Abstract

Yamen Cryptosystem: An Enhanced RSA by Using Rabin Algorithm and Huffman Coding. By Abdallah Karakra

Today, RSA algorithm is the most widely used public-key cryptosystem around the world. It is used for security in everything from online shopping to cell phones. However, the basic RSA is not semantically secure, i.e., encrypting the same message more than once always gives the same ciphertext. For this reason, the basic RSA is vulnerable to set of indirect attacks, such as *known plaintext*, *chosen plaintext*, *timing*, *common modulus*, and *frequency of blocks* (FOB) attacks. To the best of our knowledge no one points to *FOB* attack against RSA. Moreover, RSA is known to be much slower than the standards symmetric key encryption and it does not used for encrypting large data.

In this thesis, we design and implement a swift and secure variant of RSA based on Rabin and Huffman coding called *Yamen* cryptosystem to solve aforementioned limitations of the basic RSA. A new additional randomization component Y is added in *Yamen* cryptosystem. This component is encrypted by *Rabin* algorithm to improve the security level of RSA against the *indirect attacks* and make RSA semantically secure. Moreover, *Yamen* makes the factorization problem harder against *brute force attack*, since the attackers need to break the factorization of large numbers for both RSA and Rabin. Besides, employing Huffman coding compression in *Yamen* prevents *FOB* attack and speeds up the execution time for the *Yamen*.

Yamen cryptosystem comes with three sensitive enhancement factors comparing with basic RSA. These factors are *security*, *execution time* and the *Size of the ciphertext*. *Yamen cryptosystem* is semantically secure. *Yamen* generates different ciphertexts for the same message. Also, our testing results over set of file sizes of 1MB, 2BM,.., to 10 MB show that *Yamen* cryptosystem is faster than basic RSA by 45% in encryption process and 99% in decryption process. Also, we found that RSA system increases the size of ciphertext by 1% compared to the original file size, while *Yamen* cryptosystem reduces the size of ciphertext by 54% from its original sizes. This reduction depends on the number of occurrences of the symbols inside the file.