



شبكة المعلومات الجامعية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ





شبكة المعلومات الجامعية



شبكة المعلومات الجامعية

التوثيق الالكتروني والميكرو فيلم

جامعة عين شمس

التوثيق الالكتروني والميكرو فيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأفلام قد اعدت دون أية تغيرات



يجب أن

تحفظ هذه الأفلام بعيداً عن الغبار

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

To be kept away from dust in dry cool place of
15 – 25c and relative humidity 20-40 %



شبكة المعلومات الجامعية



بعض الوثائق الأصلية تالفة



شبكة المعلومات الجامعية



بالرسالة صفحات
لم ترد بالأصل

Evaluation of Different Encryption Algorithms in English and Arabic Languages

A Thesis Submitted to the
Faculty of Engineering at Cairo University
In Partial Fulfillment of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
ELECTRONICS AND COMMUNICATIONS ENGINEERING

FACULTY OF ENGINEERING, CAIRO UNIVERSITY

GIZA, EGYPT

March 2001

B
1-292

Evaluation of Different Encryption Algorithms in English and Arabic Languages

A Thesis Submitted to the
Faculty of Engineering at Cairo University
In Partial Fulfillment of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
ELECTRONICS AND COMMUNICATIONS ENGINEERING

BY
Ayman Mohamed Diao El Deen El Tantawy

Supervised by

Prof. Dr. Abdel Halim M. Shousha
Electronics & Communications
Dept. Faculty of Engineering
Cairo University

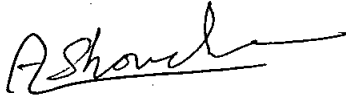
Prof. Dr. Reda Hussein Seireg
Technical Research Center of
Armed Forces

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
March 2001

Evaluation of Different Encryption Algorithms in English and Arabic Languages

A Thesis Submitted to the
Faculty of Engineering at Cairo University
In Partial Fulfillment of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY
in
ELECTRONICS AND COMMUNICATIONS ENGINEERING

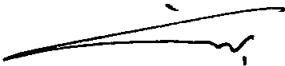
Approved by the
Examining Committee



Prof. Dr. Abdel Halim M. Shousha, Thesis Main Advisor



Prof. Dr. Ayman Ibrahim Eldesouky



Prof. Dr. Magdy Fikry Mohamed



Prof. Dr. Reda Hussein Seireg

FACULTY OF ENGINEERING, CAIRO UNIVERSITY

GIZA, EGYPT

March 2001

Table of Contents

List of Tables	viii
List of Figures	ix
Abbreviations	xi
Acknowledgement	xii
Abstract	xiii
Chapter 1 : Introduction	1
1.1 Historical Background	1
1.2 Fundamental Concept of Cryptosystems	2
1.3 Cryptographic Attacks	4
1.3.1 Ciphertext only attack:	4
1.3.3 Chosen plaintext attack:	4
1.3.4 Exhaustive attack:	5
1.3.5 Analytic attack	5
1.3.6 Statistical Attack	
1.4 Deliberate Threats to Information	5
1.5 Security Services	7
1.6 Problem Formulation	8
1.7 Summary	11
Chapter 2 : Network and Computer security	13
2.1 Security Threats in Computer Networks:	15
2.1.1 Passive Threats	15
2.1.2 Active Threats	16
2.2 Security Services	18
2.2.1 Confidentiality	19
2.2.2 Authentication	19
2.2.3 Data Integrity	20
2.2.4 Nonrepudiation	20
2.2.5 Access Control	20
2.3 Security Mechanisms	20
2.3.1 Encryption	21
2.3.2 Digital Signature	21
2.3.3 Access Control Techniques	23
2.3.4 Data Integrity Mechanisms	25
2.3.5 Authentication Mechanisms	25
2.3.6 Traffic Padding	25
2.3.7 Routing Control	25
2.3.8 Notarization	25

Chapter 3 : Algorithms for Computer Security	27
3.1 Encryption Methods	29
3.1.1 Substitution Ciphers	29
3.1.2 Transposition Ciphers	31
3.1.3 One-Time Pads	32
3.1.4 Two Fundamental Cryptographic Principles	33
3.1.5 Secret-Key Algorithms	35
3.1.6 Data Encryption Standard (DES)	36
3.1.7 DES Chaining	38
3.1.8 Breaking DES	42
3.1.9 IDEA	44
3.1.10 Digital Signatures with Symmetric Key Encryption	45
3.1.11 Asymmetric Encryption	46
3.1.12 Public-Key Algorithms	47
3.1.13 The RSA Algorithm	49
3.1.14 Other Public Key Algorithms	51
3.2 Authentication Protocols	51
3.2.1 Authentication Based on a Shared Secret Key	52
3.2.2 Establishing a Shared Key: The Diffie-Hellman Key Exchange	56
3.2.3 Authentication Using a Key Distribution Centre	59
3.2.4 Authentication Using Kerberos	63
3.2.5 Authentication Using Public Key Cryptography	65
3.3 Digital Signatures	67
3.3.1 Secret-Key Signatures	68
3.3.2 Public-Key Signatures	69
3.4 The Integer Factorization Problem (IFP)	71
3.5 Known attacks	72
3.6 Message Digests	74
 Chapter 4 : Modelling Techniques	 78
4.1 Simulation Modelling Perspectives	78
4.1.1 Discrete simulation	79
4.1.2 A continuous simulation model	79
4.2 Discrete Simulation Modelling	81
4.2.1 Event Orientation	82
4.2.2 Activity Scanning Orientation	82
4.2.3 Process Orientation	82
4.3 Continuous Simulation Modelling	83
4.4 Combined Discrete-Continuous Models	84
4.5 Petri Net Models	85
4.6 Advanced Techniques	86

Chapter 5 : Dynamic Behaviour of Different Algorithms	87
5.1 Cryptographic Security Evaluation of Hash functions	89
5.2 Evaluating Security Scheme	90
5.2.1 Design Goals and Assumptions	90
5.2.2 Description of the ESS scheme	91
5.2.2.1 By Scaling Down	92
5.3 Cryptographic Evaluation of MD4 using the ESS scheme	96
5.3.1 Scaling down the MD4 algorithm	97
5.3.2 Constructing the Transition Probability Matrix TPM	99
5.3.3 Calculating Inversion and Collision Probabilities	125
5.3.4 Transient Behaviour	127
5.4 Probability of Occurrence of English Letters	129
5.5 Probability of Occurrence of Arabic Letters	136
5.6 Applying MD4 on English Language Letters	137
5.7 Applying MD4 on Arabic Language Letters	140
5.8 Evaluation of MD5	142
5.9 Differences between MD4 and MD5	144
5.10 Cryptographic Evaluation of MD5 using the ESS Scheme	144
5.10.1 Scaling down the MD5 algorithm	145
5.10.2 Constructing the Transition Probability Matrix TPM	146
5.10.3 Applying MD5 on English Language Letters	153
5.10.4 Applying MD5 on Arabic Language Letters	154
Chapter 6 : Circular and SE Hash Functions	156
6.1 Circular Transition Probability Matrix	156
6.2 Evaluating Circular Hash Function Using ESS Scheme	157
6.2.1 Transient behaviour for Circular Hash Function	158
6.2.2 Limiting State Behaviour of Circular Hash Function	165
6.2.3 Comparison between MD4 and Circular Hash Functions	166
6.3 SE Transition Probability Matrix	166
6.4 Evaluating SE Hash Function using ESS Scheme	168
6.4.1 Transient behaviour for SE Hash Function	168
6.4.2 Limiting State Behaviour for SE Hash Function	173
6.5 Comparison Between MD4 and SE Hash Function	173
Chapter 7 : Quantitative Analysis of Different Algorithms	176
7.1 Markov Process Model	176

7.2 Dynamic Behaviour of Markov Process	178
7.3 Steady State behaviour of the Model	179
7.4 Shortest Message Length for MD4	181
7.4.1 Round 1	181
7.4.2 Round 2	181
7.4.3 Round 3	182
7.5 Shortest Message Length for MD5	182
7.5.1 Round 2	182
7.5.2 Round 4	182
7.6 Shortest Message Length for Circular Function	182
7.7 Shortest Message Length for SE Function	183
7.8 Comparison between the Shortest Message for all Algorithms	183
7.9 The Kronecker Product	186
Chapter 8 : Conclusions and Future Work	194
8.1 Qualitative Comparison between MD4 and MD5	194
8.2 Quantitative Comparison between MD4 and MD5	196
8.3 Using SE matrix as a base for Encryption algorithm	196
8.4 Conclusion	197
8.5 Recommendations for Future Work	198
References	199
Appendices	204
Appendix A: Shortest Message Length	204
Appendix B: Calculated Matrices for Different Algorithms	214