بسم الله الرحمن الرحيم

Sudan University of Science and Technology
College of Graduate Studies

A Performance Measure of RSA and DSS Algorithms in Digital Signature

قياس الأداء في خوارزميتي ر.س.أ و د س س في التو قيع الر قمي

A Thesis Submitted in Partial Fulfillment of Master Degree in Computer Science

By:
Mogtaba Fadelelmola E'safi E'nour

Supervisor

Dr. Hamid Musa Mohammed Humaida

June 2011

الايه

قال تعالي :

)إِن يَمْسَسْكَ اللّهُ بِضُرٍّ فَلاَ كَاشِفَ لَهُ إِلاَّ هُوَ وَإِن يَمْسَسْكَ بِخَيْرٍ فَهُوَ عَلَى كُلِّ شَيْءٍ قَدُيرٌ(

صدق الله العظيم

الايه (17) سورة الانعام

Dedication

I dedicate this Study to all members of my family.

Acknowledgement

Thanks are due to Dr. Hamid Musa of the University of Kordofan, for his support, scientific guidance and encouragement, which helped me to carry out this study.

List of Tables

List of Figures

Acronym

Number	Acronym	Appreciation name
1.	ANSI	*American National Standards Institute*
2.	CMT	*Cryptographic Module Testing (lab)*
3.	DES	*Data Encryption Standard*
4.	DSA	*Digital Signature Algorithm*
5.	DSS	*Digital Signature Standard*
6.	ECDSA	*Elliptic Curve Digital Signature Algorithm*
7.	FIPS	*Federal Information Processing Standard*
8.	MIPS	*Million instruction per seconds*
9.	NIST	*National Institute of Standards and Technology*
10.	PKCS #1	*Public Key Cryptography Standards*
11.	rDSA	*Reverse Digital Signature Algorithm*
12.	RNG	*Random Number Generator*
13.	SHA	*Secure Hash Algorithm*

Table of Contents

Abstract

Digital signature is used in message transmission to verify the identity of the sender and to ensure that a message has not been modified after signing. It is one of the most important applications and technique for cryptography and of achieving security in digital transactions. Its importance increases continuously in the age of computing and informatics. This research investigates the digital signature algorithms RSA and DSS in order to compare their performance in carrying these requirements, types and schemes. These algorithms are intensively discussed. There is a comparison between two algorithms with different mathematical background; nevertheless, both algorithms have public key variants. One of these algorithms was built using discrete logarithm while the other was built using factoring of large numbers.

The performance of the two public key (RSA and DSS) has been implemented and compared and the results show that signing and verification operations in the RSA and DSS.

A experiment was conducted to measure performance of that algorithms and the computational overhead in term of time and space complexity, cryptanalysis methods of those algorithms, are highlighted lists and record of time carried by breaker algorithm are given.

الخلاصة

يستخدم التوقيع الرقمي فـي عمليـة التاكـد مـن الرسـالة المرسـلة حـتي لا يتـم تعديلها من وجهة المرسـل الـي المسـتقبل ، وتعتـبر احـدي اهـم التطبيقـات فـي علـم التشفير وذلك لتحقيق السرية وعملية المصادقة في المعاملات الرقمية . ومما زاد من اهميتها ازدياد التعاملات التبادلية لنقل البيانات في عصر الحوسبة المعلوماتية .

في هذا البحث يتم دراسة التوقيع الرقمي لكل من خوارزميـة RSA و DSS مـن حيث التوقيع الرقمي اللتان تعتمدان علـي المفتـاح العـام مـن حيـث نـوع المخططـات اللتان تتبعان اليهما وذلك من الناحية الرياضية (التحليل الـي الاعـداد الاوليـة و مشـكلة اللوغرثم المقطع). ايضا تم قياس الاداء لهـاتين الخوارزميـتين فـي العمليـات اللازمـة لعملية التوقيع الرقمي من حيث الزمن وذلك باختبـار برمجـي لهـم وتـم تحديـد افضـل هذه الخوارزميات وفقا لكل العمليات ، ثم تم رصـد عـدد مـن الدراسـات الـتي قـامت بكسر هاتين الخوارزميتين وفقا للطرق الرياضية المستخدمة فـي كـل ورصـد الفـترات الزمنية لذلك.