Network security refers to an activity which is designed to protect the usability and integrity of the network and data. In network security, cryptography is the branch in which one can store and transmit data in a particular format so that only the intended user can read and process it. RSA algorithm is an asymmetric cryptography technique, which works on two keys i.e. public key and private key. The proposed method takes four prime numbers in RSA algorithm. Instead of sending public key directly, two positive integers are used, on which some mathematical calculation is done. And by using those integers two public keys would be sent to the user. The scheme has speed enhancement on RSA decryption side by using Chinese remainder theorem. So that the algorithm overcomes several attacks which are possible on RSA.

References

3. Number theory concepts and Chinese remainder theorem:
4. Saurbh Singh and Gaurav Agarwal, “Use of Chinese Remainder theorem to generate random numbers for cryptography” Research article in international journal of applied engineering research, DINDIGUL. ISSN- 0976-4259
7. Network security Concepts,
11. RSA Algorithm in Cryptography
    http://www.geeksforgeeks.org/rsa-algorithm-cryptography/
13. Chinese remainder theorem and proof
    https://brilliant.org/wiki/chinese-remainder-theorem/

Index Terms

Computer Science                      Security

Keywords

RSA, Cryptography, Network Security.