Abstract

Network Security is a complex subject that can be intercepted by well versed and skilled people. Today, with increase in networking, the folks need to know the importance of security in network. Cryptography is a field for providing security to the networks and protecting information and communication. Even after providing securities, the network is vulnerable to some of the attacks in different networking areas like Man-in-the middle attack in the area of key exchange protocol. Statistical tests are used to check these sequences, before calculating the private key and the shared key. In the paper, the generated binary sequence is converted into Octal instead of Decimal so that the memories utilized by both the generated keys are reduced and the complexity is decreased. Decimal sequence is of 10 bits whereas octal sequence is of 8 bits, so changing the sequence to Octal instead of Decimal will result in the reduction of 2 bits which may eventually reduce the complexity and memories utilized. Also, converting the binary sequence to octal allows the password to be minimum 128-bits. Previously, the password was set to the limit 256-bits range but now the limit is lowered to 128-bits range. In future, this method can be implemented on other encryption methodologies to provide a secure
environment for secure transmission of data.

References

5. Networking- A review”,2017 IEEE.
6. https://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
11. Manoj Ranjan Mishra, Jayaprakash Kar “ A STUDY ON DIFFIE-HELLMAN KEY EXCHANGE
15. Sonia Rachel , Subhashkar S ,” An Overview of the Man-In-The-Middle Attack”, National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS), 2017

Index Terms
Keywords

Diffie-Hellman, network security, complexity