Ain Shams University
Faculty of Engineering
Electronics and Communication Engineering Department

Public-Key Cryptography

A Thesis
Submitted in Partial fulfillment for the requirements of the degree of Ph.D.
In
Electrical Engineering
[Electronics and Communication Engineering]

By

Mohamed Nagib Ahmed El Sherbiny
B.Sc. 1975 & M.Sc. 1990

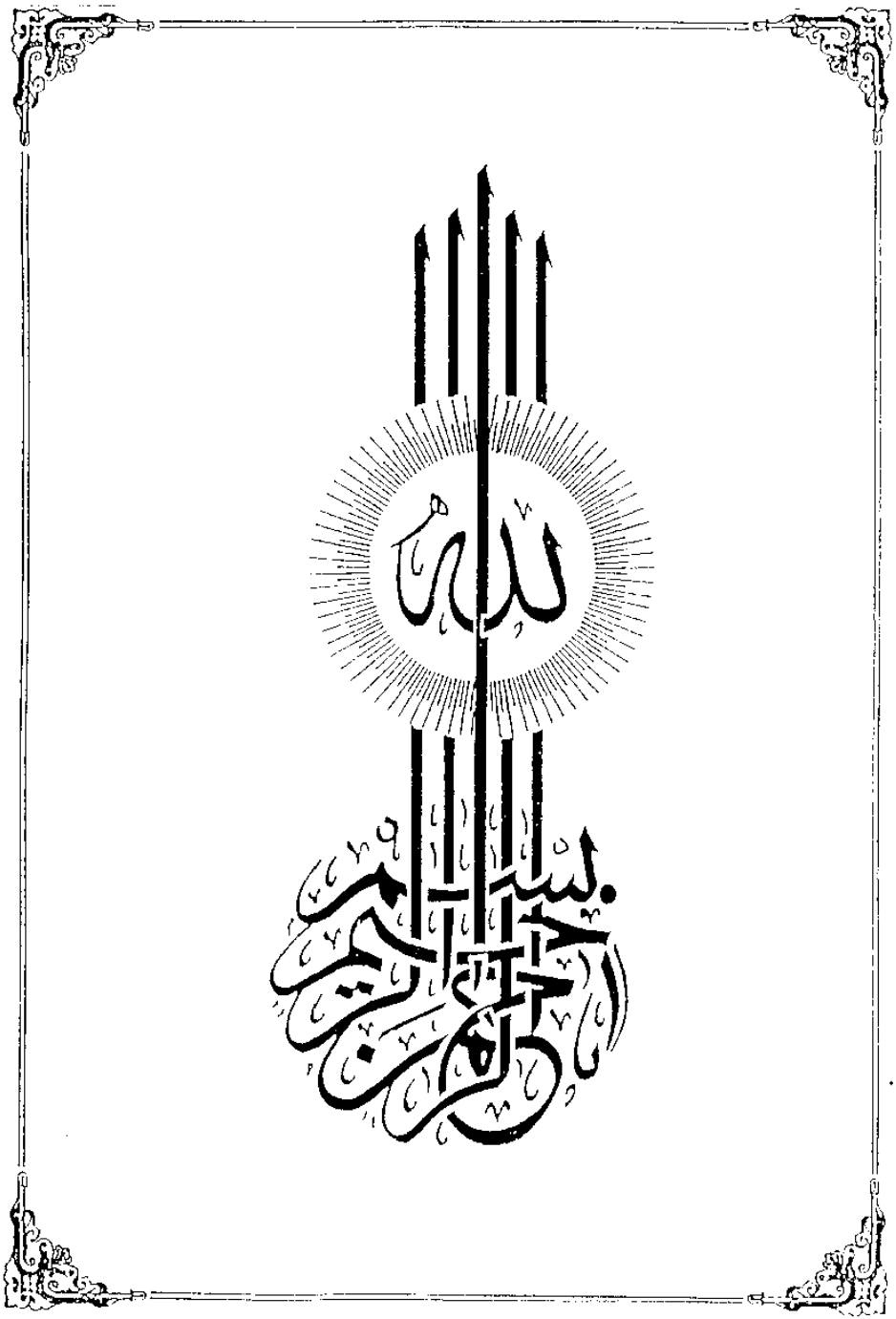
Supervised by

Prof. Dr. Mohamed Nabil Saleh
Faculty of Engineering, Ain Shams university

Ass. Prof. Dr. Ahmed El Osmany
Military Technical College

Ass. Prof. Dr. Safwat El Habiby
Military Technical College

Cairo 1996



بسم الله الرحمن الرحيم

وقل رب زدنى علما

صدق الله العظيم

سورة طه .. الآية ١١٤

Examiner Committee

Name, Title & Affiliation	*Signature*
of. Dr. Salwa Hussien El Ramly *n Shams University* *culty of Engineering*	Salwa H Ramly
of. Dr. Nabil Abdel Maksoud El Nady *formation Technology Institute*	
of. Dr. Mohamed Nabil Saleh *n Shams University* *culty of Engineering*	M. N. Saleh
ss. Prof. Dr. Ahmed El Osmany *Military Technical College*	Osmany

17 APR 1996

Statement

This dissertation is submitted to Ain Shams University for the degree of Ph.D. in Electrical Engineering (Electronics and communication Eng.).

The work included in this thesis was carried out by the author in the Department of Electronics and Communication Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or a qualification at any other University or Institution.

Date : 11/3/1996

Signature : M.N. ElSherbiny

Name : *M.N. Ahmed El Sherbiny*

Acknowledgment

I wish to express my senciere gratitude, deepest thanks and appreciation to :

1- **Prof. Dr. Mohamed Nabil Saleh**

2- **Ass.Prof. Dr. Ahmed El Osmany**

3- **Ass. Prof. Dr. Safwat El Habiby**

for their faithful supervision, helpful discussion and advise during the course of this thesis that made a large contribution to the fulfillment of this thesis.

Ain Shams University
Faculty of Engineering
Electronics and Communication Engineering Department

Summary
of the Ph.D. Thesis submitted by

Mohamed Nagib Ahmed El Sherbiny

Title of thesis

Public-Key Cryptography

Supervisors

Prof. Dr. Mohamed Nabil Saleh
Ass. Prof. Dr. Ahmed El Osmany
Ass. Prof. Dr. Safwat El Habiby

Registration Date : 7 - 12 - 1991

Examination Date : 17 - 4 - 1996

Summary

Public-Key Cryptography was born in May 1975, the child of two problems : the first is the key management problem and the second is the signature problem.

Since 1976, numerous public-key cryptography algorithms have been proposed. Many of these are insecure. Of the ones that are still considered secure, many are impractical. Either they have an impractically large key, or the

ciphertext is much larger than the plaintext. Only a few algorithms are both secure and practical. These are generally based on one of the hard problems (factorization - discrete logarithm problems). The most famous technique which is suitable for encryption/decryption, and digital signature is the Rivest-Shamir-Adleman (RSA) public-key cryptosystem. This thesis presents the RSA cryptosystem and describes the different approaches which are used to attack the RSA cryptosystem.

RSA cryptosystem must be used within a set of procedures known as a protocol which ensures that the algorithm will actually provide the security and/or authenticity required by the system. This thesis describes these protocols and presents some examples in which a protocol fails to provide the advertised level of security or authentication. From the analysis of these protocol failures, guidelines principles are extracted to develop the future protocols. We also propose a protocol used for mutual authentication and key exchange between users in a communication network.

RSA cryptosystem is based on the modular exponential function to encrypt or decrypt a message. The binary algorithm is the typical method to calculate this function and it is based on the binary representation of the exponent. We proposed the speed-up calculation of the modular exponential function by :

a) Decreasing the number of modular multiplications of the binary algorithm by, on average, 33%.
b) Reducing the time needed to calculate the modular multiplication by at least 50%.

RSA public-key cryptosystem needs large primes and any reasonably sized network needs lots of them. In this thesis, we present a fast probabilistic algorithm used for generation of random safe large prime numbers.

In this thesis, we present results for different times needed to encrypt and decrypt a message, with RSA cryptosystem, using different modular multiplications algorithms.

The main features of public-key cryptography are also described.

Abstract

Mohamed Nagib Ahmed El Sherbeny. "Public-Key Cryptography". Unpublished Doctor of Philosophy Dissertation, Ain Shams University, Faculty of Engineering, Cairo, Egypt.

This thesis is concerned with public-key cryptography. It concentrates on RSA Cryptosystem.

The thesis proposes a protocol used for key exchange and mutual authentication between users in a communication network. This protocol defeats the man-in-the-middle attack and chosen-ciphertext attack.

The thesis also presents the speed-up calculation of the modular exponential function by :

a) Decreasing the number of basic operations (modular multiplications) of the binary algorithm by, on average, 33%.

b) Reducing the time needed to calculate the modular multiplication by at least 50% using the modified systolic array..

The thesis also describes a proposed fast probabilistic algorithm used for generation of random safe large prime numbers.

The thesis also presents software implementation of the RSA cryptosystem using different modular multiplication algorithms, and computes time needed to encrypt and decrypt a message using these algorithms.