Improvements in field of Encryption and Decryption by focusing on Time attack

Aarushi Singhal, Divya Batra

Abstract

Security is one of the most important things. When data is uploaded online and is being transmitted from one place to another then it becomes vulnerable to attacks and if correct measures are not taken then it causes leakage of sensitive information. Ranging from symmetric methods to asymmetric methods for encrypting data has significantly given ways to provide security at different levels.

The symmetric technique for encryption focused on transference of data using encrypting and decrypting data by same key which did not provide security to data at major level, as use of same key for encryption and decryption can easily be leaked if data is leaked. This called for new methods to be introduced which could provide such encryption technique that could help in saving data from different attacks and can't easily be leaked.

RSA, an asymmetric cryptographic technique is one of such methods which have reduced the leakage of data by introducing 2 different keys for data encryption and decryption. One key is public that is accessible to all and the other one is private key which is only accessible to the person whom it belongs to and is not shared with others.RSA has made transmission of data easy online without any leakage as it ensures that the person who has valid key can only decrypt message. The non transference of keys has enhanced its security. As it is majorly used technique, adding more level of security to it is must. So, this research paper concentrates on minimizing the problems based on time attack and enhancing the scope of security even if the private key is lost.

Key Points: Cryptography, public key cryptography, RSA, attacks, Digital signature