



شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
على هذه الأفلام قد أعدت دون أية تغييرات



يجب أن

تحفظ هذه الأفلام بعيدا عن الغبار

في درجة حرارة من 15-25 مئوية ورطوبة نسبية من 20-40%

To be Kept away from Dust in Dry Cool place of

15-25- c and relative humidity 20-40%



شبكة المعلومات الجامعية
التوثيق الالكتروني والميكروفيلم



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Encryption-Based Techniques For Computer Network Security

A Thesis
Submitted in Partial Fulfillment of the
Requirements of the Degree of
Master of Science in Electrical Engineering
Computer and Systems Engineering

Submitted by

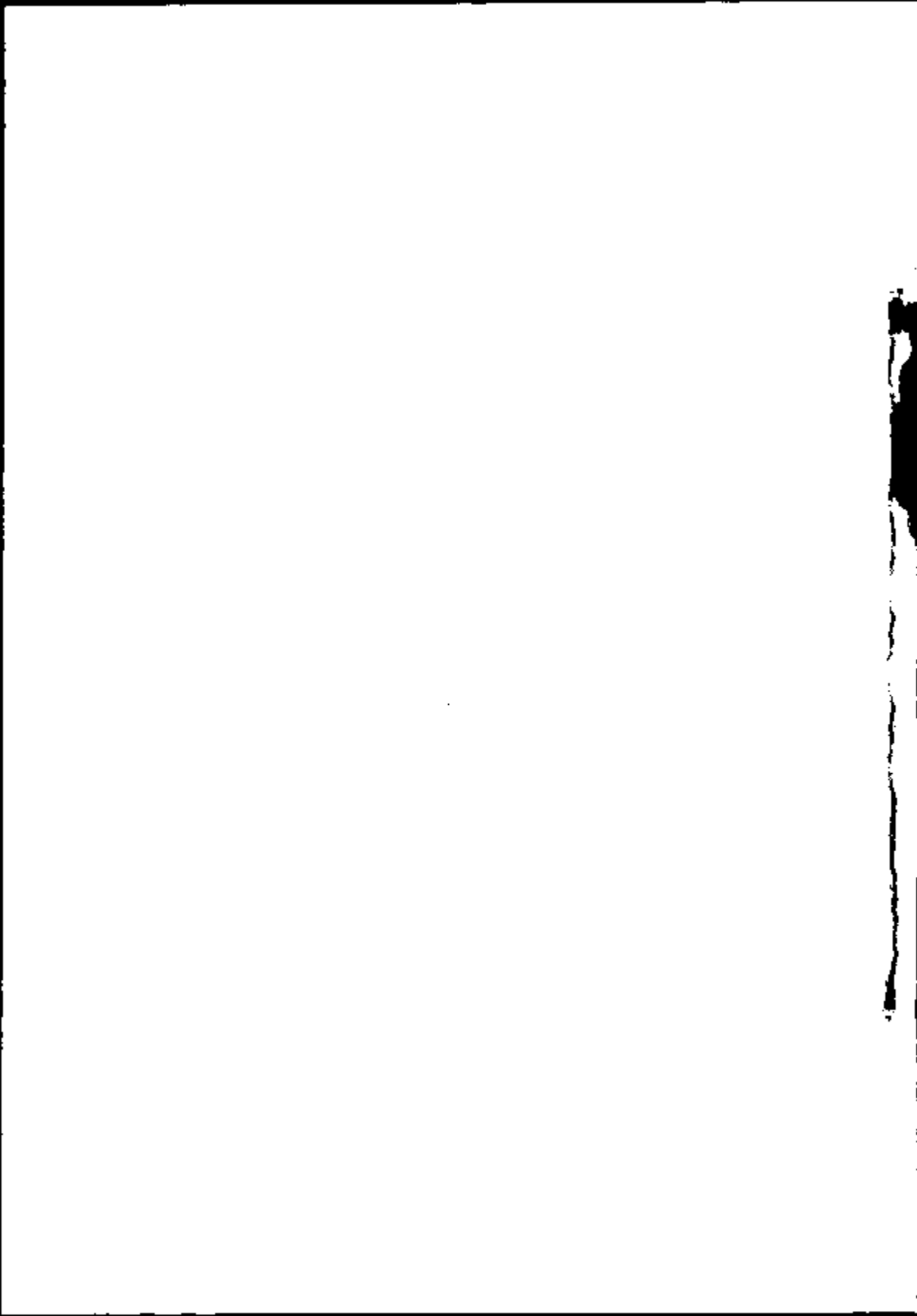
Mohammed Moustafa Mohammed

Supervised by

Prof. M.A.R. Ghonaimy
Professor of Computers
Faculty of Engineering
Ain Shams University

Dr. El-Sayed Aly El-Sayed El-Sakka
Chief Executive for IT
Al Shark Insurance Company

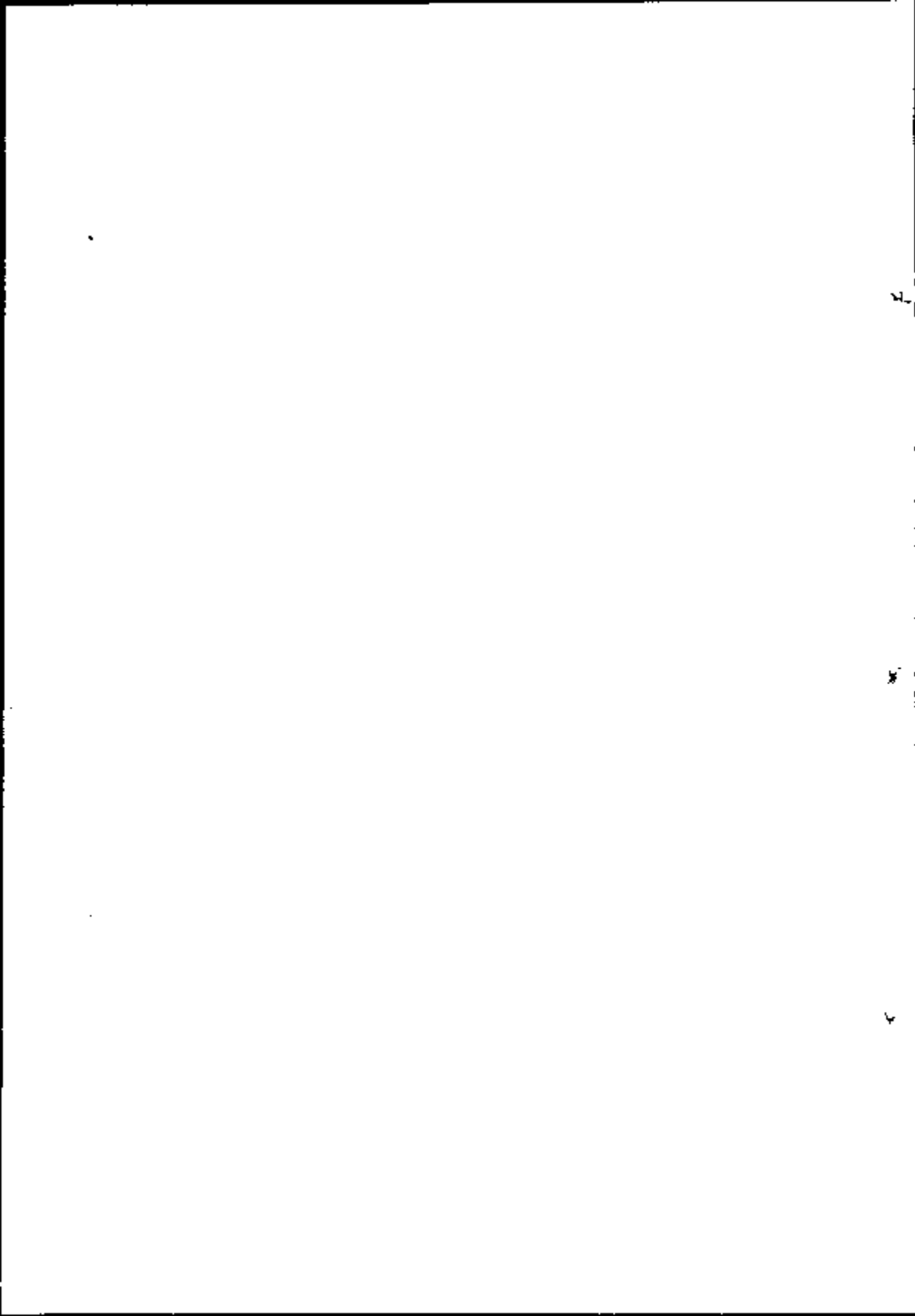
Cairo-1998



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قل هل ينبتكم بالأخسرين أعمالاً (١٠٢)
الذين ضل سعيهم في الحياة الدنيا وهم
يحتسبون أنهم يحسنون صنعا (١٠٣)

بِسْمِ اللَّهِ
صَلَّى
عَلَيْهِمْ



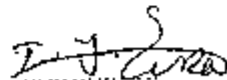
Approval Sheet

Name : Mohamed Mouslafa Mohamed Sayed
Title : Encryption-Based Techniques for Computer Network Security
Degree : Master of Science in Electrical Engineering
(Computer and Systems Engineering)

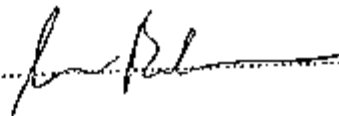
Examiners Committee

Name, Title and Affiliation _____ Signature

1- Prof. Ibrahim F. Eissa
Dean of Institute of Statistical Studies and Research
Cairo University, Cairo



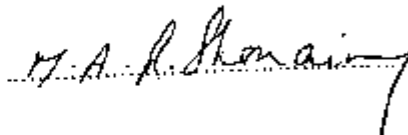
2- Prof. Osman A. Badr
Ain Shams University, Cairo
Faculty of Engineering
Computer and Systems Engineering Dept.



3- Dr. El-Sayed Aly El-Sayed El-Sakka
Chief Executive for IT
Al-Shark Insurance Company
Ph.D., Computer Engineering



4- Prof. M.A.R. Ghonaimy
Ain Shams University, Cairo
Faculty of Engineering
Computer and Systems Engineering Dept.



Date: / /1598

1900

100

100

100

100

100

Abstract

Mohammed Moustafa Mohammed: Encryption-Based Techniques
For Computer Network Security,
Ain Shams University, 1998.

This thesis discusses the problems of computer security. It survey different areas of computer security where points of security vulnerability are stated. also methods of protection are mentioned. It is clear that Computer Networks increase the problems of computer security. Lack of physical proximity, use of insecure shared media, and difficulty to identify remote users is some of security problems that are made more difficult in Computer Networks.

Basic encryption systems: Classification of the decryption algorithms is presented. Private key algorithms and public key algorithms were emphasized. Details description and analysis, suitability of use, C programs, mathematical approach for the most famous algorithms, represents the state of the art of encryption field. These algorithms are RSA (Rivest Shamir Adelman), LUC algorithm, the Merkle-Hellman Knapsack, the Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA). In addition, modern applications of the public key systems have been presented.

Hashes Functions which are used to add layers of security over the existing systems different famous algorithms are presented, they are simple hash, message authentication code (MAC), message digest (MD4), while studying and analysis for (MD4) is done. Comparison between these techniques is demonstrated. Also other technique adds other layer of security is discussed this is restricted character set (RCS)

Proposed secure message communication system for Computer Networks. Introduce message security requirements, which are message confidentiality, integrity, and authentication. Two different way to achieve message security, they are encryption algorithms and hash functions. Multilevel secure system is proposed. A developed applicable arithmetic functions to manipulating large numbers within encryption algorithms is presented.

Much insight has been gained in this study about encryption techniques for Computer networks. It is believed that using public algorithms for data encryption is undesirable while the main usage is in digital signature and key management. However in cooperation with single key systems to achieve better performance

Keywords : Encryption, Computer Security, Computer Networks, DES, RSA, IDEA, LUC, Public Key, Centralized Control, Hash Function, MD2, MD4, MD5, Local Character Set, PGP, PEM, Kerberos, PRZ, Internet Security, E-mail Security

10
a

Statement

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering (Computer and Systems Engineering).

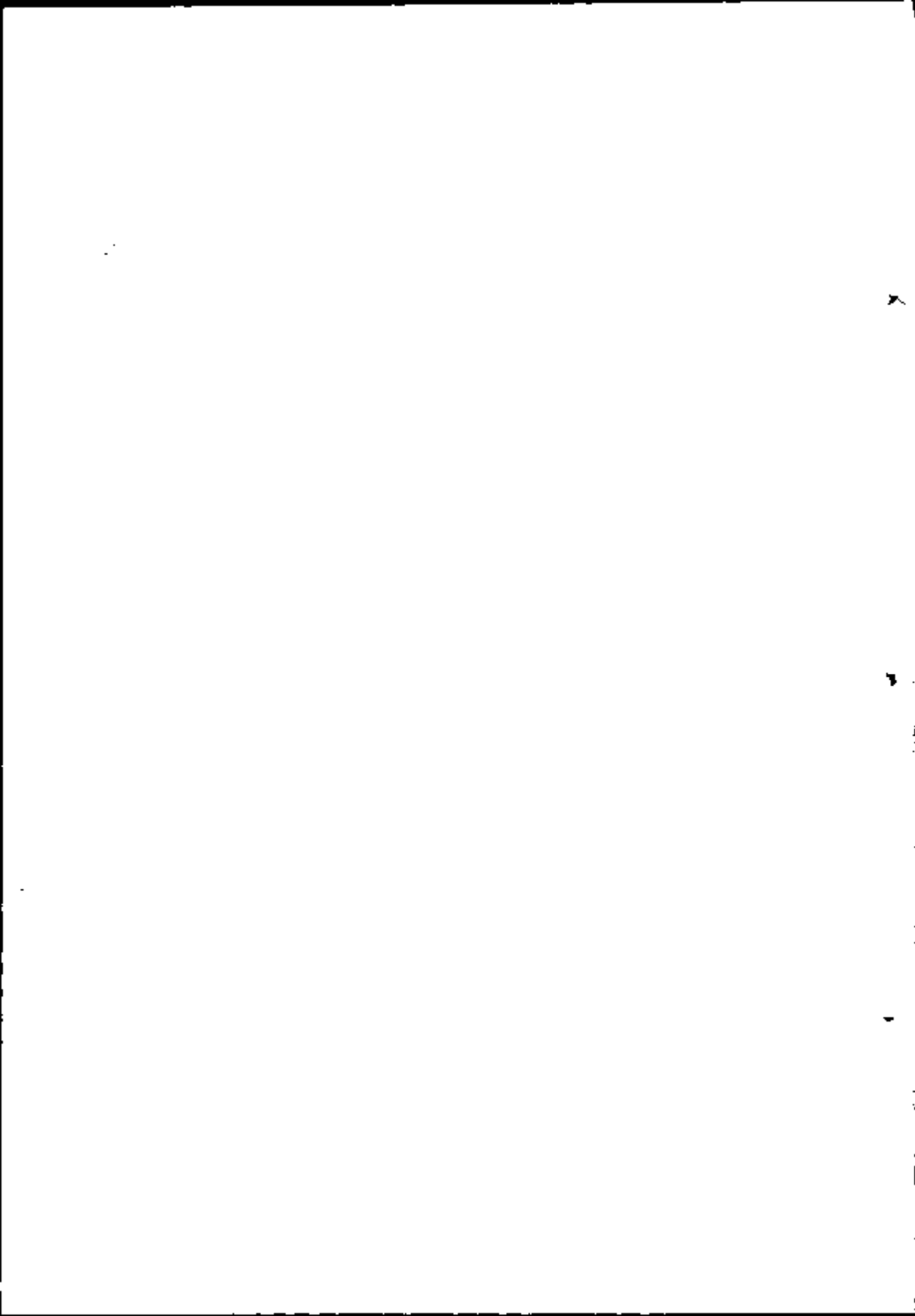
The work included in this thesis was carried out by the author at the Computer and Systems Engineering Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date 24 / 5 / 1998

Signature : 

Name : Mohammed Moustafa Mohammed



Acknowledgments

At first, I thank God who helped me greatly in this work and in any other good and beneficial work.

I would like to express my gratitude to Professor M.A.R. Ghonaimy for having the trouble to help me by devoting much of his effort and time, and for his continual guidance and tremendous encouragement.

I also appreciate very much the support given by Dr. Sayed El-Sakka during all phases of study.

I would like to express my sincere gratitude to all those who have helped me during the writing of this thesis.

A very special dedication to Dr. Refat Al-Jefny for his support during thesis preparation.

Finally, I do highly appreciate all those who have been encouraging and motivating me.

Summary

This Thesis is concerned with the study of Encryption-Based Techniques for Computer Network Security. It consists of 6 chapters

Chapter 1 survey of computer security – what it is, where it came from, where it's going, and why we should care about it. It introduces the many different areas of security in clear and simple terms. It summarizes the threats to computers and networks and Methods of protection for computer system.

Chapter 2 Survey and Programming of Basic and Advanced Encryption Algorithms. Private key algorithms and public key algorithms. History of encryption and demonstration of basic trivial algorithms used before computer revolution. Detailed description and analysis, suitability of use, C programs, mathematical approach for the most famous algorithms, represents the state of the art of encryption field. These algorithms are RSA (Rivest Shamir Adelman), LUC algorithm, the Merkle-Hellman Knapsack, the Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA). Also modern applications of the public key systems has been presented. Other security enhancement functions are discussed. Hashes Functions, different famous algorithms used to enhance computer security are presented. They are simple hash, message authentication code (MAC), message digest (MD4), while studying and analysis for (MD4) is done. Comparison between these techniques is demonstrated.

Chapter 3 Introduction to network security. It discusses the most widely used systems that have been developed to support application-level security functions for electronic mail. Two systems with similar technology but very different philosophies seem likely to dominate this area : Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM). Also, the enhanced mail system developed by technical university of Berlin is demonstrated together with Kerberos system which provides authentication service for computer networks.

Chapter 4 Study of LUC : A new published public key algorithm. A complete presentation for LUC algorithm, comparative analysis with RSA algorithm. A group of arithmetic functions have been developed for large numbers which are used to implement both RSA and LUC.

Chapter 5 A Proposed Secured Messaging System. A centralized secure message system for computer networks has proposed, which utilize all security tools to design and implement multilevel security system suitable to use by military and government agencies.

Chapter 6 Conclusions, Recommendations, and Future Work. It concludes the thesis by summarizing the results obtained and indicating the future direction of computer network security.

Appendices Developed Codes for Different Algorithms and Functions. All developed source codes for different encryption algorithms discussed in the study divided in to two main appendices. Appendix A for basic encryption systems and Appendix B for modern encryption systems. In addition to, proposed system implementation C code.

Table of Contents

1	Computer Vulnerabilities and Protection : A Survey.	1
1.1	Types of Security Breaches.	1
1.2	Points of Security Vulnerability.	2
1.2.1	Attacks on Hardware.	3
1.2.2	Attacks on Software.	3
1.2.2.1	Software Deletion.	3
1.2.2.2	Software Modification.	3
1.2.2.3	Software Theft.	4
1.2.3	Attacks on Data.	4
1.2.3.1	Threats to Data Secrecy.	5
1.2.3.2	Threats to Data Integrity.	5
1.2.4	Attacks on Storage Media	5
1.2.5	Attacks on Networks.	6
1.2.6	Security and People.	6
1.3	Methods of Protection.	7
1.3.1	Hardware Control.	7
1.3.2	Software Control.	7
1.3.3	Encryption.	7
1.3.4	Policies.	8
1.3.5	Physical Control.	8
1.4	Conclusion.	8
2	Survey and Programming of Basic and Advanced Encryption Algorithms.	
2.1	Introduction.	9
2.2	Basic Types of Encryption Schemes.	9
2.2.1	Substitution.	9
2.2.1.1	Monalphabetic Cipher.	9
2.2.1.1.1	Caesar Cipher.	10
2.2.1.1.2	Permutation.	10
2.2.1.2	Polyalphabetic Substitution Cipher.	10
2.2.1.2.1	Vigenere Tableau.	11