

بسم الله الرحمن الرحيم





شبكة المعلومات الجامعية التوثيق الالكتروني والميكروفيلم



جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



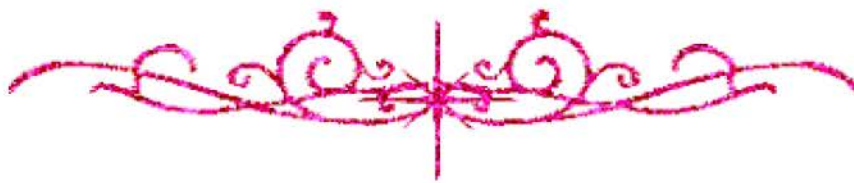


بالرسالة صفحات
لم ترد بالأصل





بعض الوثائق الأصلية تالفة



B11880

A Hybrid Encryption Technique For Increasing Data Security

By

Engineer: Mohamed Gamal El-Din Abdelhamid

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

**FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
1999**

A Hybrid Encryption Technique For Increasing Data Security

By

Engineer: Mohamed Gamal El-Din Abdelhamid

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

Under Supervision of

**Prof. Dr. Abdel Halim Shousha
Electronics and Communications
Department**

**Prof. Dr. Nevin Darwish
Computer Engineering Department**

Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY

GIZA, EGYPT

1999

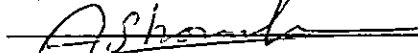

A Hybrid Encryption Technique For Increasing Data Security

By


Engineer: Mohamed Gamal El-Din Abdelhamid

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

Approved by the Examining Committee

 
Prof. Dr. Abdel Halim Shousha - Prof. Dr. Nevin Darwish, Thesis Main Advisors

Prof. Dr. Amin Mohamed Nassar, Member



Prof. Dr. Ayman El Desouki, Member



FACULTY OF ENGINEERING, CAIRO UNIVERSITY

GIZA, EGYPT

1999

List Of Figures

Figure 2.1	Authentication Approaches
Figure 2.2	Polonius Authentication Scheme
Figure 2.3	Identification and Authentication before User Session
Figure 2.4	Authentication During User Session
Figure 2.5	Access Matrix Model
Figure 2.6	Example Open Routine
Figure 2.7	Open Routine with MAC
Figure 2.8	Operational View of MAC Implementation
Figure 2.9	UNIX System V/MLS Mandatory Access Control
Figure 2.10	Confidentiality Preservation in Different Environments
Figure 2.11	Two Alternative Sequence Integrity Mechanisms
Figure 2.12	Security Transformation Model
Figure 2.13	Protocol Control Information
Figure 2.14	Key Management Communications
Figure 2.15	Originator's Digital Signature
Figure 2.16	Trusted Third Party Digital Signature
Figure 2.17	Trusted Third Party Token
Figure 2.18	In-Line Trusted Third Party - Evidence Stored
Figure 2.19	In-Line Trusted Third Party - Evidence Forwarded
Figure 3.1	Encryption and Decryption
Figure 3.2	Basic DES Functionality
Figure 3.3	DES Algorithm Sketch
Figure 3.4	S-Box Substitution
Figure 3.5	Disclosure Attack to Remote Communications
Figure 3.6	Masquerading Attack
Figure 3.7	Integrity Attack to Remote Communications
Figure 3.8	Private Key Protocol

Figure 3.9	Public Key Protocol
Figure 3.10	Arbitrated Routing Protocol
Figure 3.11	Arbitrated Communication Establishment Protocol
Figure 3.12	Kerberos Authentication Protocol
Figure 3.13	Centralized Key Distributor
Figure 4.1	DES Block Diagram
Figure 4.2	Key schedule calculation
Figure 4.3	Enciphering computation.
Figure 4.4	Calculation of $f(R,K)$
Figure 4.5	Electronic Codebook (ECB) Mode
Figure 4.6	Cipher Block Chaining (CBC) Mode
Figure 4.7	K-Bit Cipher Feedback (CFB) Mode
Figure 4.8	K-Bit Output Feedback (OFB) Mode
Figure 4.9	DES/RC5 Cascade Block Diagram
Figure 4.10	Image before Encryption
Figure 4.11	Image after Applying Encryption
Figure 5.1	Probability Of occurrence of Input and Output hamming distance (DES)
Figure 5.2	Probability Of occurrence of the encryption key and Output hamming distance (DES)
Figure 5.3	Probability Of occurrence of Input/Output hamming Distance (RC5)
Figure 5.4	Probability of Occurrence of KEY/OUTPUT hamming Distance (RC5)
Figure 5.5	Probability Of occurrence of Output1/Output2 hamming Distance (DES) (Due to input change)
Figure 5.6	Probability Of occurrence of Output1/Output2 hamming Distance (DES)(Due to key change)

- Figure 5.7 Probability Of occurrence of Output1/Output2 hamming Distance (RC5) (Due to input change)
- Figure 5.8 Probability Of occurrence of Output1/Output2 hamming Distance (RC5) (Due to input change)
- Figure 5.9 Probability Of occurrence of Input/Output hamming Distance (DES/RC5-56bit Cascade)
- Figure 5.10 Probability Of occurrence of the DES key/Output hamming Distance (DES/RC5-56bit Cascade)
- Figure 5.11 Probability Of occurrence of the RC5 key/Output hamming Distance (DES/RC5-56bit Cascade)
- Figure 5.12 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-56bit Cascade) (Due to input change)
- Figure 5.13 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-56bit Cascade) (Due to DES key change)
- Figure 5.14 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-56bit Cascade) (Due to RC5 key change)
- Figure 5.15 Probability Of occurrence of Input/Output hamming Distance (DES/RC5-128bit Cascade)
- Figure 5.16 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-128bit Cascade) (Due to input change)
- Figure 5.17 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-128bit Cascade) (Due to DES key change)
- Figure 5.18 Probability Of occurrence of Output1/Output2 hamming Distance (DES/RC5-128bit Cascade) (Due to RC5 key change)
- Figure 5.19 Probability Of occurrence of Output1/Output2 hamming Distance (comparison between DR-CAS & DD) (Due to key change)
- Figure 5.20 Probability Of occurrence of Output1/Output2 hamming Distance (comparison between DR-CAS & DD) (Due to input change)

- Figure 5.21 Probability Of occurrence of Output1/Output2 hamming Distance
(Double-DES Cascade) (Due to input change)
- Figure 5.22 Probability Of occurrence of Output1/Output2 hamming Distance
(Double-DES Cascade) (Due to DES-1 key change)
- Figure 5.23 Probability Of occurrence of Output1/Output2 hamming Distance
(Double-DES Cascade) (Due to DES-2 key change)