0
1
5
10
15
20
Offset
Press F1 to obtain help.
11:10
03-06-2014

Figure 1.7: Calculated Autocorrelation for Proposed System

Autocorrelation means that a text is compared to copies of the same text

IX. CONCLUSION

The Diffie-Hellman key exchange algorithm is one of the most interesting key distribution schemes in use today. It provides security. It uses in DES for the security. In our purposed work, we enhanced the hardness in security by adding modulus operation on the private key. Our purposed work increases the entropy and decrease the autocorrelation. We are analysed our work by CrypTool. It is analysed our work in its parameters like entropy, Floated frequency, N - gram and histogram. The entropy of our work is higher than other Diffie-Hellman algorithm. Increase in entropy shows increase in hardness in security. The entropy of our work is 3.99 and entropy of previous algorithm is 2.65 in comparison. So our work is better than older Diffie-Hellman algorithm. Our work provides good support for the systems of networks with Diffie-Hellman algorithm for sending the data safely in their different services like communication between sender and receiver in one network area. It maintains the data integrity and consistency in the data.

REFERENCES

[1] Thomas Beth and Dieter Gollmann, “Algorithm Engineering for Public Key Algorithms”, *IEEE* Journal on selected areas in communication, VOL. 7. NO 4. MAY 1989.

[2] Rohit Pandharkar and M. A. Joshi, “A New Method for Generation of Common Keys Using Transcendental Functions and Generalization of Diffie Hellman Protocol”, Technical report CORR 98-5, University of Waterloo, Canada, March 1998.

[3] Emmanuel Bresson, Olivier Chevassut, David Pointcheva and Jean-Jacques Quisquater, “Provably Authenticated Group Diffie-Hellman Key Exchange”, in *Proc. Of ACM CCS ’01,* ACM Press 2001.

[4] Michel Abdalla, Mihir Bellare, and Phillip Rogaway, “ DHIES: An encryption scheme based on the Diffie-Hellman Problem”, In Proc.of ACM CCS ’01, ACM Press September18,2001.

[5] 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.

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

[7] Mario Cagaljm, Srdjan Capkun and Jean-Pierre Hubaux, “Key agreement in peer-to-peer wireless networks”, Laboratory for Computer Communications and 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.

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

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

[10] P. Bhattacharya, M. Debbabi and H. Otrok, “Improving the Diffie-Heliman Secure Key Exchange”, 2005 International Conference on Wireless Networks, Communications and Mobile Computing.

[11] A. Chandrasekar, V.R. Rajasekar and V. Vasudevan, “Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography”, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (4),2005.

[12] Yun Chen , Xin Chen and Yi Mu, “A Parallel Key Generation Algorithm for Efficient Diffie-Hellman Key Agreement”, IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 9, MARCH 2006.

[13] Ik Rae Jeong, Jeong Ok Kwon, and Dong Hoon Lee, “Strong Diffie-Hellman-DSA Key Exchange”, IEEE COMMUNICATIONS LETTERS, VOL. 11, NO. 5, MAY 2007.

.[14] David A. Carts, “A Review of Diffie-Hellman Algorithm and its use in Secure Internet Protocols”, SANS Institue InfoSec Reading Room,2001.

[15] Zhen Cheng , Yufang Huang and Jin Xu, “Algorithm for Elliptic Curve Diffie-Hellman Key Exchange Based on DNA Tile Self-assembly”, IEEE COMMUNICATIONS LETTERS, VOL. 10, NO. 9, MAY 2008.

[16] Shengbao Wang, Zhenfu Cao, Maurizio Adriano Strangio, and Lihua Wang, “Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol”,IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 2, FEBRUARY 2008.

[17] Hua-Yi Lin, “Hypercube Routing Protocol with Secure Data Transmission Mechanisms in Sensor Networks Using Elliptic Curve Diffie-Hellman Key Agreements”, 2009 International Conference on New Trends in Information and Service Science.

[18] Eun-Jun Yoon and Kee-Young Yoo, “An Efficient Diffie-Hellman-MAC Key Exchange Scheme”, 2009 Fourth International Conference on Innovative Computing, Information and Control.

[19] Salvatore Cavalieri and Giovanni Cutuli, “Implementing Encryption and Authentication in KNX using Diffie-Hellman and AES Algorithms”, IEEE Commun. Lett., vol. 10, pp. 198-200, Mar. 2009.

[20] Vishnu Kumar, Yunjung Park, Dugki Min and Eunmi Choi, “Secure-EEDR: Dynamic key exchange protocol based on Diffie-Hellman algorithm with NOVSF code-hopping technique for wireless sensor networks”, 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering.

[21] Zhang ,Dongfang (2010), “A New Authentication and Key Agreement Protocol of 3G based on Diffie-Hellman Algorithm”, IEEE Commun. Lett., vol. 9, pp. 198-200.

[22] Mustafa Toyran and Sava Berber, “Efficient Implementation of Elliptic Curve Diffie-Hellman(ECDH) Key Distribution Algorithm in Pool-Based Cryptographic Systems (PBCSs)”, IEEE Commun. Lett., vol. 11, pp. 189-199,June 2010.

[23] S. Anahita Mortazavi, Alireza Nemaney Pour and Toshihiko Kato, “Efficient Many-to-Many Group key Management Protocol”, 2011 International Conference on Information and Computer Applications (ICICA 2011).