
International Journal of Computer Applications
© 2015 by IJCA Journal

Volume 112 - Number 13
Year of Publication: 2015

Authors:
Shaina Arora
Pooja

10.5120/19730-1429

Abstract

Cryptography is generated to create secure data transmission over networks. The algorithm chosen for cryptography should satisfy the conditions of authentication, confidentiality, integrity and non-repudiation. Recent years have witnessed the phenomenal growth of RSA. We design an algorithm to merge both enhanced RSA algorithm and El-Gamal algorithm to provide user with a higher level of data security. The enhanced RSA algorithm enables faster encryption and decryption process and generating public and private key faster than the original RSA. The Enhanced RSA Cryptosystem is based on Integer Factorization Problem (IFP), while the El-Gamal Cryptosystem is based on Discrete Logarithm Problem (DLP). This model works on the basis of combining IFP and DLP. The weaknesses of RSA algorithm when we use two prime's number are the following points which are used to break the algorithm in most cases. These weaknesses are: (a) Small encryption exponent, if you use a small exponent like e=3 and send the same message to different recipients. (b) Using the Same key for encryption and signing. (c) There is no secure Method to Transfer the Public Key From Sender to the Receiver. It Only provides the mechanism of generating Public and Private Keys. Enhanced RSA works on the Existence of three Prime Numbers that will give the ability to the enhanced encryption method to increase the difficulty of factoring of the variable (n), Its speed increases the process of encryption and decryption. While generating variable (n) by original
RSA algorithm, this generate the public and private key that contains the number of 500 digits by using two primes number with 200 digits each. Multiplication process will take longer than the time to generating the same variable (n) by using three prime numbers where each number with 200 digits. In another case more complexity of the algorithm is increased by combining the other asymmetric El-Gamal algorithm.

References

- http://searchsoftwarequality.techtarget.com/definition/cryptography
- http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
- http://www.truecrypt.org/docs/aes
- http://en.citizendium.org/wiki/Rivest_ciphers
- https://www.schneier.com/blowfish.html
- http://searchsecurity.techtarget.com/definition/RSA
- http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
- http://www.princeton.edu/~achaney/tmve/wiki100k/docs/ElGamal_encryption.html
- markus-jakobsson.com/papers/jakobsson-siacrypt00.pdf
- http://x5.net/faqs/crypto/q29.html
- http://www.accuhash.com/what-is-md5.html
- http://pcsupport.about.com/od/termsm/g/md5.htm
- Taher El-Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Algorithm", IEEE transactions on information theory.
- Lein Harn, Manish Mehta, Wen-Jung Hsin, "Integrating Diffie-Hellman Key Exchange into Digital Signature Algorithm (DSA)", IEEE Communication Letters, March 2004
Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elamal: Analysis

- Wang, Suli, Liu, Ganlai (2011) "File encryption and decryption system based on RSA algorithm". Computational and Information Sciences (ICCIS), Page(s): 797 – 800.
- Da Silva, J. C. L. (2010) "Factoring Semi primes and Possible Implications for RSA". Electrical and Electronics Engineers in Israel (IEEEI), Page(s): 000182 – 000183.
- Fei Shao, Zinan Chang, Yi Zhang (2010) "AES Encryption Algorithm Based on the


Index Terms

Computer Science                     Security

Keywords

Security  Cryptography  RSA algorithm