

{tag} International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

[Volume 170](#)

-
[Number 1](#)

Year of Publication: 2017

Authors:

Aarushi Rai, Shitanshu Jain

10.5120/ijca2017914674

{bibtex}2017914674.bib{/bibtex}

Abstract

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

1. T.R. Devi, "Importance of cryptography in network security" IEEE International Conference, Communication System and network Technologies (CSNT), 2013

2. William Stein, elementary Number Theory, Primes Congruences and Secrets. January 23, 2017
3. Number theory concepts and Chinese remainder theorem:
“<https://crypto.stanford.edu/ptbc/notes/numbertheory/crt.html>.”
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
5. R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
6. G. R. Blakey, "A Computer Algorithm for Calculating the Product AB Modulo M ," IEEE Transaction on Computers, vol. 32, no. 5, pp. 497-500, 1983.
7. Network security Concepts,
“<http://williamstallings.com/Extras/Security-Notes/lectures/publickey.html>”
8. P.C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other Systems” Advances in cryptography- CRYPTO '96, pp. 104-113, 1996.
9. Celine Blondeau and Kaisa Nyberg, “On Distinct Known Plaintext Attacks”, Aalto University Finland, WCC_2015
10. Israt Jahan, Mohammad Asif, Liton Jude Rozario “ Improved RSA cryptosystem based on the study of the number theory and public key cryptosystems” volume-4 Issue-1, pp-143-149.
11. RSA Algorithm in Cryptography
<http://www.geeksforgeeks.org/rsa-algorithm-cryptography/>
12. Nikita Somani, Dharmendra Mangal, “ An improved RSA cryptographic System”. International Journal of Computer Applications (0975-8887) volume 105-No. 16 November 2014.
13. Chinese remainder theorem and proof
<https://brilliant.org/wiki/chinese-remainder-theorem/>

Index Terms

Computer Science

Security

Keywords

RSA, Cryptography, Network Security.