Abstract

Public-key (or asymmetric key) algorithms are the most dominant cryptographic algorithms in the cryptography era. RSA, in particular, is a good example of algorithms that belong to this category which is used for many applications and its security is beyond doubt. The key size of RSA is an important factor that determines its robustness. As the computational powers evolve, the need to increase the security of cryptosystems becomes essential to achieve more robustness against cryptanalysis attacks. In the literature, the commonly used solution to achieve this goal is to increase the key size. However, in practice, keeping increasing the key size is not feasible and not unlimited; increasing the key size demands more computational power. The increase in computational power makes it hard (or impossible) to conduct the encryption process in some environments such as smart cards. Also, it should be taken into consideration that the dramatic increase in computational capabilities of new machines improves their abilities to break encryption keys. Therefore, an alternative to increasing the key size is essentially needed. In this paper, we propose a new approach for encryption that is based on RSA main algorithm while using more encryption keys with smaller sizes in addition to
An Enhanced Cryptosystem based on Shorter Keys and New Security Component

extra security information component (known as the Security Card, SeCa). Our results show that the use of multiple-shorter keys with the SeCa component produces significant improvements in the performance of RSA algorithm in terms of increasing security and reducing the computation overhead by decreasing encryption and decryption times.

References

An Enhanced Cryptosystem based on Shorter Keys and New Security Component


Index Terms

Computer Science

Security

Keywords

Security, RSA, Encryption, Decryption, Cryptanalysis Attack, Cryptography, Asymmetric Key, Key Size