University of Science and Technology

Faculty of Information Technology & Computer Science

Collage of Postgraduate Studies

MS.c in Computer Sciences

Comparing RSA Standard and RSA Variants

(Rebalanced RSA-CRT, Rebalanced Schema A and Rebalanced Schema B)

Using Encryption and Decryption Time

This thesis is submitted in Partial Fulfillment of MS.c in Information Systems

Prepared by:

Wafa Mohammed Mustafa Ahmmed

Supervisor:

Dr .Nour Eldien Abdelrahman Nour Eldien

MAY 2014

Abstract

Nowadays, electronic communication is being widely used. There are many commercial applications that require security.

By far the most important automated tool for network and communications security is encryption. Cryptography is generally divided into two schemes: private-key (asymmetric) cryptography and public-key (symmetric) cryptography. One of Asymmetric encryption is RSA; RSA is the most widely deployed Asymmetric cryptosystem.

The security of RSA was based on the number of bits in private-key; this make the decryption is slow. Many of RSA variants were designed to speed up RSA decryption in software, such as Multi-factor RSA, Rebalanced RSA and RPrime RSA.

In this research, a comparison between the variant Rebalanced RSA-CRT, Rebalanced Schema A, Rebalanced Schema B and Standard RSA is carried out to compare encryption and decryption time using different key size.

The comparisons have been implemented by using JDK1.7 as the programming environment.

The comparison results show that the decryption time in Rebalanced RSA_CRT is much faster than the Standard RSA, but the encryption time is very slow. Rebalanced RSA-CRT Scheme A and Rebalanced RSA-CRT Scheme B reduce the encryption time required by the original Rebalanced RSA-CRT, but the decryption time is a little slower than that of Rebalanced RSA-CRT.

المستخلص

في الوقت الحاضر يتم استخدام الاتصالات الإلكترونية على نطاق واسع .هناك العديد من التطبيقات التي تتطلب الأمنيه. يعتبر التشفير إلى حد بعيد الأداة الأكثر أهمية لأمن الشبكات والاتصالات .وينقسم التشفير إلى قسمين التشفير بالمفتاح العام (غير المتماثل) , و التشفير بالمفتاح الخاص (المتماثل). خوارزمية RSAهي أحدى خوارزميات التشفير غير المتماثل الأكثر أستخدما على نطاق واسع .

تعتمد الامنيه في خوارزمية RSAعلى عدد البتات في المفتاح الخاص، مما يودي ذلك الي بطء في عمليه فك التشفير .

صممت العديد من التحسينات لتسريع فك تشفير RSA القياسية برمجيا. مثل خوارزميه Multi-factor RSA، Rebalanced RSA و RPrime RSA.

في هذا البحث تمت المقارنه بين زمن الشفير وزمن فك التشفير بينRebalanced RSA-CRT ، Rebalanced Scheme A، Rebalanced Scheme B و RSA للتحقق من انها تحقق الهدف ٍ. تم تطبيق الخوارزميات باستخدام لغه الجافا باستخدام مفاتيح باطوال مختلفه.

من المقارنه نستنتج أن خوارزميه Rebalanced RSA-CRT جعلت زمن فك التشفير اسرع من RSA Standard ، ولكن اصبح زمن التشفير أبطأ من RSA Standard .

خوارزميتي Rebalanced Scheme A & Scheme B ادتا الي تسريع زمن التشفير. ولكن زمن فك التشفير اصبح ابطأ بقليل من Rebalanced RSA-CRT.

1.1 Introduction

Cryptography is the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security.

The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information.

By far the most important automated tool for network and communications security is encryption. Two forms of encryption are in common use, conventional or symmetric encryption, and public-key or Asymmetric encryption. one of cryptosystem in which encryption and decryption are performed using the same key, Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys one a public key and one a private key.

Public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, and authentication.

One of the public-key encryption was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman and first published in 1978. The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.

The encryption and decryption in RSA require taking heavy exponential multiplications modulus of a large integer N which is the product of two large primes' p and q.
The encryption and decryption time in RSA are roughly proportional to the number of bits in public and private exponents respectively. The security of RSA was based on the number of bits in private-key [2].

1.2 Research Problems

Rebalanced RSA-CRT variant and two enhancement schemes A and schemes B are proposed to reduced the decryption time.

In this research the three variants are investigated to understand each variant achieve the intended goals.

1.3 Research Objectives

The objective of this research is to investigate strength and weaknesses of Rebalanced RSA-CRT variant.

1.4 Research Tools

RSA algorithms cryptosystem was implemented by using JDK1.7, as the programming environment, which contains a BigInteger class that was used to generate large prime numbers.

1.5 Research Result

The experimental results show that, the decryption time in the original Rebalanced RSA-CRT is much faster than that in Standard RSA. And the Rebalanced RSA-CRT Scheme A and Rebalanced RSA-CRT Scheme B makes encryption time faster than that of Rebalanced RSA-CRT, but the decryption is a little slower than that of Rebalanced RSA-CRT. Still all the three variant are faster than standard RSA in decryption time.

1.6 Thesis Organization

This thesis was organized as follows; chapter two details the Standard RSA and RSA–CRT variant, chapter three discuss the Rebalanced RSA-CRT and its variants schemes. In chapter four RSA, RSA–CRT and Rebalanced RSA-CRT and its variants **(**scheme A and scheme B) are compared. In chapter five, we draw conclusions and recommendation for future work.