Cryptographic Algorithms

Institution Affiliation

Date

Cryptography is the process of learning and constructing techniques that secure communication especially where third parties are involved. It usually concentrates on the construction of protocols involved in preventing private messages from being read by the public (Schneier, 2015). Public key is a type of cryptographic system which uses pairs of private and public keys that are only known by the owner. Using a public key facilitates the authentication of origin of a message from the owner who is using a paired private key or the encryption of a message to ensure only those owners who have paired their private keys can be able to decrypt their messages. Any person using a receiver’s public key can encrypt a message and only the receiver can decrypt the message with his private key. A user should therefore find ways to generate a public and private key pair to ease their encryption and decryption computationally.

An example of a public key algorithm which facilitates the provision of digital signatures and secrecy is the RSA in the attempt to improve authenticity and confidentiality in data storage. The RSA is a computationally complex process of transmission and encryption of large information hence slower than other the hashing method. RSA‘s main use is to secure transmission of data through the creation and publishing of a public key on the basis of the factoring problem and large prime numbers. The prime number is usually a secret and on the holder can be able to decode the message. RSA is however unpopular in the direct encryption of user data due to its slow nature. It may not be semantically secure if it lacks padding since an attacker can be able to successfully launch a plaintext attack against it. There is also a possibility of a chosen cipher text to this algorithm due to the property of the product of two cipher texts being equal to the respective plain texts’ product.

Reference

Schneier, B. (2015). *Applied cryptography, second edition: Protocols, algorithms, and source code in C*.