

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]

52160

By

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

Supervised by

Prof. Dr. Mohamed Habbil Saleh

Faculty of Engineering, Ain Shams university

Ass. Prof. Dr. Ahmed El Osmany

Military Technical College

Ass. Prof. Dr. Safwat El Habbib

Military Technical College

Cairo 1996

621382
M.N.







ଅବସ୍ଥା ଓ ପ୍ରାଣୀ ଜୀବନ

ଅବସ୍ଥା ଓ ପ୍ରାଣୀ ଜୀବନ

ଓଡ଼ିଆ ଶିକ୍ଷା ମାଧ୍ୟମ

ଅବସ୍ଥା ଓ ପ୍ରାଣୀ ଜୀବନ



Examiner Committee

Name, Title & Affiliation

Signature

Dr. Salwa Hussien El Ramly

Shams University
Faculty of Engineering

Dr. Nabil Abdel Maksoud El Nady

Information Technology Institute

Dr. Mohamed Nabil Saleh

Shams University
Faculty of Engineering

ss. Prof. Dr. Ahmed El Osmany

Military Technical College

17 APR 1996

Osmany

M. N. Saleh

El Nady

Salwa El Ramly



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. El Sherbiny*

Name : M.N. Ahmed El Sherbiny

the 1990s, the number of people in the world who are undernourished has increased from 600 million to 800 million (FAO 1996).

There are a number of reasons for this increase. First, the world population has increased from 5 billion in 1987 to 6 billion in 1996, with a further 2 billion projected by the year 2025 (FAO 1996). Second, the world population is ageing, with the proportion of the population aged 65 and over increasing from 7% in 1987 to 10% in 1996 (FAO 1996). Third, the world population is becoming more urban, with the proportion of the population living in urban areas increasing from 55% in 1987 to 60% in 1996 (FAO 1996).

Fourth, the world population is becoming more educated, with the proportion of the population aged 15 and over who are literate increasing from 55% in 1987 to 65% in 1996 (FAO 1996). Fifth, the world population is becoming more mobile, with the proportion of the population who are mobile increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Sixth, the world population is becoming more affluent, with the proportion of the population who are affluent increasing from 15% in 1987 to 25% in 1996 (FAO 1996).

Seventh, the world population is becoming more diverse, with the proportion of the population who are diverse increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Eighth, the world population is becoming more heterogeneous, with the proportion of the population who are heterogeneous increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Ninth, the world population is becoming more complex, with the proportion of the population who are complex increasing from 15% in 1987 to 25% in 1996 (FAO 1996).

Tenth, the world population is becoming more dynamic, with the proportion of the population who are dynamic increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Eleventh, the world population is becoming more innovative, with the proportion of the population who are innovative increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Twelfth, the world population is becoming more creative, with the proportion of the population who are creative increasing from 15% in 1987 to 25% in 1996 (FAO 1996).

Thirteenth, the world population is becoming more productive, with the proportion of the population who are productive increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Fourteenth, the world population is becoming more efficient, with the proportion of the population who are efficient increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Fifteenth, the world population is becoming more effective, with the proportion of the population who are effective increasing from 15% in 1987 to 25% in 1996 (FAO 1996).

Sixteenth, the world population is becoming more successful, with the proportion of the population who are successful increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Seventeenth, the world population is becoming more prosperous, with the proportion of the population who are prosperous increasing from 15% in 1987 to 25% in 1996 (FAO 1996). Eighteenth, the world population is becoming more wealthy, with the proportion of the population who are wealthy increasing from 15% in 1987 to 25% in 1996 (FAO 1996).

Acknowledgment

I wish to express my sincere 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.

[The page contains faint, illegible text, likely bleed-through from the reverse side of the document.]

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

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

multiplications algorithms.

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

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

least 50%.

b) Reducing the time needed to calculate the modular multiplication by at algorithm by, on average, 33%.

a) Decreasing the number of modular multiplications of the binary

function by :

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

users in a communication network.

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

the RSA cryptosystem.

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

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.

the 1990s, the number of people in the UK who are employed in the public sector has increased by 1.5 million, from 2.5 million in 1980 to 4 million in 1995.

There is a growing awareness of the need to improve the efficiency of the public sector. The Government has set a target of reducing the public sector borrowing requirement to zero by the year 2000. This has led to a number of initiatives to improve the efficiency of the public sector, including the introduction of competition and the restructuring of public services.

One of the main initiatives to improve the efficiency of the public sector is the introduction of competition. This has led to a number of public services being privatised, including the water supply, the electricity supply, and the telecommunications industry.

Another initiative to improve the efficiency of the public sector is the restructuring of public services. This has led to a number of public services being reorganised, including the health service, the education system, and the social security system.

These initiatives have led to a number of improvements in the efficiency of the public sector. However, there are still a number of challenges that need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000.

One of the main challenges is the need to improve the efficiency of the public sector. This can be achieved by a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

Another challenge is the need to improve the efficiency of the public sector. This can be achieved by a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.

These challenges need to be addressed in order to achieve the target of reducing the public sector borrowing requirement to zero by the year 2000. This will require a number of measures, including the introduction of competition, the restructuring of public services, and the improvement of public service delivery.