ELECTRONIC CRYPTOGRAPHY SYSTEMS

MAN MOHAN KAKAR

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, DELHI

JANUARY, 1982

ELECTRONIC CRYPTOGRAPHY SYSTEMS

By

MAN MOHAN KAKAR
ELECTRICAL ENGINEERING DEPARTMENT

Submitted

In fulfilment of the requirements of the
Degree of Doctor of Philosophy
to the
Indian Institute of Technology, Delhi

January, 1982.

C E R T I F I C A T E

This is to certify that the thesis entitled "Electronic Cryptography Systems" being submitted by Mr. M.K. Kakar to the Indian Institute of Technology, New Delhi, for the award of the degree of Doctor of Philosophy is a record of bonafide research work carried out by him under my guidance and supervision.

The results contained in this thesis have not been submitted in part or in full, to any other University or Institute for the award of any degree or diploma.

(M. IBRAHIMSHA)
Thesis Supervisor

January, 1982.

ABSTRACT

The overall aim of this dissertation is to assess the degree of security offered by the important possible electronic cryptographic systems and to examine possible improvements in the systems in use. After introducing the basic concepts of a cryptographic system in chapter I, a summary of results and findings of this work is given in chapter II. Chapter III and IV describe the different shift register configurations possible for use in crypto-systems and the existing known methods for their solution. Chapter V briefly describes an attempted approach for the solution of non-linear feedback shift registers, which did not prove successful. An analytical approach for the solution of non-linear feedback shift registers has been evolved during the course of this work and is described in chapter VI. Chapter VII gives an interpretation of this approach, which leads to the number of key bits required for solution by the approach evolved. Chapter VIII discusses the capabilities of this approach. Chapter IX describes the possible improvements in the shift register systems in common use now-a-days, keeping in view the cryptographic weakness of these systems against the approach evolved. Chapter X introduces the basic concepts of information lossless machines and chapter XI examines the characteristics of these machines in relation to their use in crypto-system. In view of the promise of

higher order information lossless machines giving better crypto-systems, the maximum order achievable by a N-state machine has been investigated in chapters XII, XIII and XIV, wherein a new representation of sequential machines has been evolved in chapter XII. Chapter XV gives two suggested configurations of information lossless machines for use as cryptosystems. Chapter XVI examines the use of one-way functions for cryptography purposes, in comparison with the existing systems. In chapter XVII some suggestions have been given for future investigations in areas connected with electronic cryptographic systems.

CONTENTS