Abstract

Exchanging cryptographic keys has been a problem with respect to security. Whitfield Diffie and Martin Hellman proposed the Diffie-Hellman key exchange algorithm to overcome the problem. Since then, the concept of key exchange over an unsecured network has completely been revolutionized. The algorithm is based on using arithmetic calculations for transmission of the shared session keys. The purpose of this algorithm is to enable users to securely exchange keys which can be used for later encryptions. This ability to securely exchange session keys dynamically and publicly between a group of users has become the foundation for secure group applications such as distributed computing, distributed databases and conference calls. Man-in-the-middle attacks are better secured using the Diffie-Hellman algorithm. Over time, Diffie-Hellman algorithm has been altered several times by various authors. However, some limitations to the Diffie-Hellman algorithm still persist. One of the limitations of the Diffie-Hellman algorithm is that it is computationally intensive thereby increasing the time complexity when generating public keys. The proposed algorithm has similar grounds with the Diffie-Hellman algorithm, and a new technique is used for sharing session keys which overcome the time
Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm

complexity limitation of the Diffie-Hellman algorithm. The proposed "Multiplicative Key Exchange Algorithm" uses simple arithmetic equations to generate and exchange keys over an insecure network.

References

2. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 4, Issue 1, January-February 2015 ISSN 2278-6856

Index Terms

Computer Science | Algorithms

Keywords

Security; Diffie-Hellman; Key Exchange; Multiplicative; time complexity