بسم اللّه الرحمن الرحيم

شبكة المعلومات الجامعية
التوثيق الالكتروني والميكروفيلم

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING

Electronics and Communications Engineering Department

Data Communication Ciphering Systems
"Analysis of Block Cipher Systems"

A Thesis

Submitted in Partial Fulfillment for the Requirements
of the Degree of Master of Science in Electrical Engineering
(Electronics and Communications Engineering)

Submitted By

Atef Hosny Soliman

B.Sc. of Electrical Engineering
(Electronics and Communications Engineering)
Military Technical College, 1985

Supervised By

Prof. Dr. Salwa Hussein El-Ramly
Dr. Talaat Abdel Latief El-Garf

Cairo-2000

EXAMINERS COMMITTEE

ame : **Atef Hosny Soliman**

hesis : **Data Communications Ciphering Systems**
"Analysis of Block Cipher Systems"

egree : **Master of Science in Electrical Engineering**

(Electronics and Communications Engineering)

Name, Title, and Affiliation	**Signature**
Prof. Dr. M. Marzouk M. Ibrahim Emer: Prof, Faculty of Eng., Ain Shams University, Cairo.	M. Marzouk Ibrahim
Prof. Dr. Nabil Abdel Maksoud EL-Nady Ain Shams University, Cairo Military Technical College, Cairo.	
Prof. Dr. Salwa Hussein El-Ramly Ain Shams University, Cairo Faculty of Engineering.	Salwa El Ramly
Dr. Talaat Abdel Latief El-Garf Cipher Department Signal Corps.	Talaat

Date:28/8/2000

STATEMENT

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

The work included in this thesis was carried out by the auther at the Electronics and Communications Engineering Department, Faculty of Engineering, Ain Shams University.

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

Date : 28/8/ 2000
Signature :
Name :Atef Hosny Soliman

ACKNOWLEDGMENT

All gratitude is due to ALLAH. Thence, the author wishes to express his deepest gratitude and thanks to Prof. Dr. Salwa Hussien EL-Ramly, Ain Shams University, for her valuable advice, extensive assistance, constructive ideas and encouragement during the course of the thesis, that made a large contribution of the fulfillment of this thesis.

The author wishes to express his sincere thanks and appreciation to Dr. Talaat Abdel Latief EL-Garf for the supervision, useful assistance, inspiration, encouragement, helpful suggestions and guidance during the study and fulfillment of this work.

The author also wishes to express his gratitude to all the staff members of the Electronics and Communications Engineering Department for their kind help.

Abstract

Atef Hosny Soliman. Data Communication Ciphering Systems "Analysis of Block Cipher Systems". Master of Science dissertation, Ain Shams University,

Communication Systems are vulnerable to passive wiretapping (Eavesdropping) which threats secrecy and active wiretapping (Tampering) which threats authenticity. This thesis is devoted to study and analyze Block Cipher techniques applied in Data Communication Ciphering Systems.

Early Cipher Systems including Substitution and Transposition Ciphers are presented. Modern Cipher Systems including Stream Cipher Systems, Block Cipher Systems and Public Key Cryptosystems are studied.

Block Cipher Systems are studied and analyzed. A Complete package of different elements which affect the security level of Block cipher Systems is presented in this thesis.

A Complete package of the significant statistical tests for local Randomness is presented in this thesis including mathematical description.

A new proposed method to build up dynamic

Look-Up-Tables (S-boxes) changing with every change of the secret key is presented in this thesis, in addition to the computer simulation programs. This new approach will lead to build up more secure Block Cipher Systems with dynamic change S-boxes and consequently solve the problem of the fixed structure Block Ciphers.