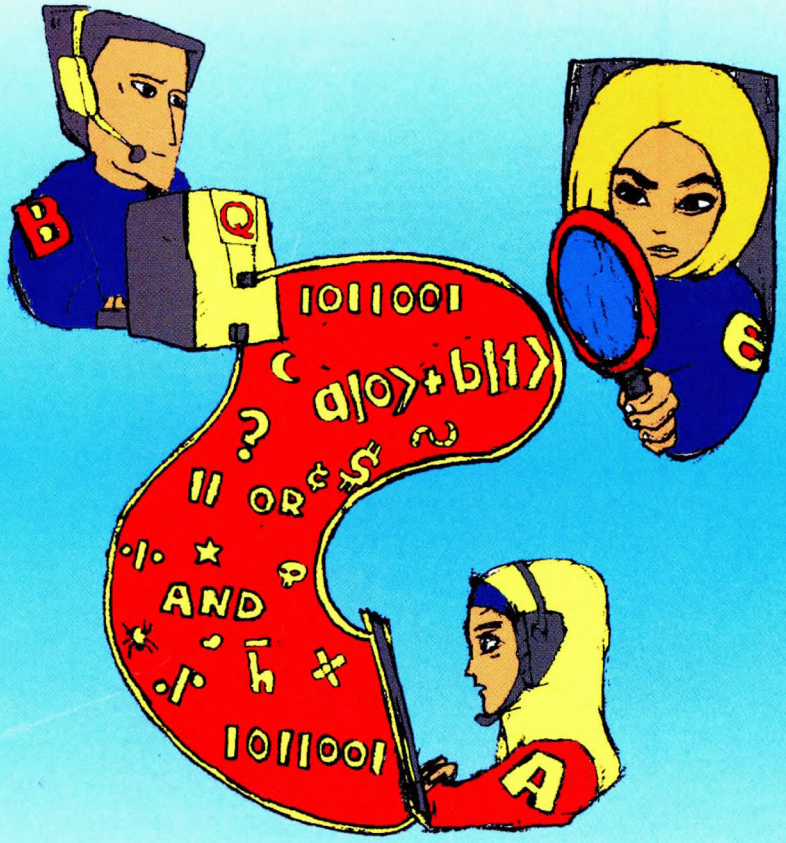
# MATHEMATICAL ASPECTS OF CLASSICAL AND QUANTUM CRYPTOGRAPHY




**Thomas Bier**
**Mohamed Ridza Wahiddin**

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

PERDANA LEADERSHIP FOUNDATION
YAYASAN KEPIMPINAN PERDANA


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

# MATHEMATICAL ASPECTS OF CLASSICAL AND QUANTUM CRYPTOGRAPHY


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

# MATHEMATICAL ASPECTS OF CLASSICAL AND QUANTUM CRYPTOGRAPHY

THOMAS BIER
Visiting Research Associate at Kulliyyah of Science, IIUM
and Associate Professor at Institute of Mathematical Sciences, UM

MOHAMED RIDZA WAHIDDIN
Professor at Kulliyyah of Science, IIUM

Published by:
Research Centre
International Islamic University Malaysia
53100 Kuala Lumpur
Malaysia
Tel: 603-2056-5010 Fax: 603-2056-4862
e-mail: rescentre@iiu.edu.my

First edition, 2004


Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Bier, Thomas
Mathematical aspects of classical and quantum cryptography / Thomas Bier, Mohamed Ridza Wahiddin
Includes index
Bibliography
ISBN 983-2957-19-4
1. Mathematics. 2. Physics. 3. Cryptography. 4. Quantum theory
I. Mohamed Ridza Wahiddin
652.42

ISBN: 983-2957-19-4

# CONTENTS


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

# PREFACE

In this book we give some introduction to the mathematical background for cryptography and for cryptanalysis, both for the classical and for the quantum case. We first give a brief description of the topics treated.

In the first chapter on classical cryptography we first discuss general monoalphabetic and polyalphabetic substitutions, and their relationship to modular arithmetic and to matrices. We give a brief sketch of the data encryption standard DES and the new advanced encryption standard AES. We discuss public-key encryption and its relation to factoring problems of integers.

In the second chapter we discuss various number theoretic questions that have arisen in our analysis of problems that are arising in classical cryptography. These include the question of quadratic residuosity modulo prime and composite integers, the discrete logarithm problem for prime moduli and some of its number theoretic background, and several questions on multipliers in modular arithmetic. The notion of a multiplier arises in calculation modulo large integers, as they are required for example in public key cryptography, but also in the discrete logarithm problem and in other instances. We have tried to give a reasonably broad treatment of this aspect in the second chapter. We only briefly touch on further algorithms, on special primes, and on electronic signatures and authentication.

In the third chapter we give mathematical constructions for binary sequences, in particular for binary shift register sequences. This includes linear sequences, as well as several questions on non linear and in particular quadratic shift register sequences. The non linear constructions are based on Boolean functions. One of the tools is a digraph method first used by D. Shanks.

The fourth chapter gives an introduction to the area of quantum cryptography. We also give an introduction to quantum cryptography and quantum computing. Some physical aspects of quantum optics like squeezed light are also presented.

In the fifth chapter for mathematical background on entanglement we consider certain tensor product construction of matrices relating to the notion of entanglement of particles, e.g. of photons. Some constructions are given that reduce the matrix questions to questions in the construction of tensor products of vectors, in particular to the problem of determining the tensor length for certain non decomposable tensors. We introduce agreement system, and more conceptually relational systems, and prove several results about such systems. We end by showing a non existence theorem for configurational Steiner triple systems.

This brief description of contents already shows that some of the material is non standard, and we believe that some of it may also not have been written down elsewhere. Due to the difficulties and restrictions that we faced during the writing, this implies certain imperfections and omissions. For these and for all remaining errors we take the full responsibility.

We have tried to achieve a blend of the still novel and largely unexplored area of quantum cryptography with some related mathematical material in order to make this text interesting and accessible for students of mathematics, physics, and computer science at advanced undergraduate and at graduate level.

This text is based upon our collaboration dating back to the time when the second named author, who is now a senior professor at the International Islamic University of Malaysia, was a professor at the University of Malaya, where also the first named author holds a temporary position. The present text was written while the first named author was a research associate of the International Islamic University Malaysia from an IRPA grant of the second named author from October 2002 to March 2003.

Kuala Lumpur, May 2004.

TB
UM, KL

MRW
IIUM, KL

# ACKNOWLEDGEMENTS

The authors should like to acknowledge the support from their families, that is of the wife of T. Bier, Dr. Yuriko Suwa-Bier and son Beato Suwa and of the wife of M.Ridza Wahiddin, Latifah Mansoor and of son Sulaiman and daughters Nasuha and Nadwiyah.

They also like to thank Mr. Muhammad Salihi Abdul Hadi, Mr. Pah Chin Hee, Mr. Tan Tu How, Mr. Wong Kok Bin and Mr. Zahari Dollah for their valuable comments on specific items.

This work was partially financed by the International Islamic University Malaysia and by the IRPA Grant No 09-02-08-0203-EA002 of M.Ridza Wahiddin. T. Bier acknowledges support for visiting IIUM as an invited professor and a research associate which made the writing of this text possible. He also thanks Prof. Kamel Ariffin M. Atan for an invitation to INSPEM (UPM) in Serdang in April 2003, where a part of the second chapter was written.


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

CHAPTER

# 1

# Classical Cryptography

## 1.1 Monografic Substitution

Monografic substitution refers to all substitutions subject to the rule “one letter by one letter”.

### 1.1.1 Standard and Monoalphabetic Substitutions

We assume that we are given a set of letters, called the (plaintext) alphabet, usually taken to be a set like

$$P=\{A,B,C,\ldots,X,Y,Z\} \text{ OR } P=\{A,B,C,\ldots,Y,Z,,0,1,2,\ldots,9\}, \tag{1.1}$$

which in this case consists of either 26 or 36 letters. Another common form has 25 letters, with $i = j$.

We then assume that we are also given a set of ciphers, which can consist of the same or of a different set of symbols. In the simplest case of 26 letters the set of cyphers may be chosen also to be

$$\boldsymbol{C = \{A,B,C,\ldots,X,Y,Z\}.} \tag{1.2}$$

An *encryption* is a bijective mapping from the set consisting of the normal alphabet to the set of cyphers. If the set of cyphers and the normal alphabet are identical, then we consider the encryption as a permutation of this common set. The *decryption* is the process of finding the inverse of that bijection. A *deciphering* is the problem of guessing the bijection from some knowledge of (a piece or the total of) the string of ciphers.

Examples: The cyclic encryption:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | E | F | G | H | I | J | K | L | M | N | O | P |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

The password encryption: International Islamic University, use each letter only once, then fill in the rest in alphabetic order.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | N | T | E | R | A | O | L | S | M | C | U | V |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Y | B | D | F | G | H | J | K | p | Q | W | X | Z |

This device is associated with the 18-th century French cryptographer F. Vigenere, see also appendix A.

A more sophisticated way of encryption, which is able to performed by machine, and has the advantage that encryption and decryption is a symmetrical process, can be obtained by first identifying the alphabet with numbers:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

and then considering these numbers as element in the (modular) cyclic group $Z/26 = \{0,1,2,\ldots, 25\}$. We may then use for the encryption process (in the simplest case) a linear function

$$f(x) = a.x + b \tag{1.3}$$

where we perform modular arithmetic modulo 26, or modulo the size of any other suitable alphabet. Clearly the first example given above is the case $a = 1, 6 = 3$.

This gives rise to the first mathematical problem: For which values of $a$, $b$ G $Z/26$ is the function $f$ in (1.3) actually bijective. This can be answered very simply, in terms of a notion in algebra: Recall that a ring $R$ is any system with addition and multiplication, where the operation of addition forms a group, and multiplication is distributive over addition. In particular $Z/26$,

as well as any $Z/n$ is a ring, with usual modular arithmetic. It contains an element 1 which satisfies $1 \bullet x = x$ for all $x$ E $R$. We say that $a$ £ $R$ is a *unit* iff there exists an element $c$ e $R$ with $a \bullet c = 1$.
Example: The units in the ring $Z$/26 are precisely the 12 numbers

$$U(Z/26) = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \quad (1.4)$$

For the following lemma we want to assume that the given alphabet consists of $n$ letters which are identified with the numbers $0, 1, \ldots, n - 1$ in the group $Z/n$.

We also recall that the number 0(n) called Eulers Phi function is defined to be

$$o)(n) = \backslash\{x \in Z : 1 < x < n, gcd(x,n) = 1\}|. \quad (1.5)$$

It can be worked out by using a formula that uses the prime power factorization of $n$ as $n = p\backslash^1 \bullet p_2^2 \ldots\ldots\ldots\ldots r\%-$ :

$$(j)\{n) = (_{Pl} - 1)Pi^{1}{}_{-1} \quad (P_2 - 1)P2^{>\sim 1} \ldots\ldots\ldots\ldots (Pr - 1)Pr^{r\sim 1'} \quad C^{1}\text{-}^{6})$$

In particular, if $n = p$ is a prime number, then $o(p) = p - 1$, and if $n = p^e$ is a prime power, then $o\{p^e) = (p - 1)p^{e-1}$.

Lemma 1 The function (1.3) is bijective iff a is a unit (as in (1.4) ) in the ring $Z/n$. The number of units of the ring $Z/n$ is given by 0(n), i.e. Eulers Phi function. Hence there are $o(n) \cdot n$ distinct bijective functions of the form (1.3).

The proof of this lemma is standard elementary number theory. See [17], [18] or [11].
In particular there are $12 \bullet 26 = 312$ ways of forming a linear bijection / for the standard alphabet.

Exercise: Find the number of ways of forming a linear bijection (1.3) for an alphabet of size 36.

We first work out the example $a = 3$, $b = 5$ to find the corresponding encryption and decryption.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | **1** | **2** | 3 | 4 | 5 | **6** | 7 | **8** | 9 | **10** | **11** | **12** |
| 5 | **8** | **11** | 14 | 17 | **20** | 23 | 0 | 3 | **6** | 9 | **12** | 15 |
| F | I | L | **0** | R | U | X | A | D | G | J | M | P |

# MATHEMATICAL ASPECTS OF CLASSICAL AND QUANTUM CRYPTOGRAPHY

This book treats problems on the mathematical and physical background of a topic of much current interest: cryptography, as well as cryptoanalysis. While numerous textbooks have been written on the subject itself, this text is mainly concerned with the mathematical and the quantum mechanical aspects of the interesting and quickly growing area of cryptography.

The first chapter gives a general introduction to the ideas of cryptography. The other chapters are on number theoretic aspects of cryptography, on shift register sequences, on quantum information and quantum computing and a mathematical treatment on the quantum optics idea of entanglement.

The blend of the still novel and largely unexplored area of quantum cryptography with the related mathematical material makes this text interesting and accessible for students of mathematics, physics and computer science at advanced undergraduate and at graduate level.

This text is based upon our collaboration dating back to the time when the second named author, who is now a senior professor at the International Islamic University Malaysia was a professor at the University Malaya, where also the first named author holds a temporary position. The present text was written while the first named author was a research associate of the International Islamic University Malaysia from an IRPA grant of the second named author from October 2002 to March 2003.

ISBN 983-2957-19-4
9 789832 957195

**Research Centre**
**International Islamic University Malaysia**
Jalan Gombak, 53100 Kuala Lumpur
Tel: 603 - 2056 5010
Fax: 603 - 2056 4862
E-mail: rescentre@iiu.edu.my

PERDANA LEADERSHIP FOUNDATION
YAYASAN KEPIMPINAN PERDANA