A Hybrid Cryptosystem using DNA, OTP and RSA

Volume 172
Number 8

Year of Publication: 2017

Authors:
Mahbuba Begum, Jannatul Ferdush, Md. Golam Moazzam

Abstract

Cryptography is one of the major elements in data security and communication security. It is a technique of securing the communication by preventing third parties. A hybrid cryptosystem is the special set of rules using multiple ciphers or a combination of a series of well-defined steps that can be followed as a procedure of different types together by taking best advantage of each cipher. In this cryptosystem, a random secret key is generated used as a symmetric cipher which is required for all parties. Then the system encrypts this key via an asymmetric cipher using the recipient's public key. DNA cryptography is a new optimistic field in cryptography which hides the data in terms of DNA sequence to make it secured. The OTP (one-time pad) is an encryption technique in which a plaintext is paired with a one-time pre-shared key which is equal to or longer than the size of the message being sent. In RSA, a public key is used for encryption which specifies the transformation of plaintext into ciphertext and this encryption key differs from the decryption key which is kept private to secure data transmission. In this paper, a hybrid cryptosystem is proposed using DNA, the generic OTP technique and RSA to ensure high security in three levels. This method is very efficient for encrypting data, hiding text and
preventing attacks.

References

1. ^a b c "Intro to Numbers Stations". Retrieved 13 September 2014.

Index Terms

Computer Science Security

Keywords
A Hybrid Cryptosystem using DNA, OTP and RSA

DNA, One Time Pad, RSA.