Enhancement RSA Security using Polynomials and Rabin Functions

Alshammari, Shaden

The maturity of the electronic commerce, internet banking facilities, and software protection systems issues stimulate the world's attention to create a safe electronic data exchange environment. RSA is the most common cryptography algorithm using an asymmetric key for encryption and digital signatures. However, it becomes less secure because it depends on prime factorization. The vulnerability of RSA has increased with the development of research in the field of factoring algorithms, enhanced over the past two decades. This mathematical study proposes a new algorithm called Polynomial RSA (P-RSA) to enhance the security of the original RSA algorithm. Two techniques were used to achieve this goal; one is using more than two prime numbers for building the keys; two is using Rabin function to make random guessing of the prime numbers more difficult. The proposed algorithm, P-RSA, has been tested in this research on 160 random numbers. The ensuing outcomes were scattered, which makes deducing plaintexts given any number of cipher texts impossible. Also, the complexity time in generating the keys in P-RSA is more than the traditional RSA. This makes the time necessary to break the keys in P-RSA longer than the traditional RSA. In conclusion, using more than two primes for generating the keys reduces the vulnerability of breaking them over the next decades. This could lead to a much safer environment for current and future sensitive industry information.

Awards Won: