Abstract

With the significant advances in communication networks over the last few decades, smart cards have been widely used in many e-commerce applications and network security protocols due to their low cost, portability, efficiency and cryptographic properties. In this paper, we analyze Sood et al.'s smart card based authentication scheme and demonstrate that the scheme is vulnerable to masquerade user attack, offline password guessing attack, time concurrency weaknesses and fails to achieve mutual authentication. A secure dynamic identity based remote user authentication scheme without verification tables, is proposed in this paper and the scheme resolves the aforementioned problems of Sood et al.'s scheme. The computation cost of the proposed scheme is comparable to Sood et al.'s scheme and it is highly secure taking into consideration the complexity of calculating discrete logarithms and the resistance to various attacks.
An Enhanced Secure Remote User Authentication Scheme without Verification Table

- H. C. Shih, "Cryptanalysis on Two Password Authentication Schemes,"
An Enhanced Secure Remote User Authentication Scheme without Verification Table

Laboratory of Cryptography and Information Security, National Central University, Taiwan, July 2008


Index Terms

Computer Science

Security

Keywords

Remote User Authentication, Smart Cards, No Verification Table, Cyclic groups, Discrete Logarithm