Abstract

The area of security has become more important to personal computer users, organizations, and the military due to the continuous advancements in technology and computing resources. With the advent of Internet and ease of data sharing among users, the integrity of the data has become quite an issue. Moreover, with better computational resources the number of threats also increases. This further pushes for a stronger and better security measures. The entire field of security is vast and in an evolutionary stage. In this paper, we have re-engineered a well known and widely used public-key algorithm of Diffie-Hellman. The paper also provides an insight into other public-key algorithm. In our work, we have proposed some amendments in DH so as to improve the secret key values. Experimental results show that our proposed amendments in DH give significant improvements.

References

and Decision, 2009.

**Index Terms**

Computer Science

Security

**Keywords**

Cryptography

Security goals

Security threats