RESEARCH ARTICLE OPEN ACCESS

Advancement in Diffie-Hellman algorithm

Monalisa Jha, Shraddha Patil
(Department of Electronics and Telecommunication, Symbiosis international University, Pune-46)
(Department of Electronics and Telecommunication, Symbiosis international University, Pune-46)

ABSTRACT
The aim of this research is to compare the existing Diffie Hellman Algorithm and the proposed, Advancement in Diffie Hellman Algorithm. The Diffie Hellman algorithm is used to generate a secret key for secure transactions and communication at organizations. In Advanced Diffie Hellman Algorithm, we apply certain mathematical algorithms at both the ends, that is, sender and receiver, in order to make the communication more secure. Thus, the information sent from one end to the other would be in encrypted form, making it difficult to decipher.
Keywords - *Diffie-Hellman, authentication mechanism, key exchange*

I. INTRODUCTION

The year 1976 marked as a landmark period in which the famous Diffie Hellman key exchange cryptography emerged. This first practical method intends to produce private secret key shared over a public medium or a public channel. Diffie-Hellman key exchange is widely used to establish session keys in Internet protocols. It is the main key exchange mechanism in SSH (secure shell) and IPSec (IP security) and a popular option in TLS (transport layer security).Diffie Hellman is commonly implemented and deployed with these protocols and we find that, in practice, it frequently offers less security than widely believed. [2] In this paper, we intend to take the concept of key exchange by Diffie Hellmen forward and induce methods to secure this key exchange algorithm by using simple mathematical algorithms. The mathematics behind this algorithm is conceptually simple and includes [1] the algebra of exponents and modulus arithmetic. The new algorithm is called Advancement in Diffie Hellman Algorithm.

II. DIFFIE HELLMAN ALGORITHM

For this discussion we will use Alice and Bob, two of the most widely traveled Internet users in cyberspace, to demonstrate the Diffie Hellman key exchange. [3] Table 1 shows the Diffie Hellman key exchange algorithm.

Table 1: Diffie Hellman algorithm

Alice	Bob
Alice chooses secret number 'a'	Bob chooses secret number 'b'.
Calculates (g^a)mod p	Calculates (g^b)mod p
This value is sent to Bob	This value is sent to Alice
Alice has now (g^b)mod p	Bob now has (g^a)mod p
Let us assign this as 'Bob_value'	Let us assign 'Alice_value'
Now Alice calculates (g^(Bob_value))^a mod p	Now Bob calculates (g^(Alice_value))^a mod p
This value is secret value	This value is secret value

III. THE ADVANCED DIFFIE HELLMAN ALGORITHM

The Advanced Diffie Hellman algorithm has been proposed in order to make the original Diffie Hellman algorithm more secure. Our main aim here is to compute the values of secret number chosen by the two organizations using certain mathematical algorithm. This would ensure the confidentiality of the chosen values of 'a' and 'b;, that is the secret number.

Our next aim would be to secure the data sent from one organization to another. Alice sends the value (g^amodp) to Bob in the original Diffie Hellman, but here we have cubed this value and then sent to Bob. This would make man in the middle attack more difficult. With this as the area of focus, we hereby propose the Advanced Diffie Hellman. Fig.2 shows the Advanced Diffie Hellman algorithm.

Alice	Bob
Calculate (p+a).	calculate (p+b)
Multiply (p+a) with p.	Multiply (p+b) with p.
find mod of complex_1 i.e.((p+a)*p)%g	find mod of complex_2 i.e.((p+b)*p)%g
Put this value of the above in complex_1.	Put this value of the above in complex_2.
Calculate the square of (complex_1) ^2.	Calculate the square of (complex_2)^2
This value is again added to compex_1.	This value is again added to compex_2.
Calculate the square of (complex_1) ^2.	Calculate the square of (complex_2)^2
This value is again added to compex_1.	This value is again added to compex_2.

This new values is called new_complex_1	This new value is called new_complex_1
a1=g^(new_complex_1) mod p	b1=g^(new_complex_2) mod p
Take cube of a1	Take cube of b1
(a1^3) is sent to Bob	(b1^3) is sent to Alice

IV. ADVANTAGES OF THE ADVANCED DIFFIE HELLMAN ALGORITHM

Complexity - The complexity of the algorithm is increased. Values of the chosen number 'a' and 'b' are made complex. If a cryptanalyst tracks down the values of the chosen numbers, it would be difficult to decrypt and find 'a' and 'b'. The cryptanalyst would be finding only a1 and b1.

Man in the middle attack - If an attacker finds the data being sent from Alice to Bob, he would be capturing (a1^3) or (b1^3). It would make the task difficult to arrive at the actual value since the actual values are cubed and then sent.

Security - The Diffie Hellman code had no security over the chosen secret key 'a' and 'b'. If the cryptanalyst deciphered the values of and b, the secret key would be obtained. In the Advancement Diffie Hellman, the values of 'a' and 'b' have been encrypted. Even if the values of 'a' and 'b' are deciphered, this algorithm would make the values more secure.

Reverse process - Reverse engineering or reverse process would be very difficult for the cryptanalyst.
The major advantage of this algorithm is that the users are making their own secret numbers more secure by performing algorithms at their own end.

V. CONCLUSION

The Diffie Hellman key generation protocol did not have any mechanism to secure the secret key of the two parties involved. We have introduced certain operations to make the attack more difficult. However, various other implementations are possible. When the data is sent from one party to another, instead of cubing, one can introduce some other operations as well.

Acknowledgements

We gratefully acknowledge the contributions of our guiding light, our professor, Mrs Dipti Kapoor Sarmah, who showed us the direction and cleared our doubts.

REFERENCES

Journal Papers:

[1] Preeti and Bandana Sharma, *" Review Paper on Security in Diffie-Hellman Algorithm," Volume 4, Issue 3, March 2014.*

[2] David A. Carts, *"A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols," SANS Institute Reading Room site.*

[3] Paul C. Kocher, *"Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems," Cryptography Research Inc.,CA 94105,USA.*

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

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

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

[7] 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.*

Books:

[8] William Stallings*, "Cryptography and Network Security :Principles and Practice", 5th Edition, Pearson education.*

[9] Behrouz Forouzan , Debdeep Mukhopadhyay*, " Cryptography and Network Security", 2nd Edition, Tata McGraw-Hill Education.*