Abstract

A digital signature is a cryptographic method for verifying the identity of an individual. It can be a process, computer system, or any other entity, in much the same way as a handwritten signature verifies the identity of a person. Digital signatures use the properties of public-key cryptography to produce pieces of information that verify the origin of the data. Several digital schemes have been proposed as on date based on factorization, discrete logarithm and elliptical curve. However, the Swati Verma and Birendra Kumar Sharma [8] digital signature scheme which combines factorization and discrete logarithm together making it difficult for solving two hard problems from the hackers point of view. This paper presents the implementation of same, with the help of different tools and further analyzes them from different perceptions.

References

- T. ElGamal. A public key cryptosystem and a signature scheme based on discrete


- S. Wei. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Progress on Cryptography, pages 107-111, 2004


**Index Terms**

Computer Science

Security

**Keywords**

Cryptography  Integer Factoring  Discrete Logarithm  Digital Signature