

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**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  
التوقيع الرقمي

***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 تعالى :

(إِن يَمَسُّكَ اللَّهُ بِضُرٍّ فَلَا كَاشِفَ لَهُ إِلَّا هُوَ وَإِن يَمَسُّكَ بِخَيْرٍ فَهُوَ عَلَىٰ كُلِّ شَيْءٍ قَدِيرٌ)

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***

<b>No. of Table</b>	<b>Title</b>	<b>Page No.</b>
Table (1)	Execution time of RSA, DSS and proposed algorithm.	<b>39</b>
Table (2)	Execution time of RSA and DSA algorithm in laptop and PDA	<b>40</b>
Table (3)	Execution time of RSA, DSS and proposed algorithm.	<b>41</b>
Table (4)	Test data with key size 512	<b>51</b>
Table (5)	Test data with key size 1024	<b>51</b>
Table (6)	Test data with key size 4096	<b>51</b>

***List of Figures***

<b>No. of Table</b>	<b>Title</b>	<b>Page No.</b>
Fig (1)	digital signature Diagram	<b>17</b>
Fig (2)	RSA Approach	<b>23</b>
Fig (3)	DSS approach	<b>28</b>
Fig (4)	SHA-1 Approach	<b>31</b>
Fig (5)	Comparison of Key generation using RSA and DSS	<b>38</b>
Fig (6)	Comparison of signing using RSA and DSS	<b>39</b>
Fig (7)	Comparison of verifying using RSA and DSS	<b>39</b>
Fig (8)	Comparison of Key generation, signing and verifying RSA	<b>40</b>
Fig (9)	Comparison of Key generation, signing and verifying	<b>40</b>
Fig (10)	Comparison of Key generation, signing and verifying RSA and DSS	<b>41</b>

### **Acronym**

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

## *Table of Contents*

<b>Code</b>	<b>Subject</b>	<b>Page No</b>
	الاية	<b>II</b>
	<i>Dedication</i>	<b>III</b>
	<i>Acknowledgement</i>	<b>IV</b>
	<i>list of table</i> <i>list of figure</i>	<b>V</b>
	<i>Acronym</i>	<b>VI</b>
	<i>Index</i>	<b>VII</b>
	<i>Abstract</i>	<b>X</b>
	الخلاصة	<b>XI</b>
	<i>Chapter One</i> <b>OVERVIEW</b>	<b>1</b>
1.1	<i>Introduction</i>	<b>2</b>
1.2	<i>The thesis plan</i>	<b>4</b>
1.2.1	<i>Problem.</i>	<b>4</b>
1.2.2	<i>Hypotheses</i>	<b>4</b>
1.2.3	<i>Objectives</i>	<b>5</b>
1.2.4	<i>Methodologies.</i>	<b>5</b>
1.3	<i>Overview of Cryptography</i>	<b>6</b>
1.3.1	<i>Types of Cryptographic Algorithms</i>	<b>6</b>
1.3.2	<i>Symmetric and asymmetric algorithms</i>	<b>8</b>
1.3.3	<i>digital signature:(overview, Requirements, Types of digital signature)</i>	<b>8</b>
1.4	<i>Research structure</i>	<b>11</b>
	<i>Chapter Two</i> <b>DIGITAL SIGNAGURE</b>	<b>13</b>
2.1	<u>digital</u> signature:	<b>14</b>
2.2	Uses of digital signatures	<b>16</b>
2.2.1	<i>Authentication</i>	<b>16</b>
2.2.2	<i>Integrity</i>	<b>16</b>
2.2.3	<i>Non-repudiation</i>	<b>17</b>
2.3	Using digital signatures with trusted applications	<b>18</b>
2.4	Digital signatures vs. ink on paper signatures	<b>18</b>
2.5	Advantages and Disadvantages of Digital Signature	<b>19</b>
2.6	Some digital signature algorithms	<b>19</b>
2.7	Overview of RSA	<b>21</b>



2.7.1	Security and practical considerations	<b>23</b>
2.7.2	Integer factorization and RSA problem	<b>25</b>
2.8	Overview of DSA	<b>25</b>
2.9	Hash Secure Algorithm	<b>29</b>
	<i>Chapter Three</i> <i>RSA and DSS Algorithm</i>	<b>32</b>
3.1	Overview	<b>33</b>
3.2	RSA Algorithm:	<b>33</b>
3.3	DSA algorithm	<b>35</b>
3.4	Compression of various digital signature schemes	<b>38</b>
3.5	Types of attacks	<b>40</b>
3.6	performance effects	<b>46</b>
3.7	Experiment	<b>48</b>
	<i>Chapter four</i> <i>Conclusion</i>	<b>54</b>
4.1	Conclusion	<b>62</b>
4.2	Further work	<b>64</b>
4.3	References	<b>65</b>
4.4	<i>Appendix</i> <ul style="list-style-type: none"> <li>• <i>A : RSA Source Code</i></li> <li>• <i>B : DSA Source Code</i></li> <li>• <i>C : SHA-1 Source Code</i></li> <li>• <i>D : Code for Generation , signing , verification using RSA</i></li> <li>• <i>E : Code for Generation , signing , verification using DSA</i></li> </ul>	<b>66</b>

## **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 في عملية التأكد من الرسالة المرسله حتي لا يتم تعديلها من وجهة المرسل الي المستقبل ، وتعتبر احدي اهم التطبيقات في علم 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 خوارزمية RSA و DSS من حيث التوقيع الرقمي اللتان تعتمدان علي المفتاح العام من حيث نوع المخططات اللتان تتبعان اليهما وذلك من الناحية الرياضية (التحليل الي الاعداد الاولية و مشكلة اللوغرثم المقطع). ايضا تم قياس الاداء لهاتين الخوارزميتين في العمليات اللازمة لعملية التوقيع الرقمي من حيث الزمن وذلك باختبار برمجي لهم وتم تحديد افضل هذه الخوارزميات وفقا لكل العمليات ، ثم تم رصد عدد من الدراسات التي قامت بكسر هاتين الخوارزميتين وفقا للطرق الرياضية المستخدمة في كل ورصد الفترات الزمنية لذلك.