Abstract

Network and Internet applications are growing very fast, since the need to secure these applications are very fast. So the importance and the value of the swapped data by the Internet and other media types are increasing. The protection of multimedia data, sensitive information like credit cards, banking transactions and social security numbers is becoming very important. For secure transmission of data in open network, encryption is very important methodology. In recent years many encryption methods have been proposed and used to protect confidential information. In this survey paper many different asymmetric cryptography techniques, like RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm) are analyzed. Also discussed many other efficient algorithms.

References

- Liang Wang, Yonggui Zhang, 2011, "A New Personal Information Protection
A Survey and Performance Analysis of Various RSA based Encryption Techniques

Approach Based on RSA Cryptography”, IEEE.
- Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, 2013,
“Quantum Key Distribution by Using Public Key Algorithm (RSA)”, IEEE.
- Norhidayah Muhammadi, Jasni Mohamad Zaini, Md Yazid Mohd Saman,
“Loop-based RSA Key Generation Algorithm using String Identity”, 13th International
Conference on Control, Automation and Systems (ICCAS 2013).
- Ms. Ritu Patidar, Mrs. Rupali Bhartiya, 2013, “Modified RSA Cryptosystem Based
on Offline Storage and Prime Number”, IEEE.
- Malek Jakob Kakish, “Enhancing The Security Of The RSA Cryptosystem”,
IJRRAS August 2011.
- KetuFile White Papers “Symmetric vs. Asymmetric Encryption”, a division of
Midwest research corporation.
- A fast implementation of the RSA algorithm using the GNU MP library. By Rajorshi
Biswa, Shibdas Bandyopadhyay, Anirban Banerjee, IIIT – Calcutta.
- Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the
Asian Network for Scientific Information.

Index Terms

Computer Science
Security

Keywords
RSA  i-RSA