ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Extension of Diffie Hellman Algorithm for Multiple Participants

Shivani Atish Gaonkar[1], H. Manjunath Pai[2]

PG Student, Department of ECE, NMAMIT, Nitte, Karnataka, India[1]

Assistant Professor, Department of ECE, NMAMIT, Nitte, Karnataka, India[2]

Abstract: Diffie Hellman key exchange algorithm was proposed in 1976. Extension of this algorithm is done for multiple participants. The number of exponentiations will vary by N. If large number of participants is involved then it becomes complicated. Here we reduce the complexity and increase the speed by making use of divide and conquer technique. It divides the total number of participants into smaller groups and applies algorithm on them independently. There are $\log_2 N+1$ exponentiations obtained which are less compared to N and makes the key exchange simpler. Software implementation of extension of this algorithm is done using MATLAB. Further hardware implementation is carried out by making use of a DSP processor.

Keywords: Diffie Hellman key exchange algorithm.

I. INTRODUCTION

Cryptography is art and science of scrambling data to avoid transmission of data which is not secure. When data is transferred there is a risk of the data being damaged so it is transmitted in some other format so that the intruder cannot detect the data that been sent. Encryption and Decryption are the two main aspects of Cryptography. Encryption is a process of converting a simple understandable form of data into cipher text whereas decryption is exactly the opposite process where cipher text gets converted into plain text. Symmetric key and asymmetric key cryptography are two types. If same key is used for encryption and decryption process its symmetric cryptography and different keys are used then its asymmetric cryptography.

Diffie Hellman Key Exchange is an algorithm used in public key cryptography as it uses asymmetric type of key exchange. First developed by Whitfield Diffie and Martin Hellman in 1976.Ralph Merkle was remarked as an inventor of this algorithm due to his contribution to the field of public key cryptography. Two parties without any prior knowledge about each other can share same secret and if the keys exchanged between them remain the same then it is said to be a secure transmission.

This algorithm is used in security protocols such as SSL, IPSEC etc. session keys are created for every session and gets destroyed at the end of each session. No need to store them for the future. Agreement of keys can be done over internet.

Extension of Diffie Hellman Algorithm is carried out by several researchers and different methods are used to add participants into the algorithm. Divide and Conquer method is used here which allows the total number of participants involved to be divided first in every step and then adding a secret value to it. By raising this value to its exponent the key is obtained in every step. The secret value is called the private key and it is not known to the participants whereas the public key which is obtained is known to all the participants involved. Here key exchange is carried in such a way that in the last round when all the intermediate results are obtained, every participant can add his/her own private key to the result it has obtained and obtains the secret key. On comparing this extension method to the other methods it is found that it will reduce the total number of exponentiations from N which is for a normal circular arrangement to log2N+1.we can check results by increasing the participants in powers of 2. Another observation to be made is that the number of steps involved will vary by 3N-2 where N is the number of participants involved. Further the hardware implementation of this extension is carried out using DSP processor and results are obtained.

II. RELATED WORK

Whitfield Diffie and Martin Hellman proposed an algorithm called Diffie Hellman key exchange algorithm as in [1], explained a secure exchange of key can be used for subsequent exchange of messages. It appeared first in the paper that defined public key cryptography [DIFF76b]. Twenty years later this algorithm was extended for group communication by Steiner M et al as in [2], where they have defined a class of "natural" extensions of Diffie Hellman key exchange to the n-party setting and have shown that the security of a generic n-party protocol is equivalent to the security of the original 2-party. G.P.Biswas as in [3], explained two concepts of extension. The extension in the first case can generate multiple DH-style keys with comparatively less key generation overhead. It also provides more protection to the keys and increases applicability. On the other hand, the extension

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

proposed in the second case can generate a multi-party key for large static groups.

III. DIFFIE HELLMAN KEY EXCHANGE ALGORITHM

This algorithm allows two parties that have no prior knowledge about each other to jointly establish a shared secret. Secure transmission of data takes place between the two parties. They have to first agree upon two parameters such as prime number and primitive root that are been used.

Steps involved:

- The two parties are A and B. Both agree upon two positive integers, n and g where n is a prime number and g is a group generator.
- Party A randomly chooses a positive integer x, smaller than n and its called as A's private key. B also chooses its own private key y.
- A and B compute public keys using X = ((g) ^ x) mod n and Y = ((g) ^ y) mod n, respectively.
- They exchange public keys through a communication channel.
- On receiving these keys, they will compute shared key K, using K =(Y) ^x mod n = (g) ^xy mod n and K = (X) ^y mod n = (g) ^xy mod n.
- In the last step we observe that x and y both are raised to the generator which indicates that two exponentiations are involved in this case.

Example of Two Party Diffie Hellman key Exchange :

- Mark and Steve agree that p=23 and g=5.
- Mark selects a private key XA=6 and calculates a public key.
- YA ≡ 5^6 ≡ 8 (mod 23). He sends this to Steve.
- Steve selects a private key XB=15 and calculates a public key.
- YB ≡ 5^15 ≡ 19 (mod 23). He sends this to Mark.
- Mark calculates the shared secret S ≡ YB^XA ≡ 19^6 ≡ 2 (mod 23).
- Steve calculates the shared secret. S ≡ YA^XB ≡ 8^15 ≡2 (mod 23).

A. *Flowchart for Two Party Diffie Hellman Algorithm*

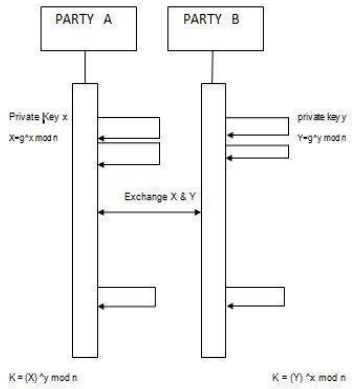

Fig. 1: Flowchart of two party Diffie Hellman algorithm

B. Three party Diffie Hellman using circular arrangement method.

It involves a circular arrangement in which the keys are circulated among all the participants in continuous manner such that each participant will add his/her private key to the existing value and move it further such that each round is completed and at last its observed that key exchanged by all the three participants is the same. Three participants will have three keys in three rounds using this arrangement.

- The parties agree on parameters p and m. a, b and c are the private keys.
- In the first round, Alice computes m^a, sends it to Bob. Bob then computes $(m^a)^b = m^{ab}$ and sends to Carol. Next Carol computes $(m^{ab})^c = m^{abc}$ as her secret.
- In the second round, Bob computes m^b and sends it to Carol. Carol computes $(m^b)^c = m^{bc}$ and sends to Alice. Alice computes $(m^{bc})^a = m^{bca} = m^{abc}$ as her secret

IV. PROPOSED METHOD

The divide and conquer strategy is applied to a group of multiple participants in which we make use of simple steps such as exponentiation, swapping the results, adding private key to the result which is obtained and obtaining the secret key.A1, B1, C1, D1, E1, F1, G1, and H1 are the chosen eight participants. Each will select a, b, c, d, e, f, g, h as their private keys.

- A1, B1, C1, and D1 perform one exponentiation each to yield m^{abcd}; which is sent to E1, F1, G1, and H1.
- In return, A1, B1, C1, and D1 will receive m^{efgh}.A1 and B1 perform one exponentiation each, to yield m^{efghab}, and they send it to C1 and D1, while C1 and D1 yield m^{efghcd}, and send to A1 and B1.
- A1 performs an exponentiation, yielding $m^{efghcda}$, which is sent to B1; similarly, B1 sends $m^{efghcdb}$ to A1. C1 and D1 do similarly.
- A1 performs one final exponentiation, yielding the secret $m^{efghcdba} = m^{abcdefgh}$, while B1 does the same to get $m^{efghcdab} = m^{abcdefgh}$, again, C1 and D1 do similarly.
- Participants E1 to H1 simultaneously do the same operations using m^{abcd} as their starting point.
- All participants possess the secret $m^{abcdefgh}$, but each participant will have performed only four modular exponentiations, rather than the eight implied by a simple circular arrangement.

A. *Comparative Analysis of Key Distribution Protocols*

Table 1: Comparative analysis of key distribution protocols

PROTOCOL	EXPONENTIATIONS	NUMBER OF STEPS
NORMAL METHOD	N	N^2
PROPOSED METHOD	log2(N)+ 1	3N-2

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Table 1 shows comparative analysis based on the number of steps involved and the exponentiations involved in the two protocols that are mentioned.

B. Flowchart for Proposed Method

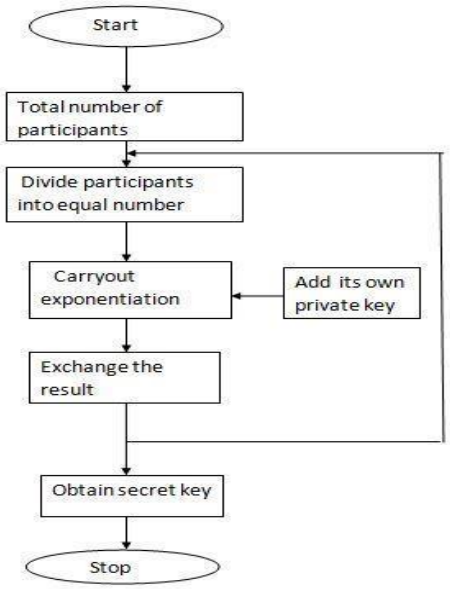

Fig. 2: Flowchart of proposed method

C. Observations

Table 2: Results for normal and proposed method

NORMAL METHOD			
PARTICIPANTS		EXPONENTIATIONS	STEPS
2		2	4
4		4	16
8		8	64
16		16	256
PROPOSED METHOD			
PARTICIPANTS		EXPONENTIATIONS	STEPS
2		2	4
4		3	10
8		5	22
16		9	46

Table 2 shows the results when 2,4,8,16 participants are involved proposed method has less number of exponentiations and the steps compared to the normal method.

V. SOFTWARE IMPLEMENTATION USING MATLAB

Diffie Hellman key exchange is designed here for eight participants in MATLAB using the divide and conquer strategy that is been explained with the use of flowchart and algorithm.

First all the eight participants will choose a particular number as its secret number and the process will begin. The prime number and the value of generator is also given a input. There will be four rounds involved for eight participants and in every round one exponentiation takes place so it requires four exponentiations. At the end of each round some intermediate result will be obtained by each participant and in the fourth or final round all participants will share the same key which makes the process secure.

Even if all the intermediate results are known the final key cannot be revealed.

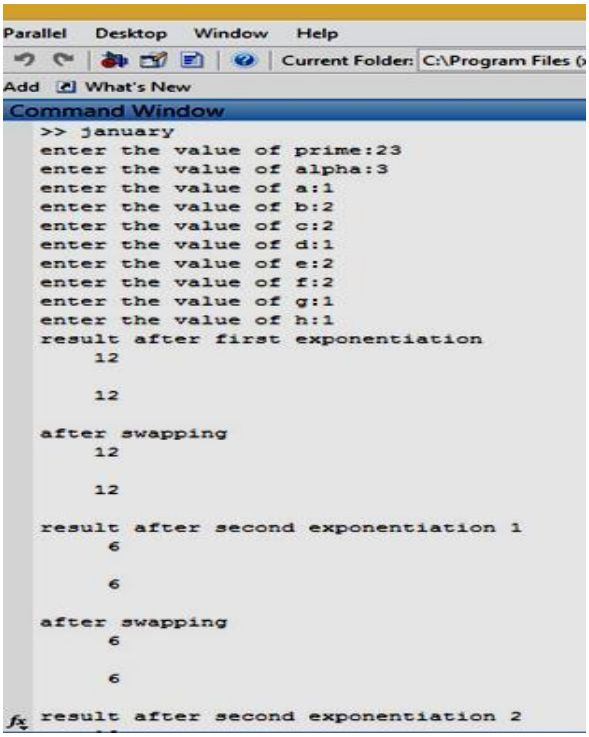

Fig.3: First and second exponentiation

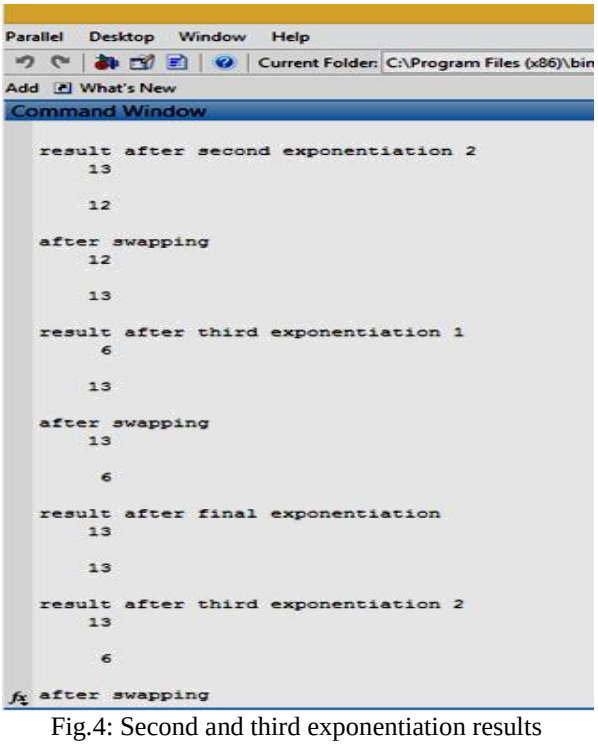

Fig.4: Second and third exponentiation results

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

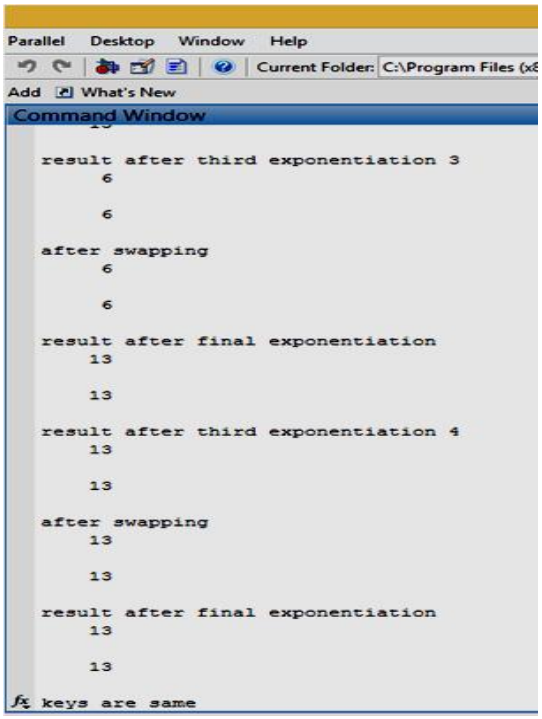

Fig.5: Third and final exponentiation results

VI. HARDWARE IMPLEMENTATION USING DSP

Hardware implementation is done using DSP TMS320C6713 kit. The input is provided and output is detected using code composer studio (CCS v3.3). The program is written using c coding and compiled with code composer studio and then it is dumped on to a Digital signal Processor. The c program is written by making use of arrays in order to store the large numbers and these are given as input. The key values are observed after taking the modulus of resulting value obtained.

Following Figures show hardware implementation of Diffie Hellman key exchange for eight participants using DSP TMS320C6713.

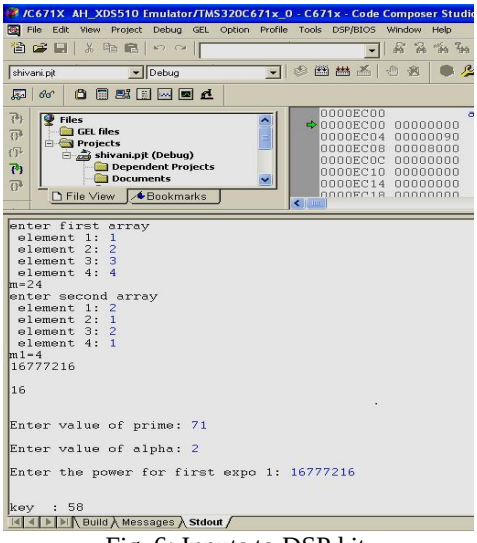

Fig. 6: Inputs to DSP kit

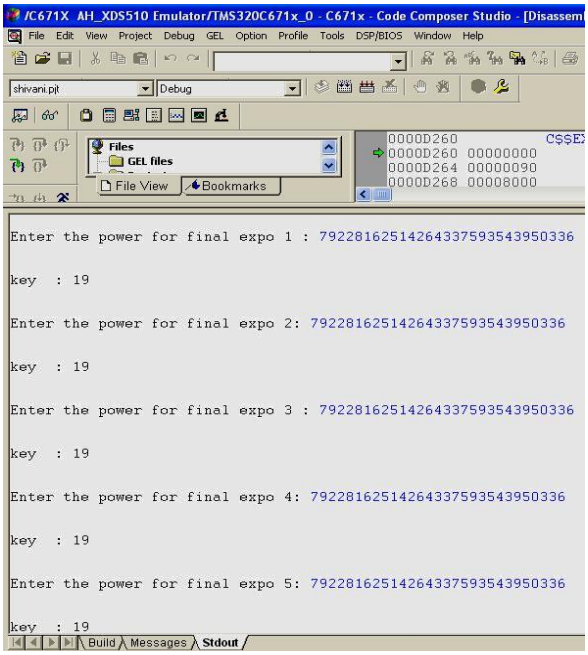

Fig. 7: Output results using DSP

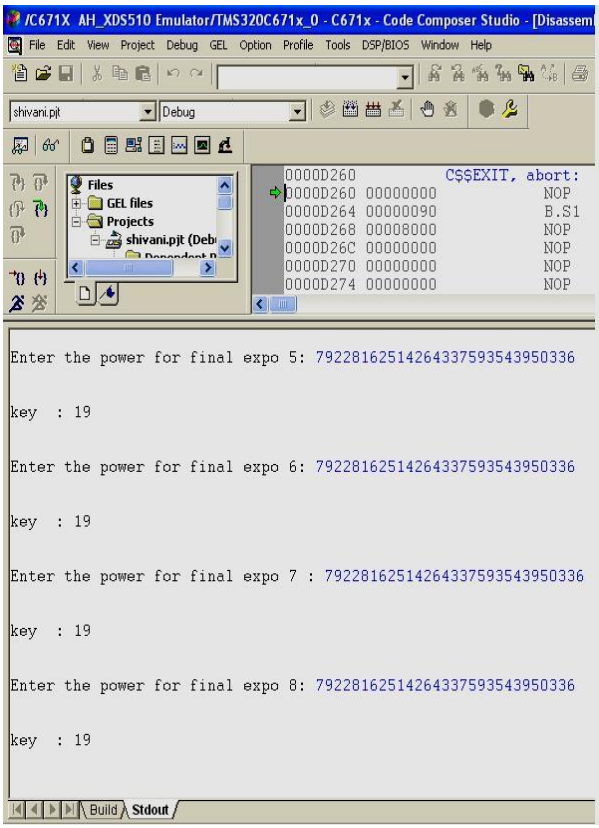

Fig. 8: Output results using DSP

Results: prime number and primitive root given as input and every member will use some number as his private key. Here a, b...h have used a number as its secret.3N-2 steps are taken and log2N+1 exponents are used to get final result in which the entire N=8 members will generate the same key.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

In example1 using MATLAB, for p=23 and alpha=3 the final key will be 13 which is given to all the participants in the final round. Similarly in example 2 using DSP processor where the code is written in c language, for p=71 and alpha=2, the keys obtained in the final round will be 19.

It requires 22 steps for generating keys for eight participants.

VII. CONCLUSION

The proposed method used is simpler compared to other methods used for extension of Diffie Hellman algorithm. Less Numbers of steps are taken and there will be less exponentiation involved. Exponentiations make the process complicated so by reducing these exponentiations we are reducing the complexity. Speed factor is more since only a few steps are taken to get the final results. Extension is carried out for eight participants and can be further expanded for a larger number.

REFERENCES

[1] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography" IEEE transactions on information theory, Vol-22 .NO-6, pp. 644-654, November 1976.

[2] Steiner M, Tsudik G, Waidner M, "Diffie Hellman key distribution extended to groups" conf .computer and communication security, pp. 31-37, 1996.

[3] G.P.Biswas, "Diffie-Hellman technique: extended to multiple two party keys and one multi-party key" IET Information Security, Vol-2, NO-1, pp.12-18, September 2006.

[4] International Journal of Engineering Science and Innovative Technology (IJESIT)Volume 1, Issue 2, November 2012 69 Diffie-Hellman and Its Application inSecurity Protocols.

[5] William Stallings,"Cryptography and Network Security",chapter 10,pp 301-304,Fourth Edition 2006.