Basic Methods of Cryptography

Basic Methods of Cryptography

Jan C.A. VAN DER LUBBE
Associate Professor
Information Theory Group
Department of Electrical Engineering
Delft University of Technology

Translated by Steve Gee

Delft Academic Press / VSSD

Published by:
Delft Academic Press / VSSD
Leeghwaterstraat 42, 2628 CA Delft, The Netherlands
tel. +31 15 27 82124, e-mail: hlf@vssd.nl
www.delftacademicpress.nl

ISBN Ebook 978-90-6562-239-6
NUR 983

Keywords: cryptography.

Contents

Preface

As a result of current technological developments, the computer can now be found in all layers of our society and the possibilities for communication have grown immensely. At present, information is being communicated and processed automatically on a large scale. There are numerous examples: medical or fiscal computer files, automatic banking, video-phone, pay-tv, facsimiles, tele-shopping, global computer networks, etc. All these examples increasingly require measures for secure storage and transportation of the information. There are many reasons for this growing need. Protection of the information may be necessary to guard economic interests, to prevent fraud, to guarantee the privacy of the citizen, etc.

Cryptology is the science which is concerned with methods of providing secure storage and transportation of information in its widest sense.

In this book we will cover the fundamentals of secure storage and transportation of information, as they are currently being developed and used. The objective of this book is to allow the reader to become acquainted which the various possibilities of cryptology, and also with the impossibilities and necessary conditions involved in the use of cryptology.

This book is written for anyone who is in some way or other involved in protecting information processing and communication: engineers, system designers, application programmers, information analysts, security officers, EDP-auditors, etc.

This book has resulted from lectures given by the author to students of the Faculties of Electrical Engineering, Technical Mathematics and Informatics, Systems Engineering and Policy Analysis and Applied Physics of the Delft University of Technology and from the course in cryptology provided by TopTech Studies, which is responsible for the post-doctoral courses of the Delft University of Technology, and of which the author is the director.

The author wishes to thank dr.ir. J.H. Weber for his assistance during the lectures in cryptology at the Delft University of Technology and also all his TopTech cryptology course colleagues (in particular ir. R.E. Goudriaan of

the International Nederlanden Bank), as they have taught the author a great deal about the practical aspects of the use of cryptology.

Delft J.C.A. van der Lubbe
May 1997

Abstract

Chapter 1 focuses mainly on the role of cryptology within the total field of security. We will examine the various objectives of security and an initial summary of the available cryptographic methods is provided.

In Chapter 2 we will deal with the more classical forms of cipher systems, such as the transposition and the substitution ciphers. In addition, we will also take a look at the methods employed by cryptanalysts ('hackers') for cracking existing security measures.

In many cases, the strength of a cryptographic algorithm depends almost entirely on the obtainable level of security. However, since the term 'security' is itself far from clear, in Chapter 3 we will first deal with the concept of security, using terms from the field of information theory, and we will also pay attention to how security can be achieved.

One of the currently most popular cryptographic algorithms, which is based on enciphering with secret keys, is the DES algorithm. The principles of this algorithm are explained in Chapter 4.

Chapter 5 focuses on the use of shift registers for providing pseudorandom sequences, which can be used for generating keys as well as enciphering bit streams. In this chapter we will also study the term 'randomness'.

Chapter 6 is concerned with so-called public key systems; cryptographic algorithms with a secret and a public key. The RSA algorithm is an important example of such a system.

Chapter 7 deals with other types of cryptographic protection concerned with authentication and integrity. These items involve techniques which enable us to determine whether a transmitted message is intact and whether a message purported to be transmitted by some entity was really transmitted by that entity. Amongst other things we will examine digital signatures and zero knowledge techniques for identification.

In general ,we can say that no matter how good our cryptographic algorithms may be, the overall security always relies on the extent to which the secret keys remain secret. Chapter 8 therefore looks at the problem of key management, which is concerned with securely generating, distributing, etc., keys, as well as the specific aspects of the security of networks.

Finally, there are two appendices. Appendix A explains Shannon's measure of information and is meant for those who are not yet acquainted with the fundamentals of information theory. Appendix B covers several specific techniques for encrypting imagery.

Notation

A_d	Number of residues with d elements
C	Ciphertext
$C(\tau)$	Autocorrelation
CI	Coincidence index
CI′	Pure estimator of CI
d	Part of the secret key of RSA; number of elements of the residue
δ	Hamming distance
$DK(.)$	Decipherment with a symmetric algorithm using a key K
$dS_X(.)$	Decipherment with an asymmetric algorithm using a secret key S_X
D_L	Redundancy in a text of length L
e	Part of the public key of RSA
E	Expansion operation of DES
$E(.)$	Expectation
$EK(.)$	Encipherment with a symmetric algorithm using a key K
$eP_X(.)$	Encipherment with an asymmetric algorithm using a public key P_X
ε	Number of elements of an alphabet
ϕ	Euler totient function
$f(.)$	Characteristic polynomial
$f(.,.,.)$	Feedback function of a shift register
$F(.,.)$	Cipher function DES
$G(.)$	Generating function
χ	Chi-test
$h(.)$	Hash-code
H	Hypothesis
$H(.)$	Marginal information measure
$H(K/C)$	Key equivocation
$H(M/C)$	Message equivocation
$H(K/M,C)$	Key appearance equivocation
I	Identification sequence
IP	Initial permutation

IV	Initial vector
J	Jacobi symbol
K	Secret key of a symmetric algorithm
kDES	First k bits of the result of an encipherment using DES
K_i	Subkey of DES
K_{ij}	Key for Diffie–Hellmann protocol
KS	Session key
l	Length of a run
L	Length of a message
LC	Linear complexity profile
m	Number of sections of a shift register
$mgK(.)$	Result of a MAC using key K
M	Plaintext, original message
MK	Master key
mod	Modulo addition
N	Length of (pseudo)random sequence
$oK(.)$	Result of a one-way function using key K
p	Period of a shift register sequence; prime number
P_X	Pubic key of X for an asymmetric algorithm
Pe	Error probability
PeD	Error probability distance
q	Prime number
r	Total number of runs in a binary sequence
R	Random sequence
S	Knapsack sum; security event
S_X	Secret key of X for an asymmetric algorithm
s_i	Element of a shift register sequence; secret number for zero-knowledge techniques
T	Period
T_K	Encipherment transformation
TK	Terminal key
UD	Unicity distance
var	Variance

1

Introduction to cryptology

1.1 Cryptography and cryptanalysis

The title of this book contains the word *cryptography*. Cryptography is an area within the field of *cryptology*. The name cryptology is a combination of the Greek *cruptos* (= hidden) and *logos* (= study, science). Therefore, the word cryptology literally implies the science of concealing. It comprises the development of methods for *encrypting* messages and signals, as well as methods for *decrypting* messages and signals. Thus, cryptology can be divided into two areas: *cryptography* and *cryptanalysis*.

Cryptography can be defined more specifically as the area within cryptology which is concerned with techniques based on a secret key for concealing or enciphering data. Only someone who has access to the key is capable of deciphering the encrypted information. In principle this is impossible for anyone else to do.

Cryptanalysis is the area within cryptology which is concerned with techniques for deciphering encrypted data without prior knowledge of which key has been used. This is more commonly known as 'hacking'.

It is evident that cryptography and cryptanalysis are very closely related. One is only able to design good (sturdy) cryptographic algorithms when sufficient knowledge of the methods and tools of the cryptanalysists is available. The person responsible for the implementation of this type of security measure must therefore obtain this knowledge and be aware of the methods of a potential intruder. Obviously, successful cryptanalysis requires at least a fundamental insight into cryptographic algorithms and methods.

This book will focus mainly on cryptography.

A first impression of what a cryptographic algorithm does is given by considering the following situation, which also offers the opportunity of

introducing some notation. Suppose *A* (the transmitter) wishes to send an enciphered message, i.e. secret code, to *B* (the receiver). Often, the original text or *plaintext* is simply denoted by the letter *M* of message and the encrypted message, referred to as the *ciphertext*, by the letter *C*. A possible method is for *A* to use a secret key *K* for *encrypting* the message *M* to the ciphertext *C*, which can then be transmitted and decrypted by *B*, assuming that B also possesses the secret key *K*. This is illustrated in Figure 1.1. *EK* represents the encryption of the message with the aid of *K*; the *decryption* of the message is represented by *DK*. Hereafter we will use the following notation:

$C = EK(M)$
(i.e. original text *M* is encrypted to ciphertext *C* with the secret key *K*);

$M = DK(C)$
(i.e. ciphertext *C* is decrypted to the original text *M* with the secret key *K*).

An example of what occurs at the transmitter and receiver is given by Figure 1.2. It is up to the reader to find the correct key. This should prove not too great a problem for those who can use a word-processor .

Figure 1.1. Cipher system.

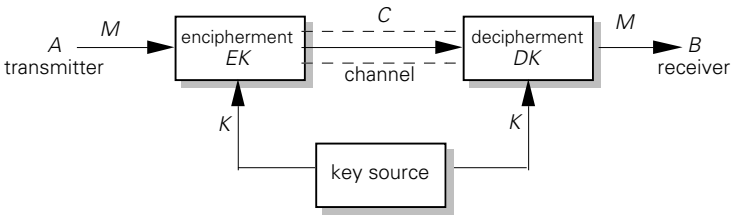
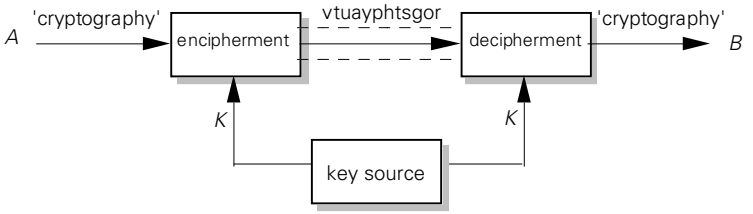


Figure 1.2. Example of encipherment and decipherment.



The Advanced Encryption Standard: Rijndael

K. Cartrysse and J.C.A. van der Lubbe

Supplement to the books

"Basic methods of cryptography"

and

"Basismethoden cryptografie"

October 2004

Contents