CRYPTANALYSIS OF PUBLIC-KEY CRYPTOSYSTEMS

Presented By
Dieaa Ibrahim Nassr Abdelhai

Supervised By
Assoc. Prof. Sameh S. Daoud
Assoc. Prof. Hatem M. Bahig
Dr. Ashraf M. Bhery

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS
FOR THE **Ph.D.** DEGREE
(COMPUTER SCIENCE)
SUBMITTED TO
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT

AIN SHAMS UNIVERSITY

Author:	**Dieaa Ibrahim Nassr Abdelhai**
Title:	**Cryptanalysis of Public-Key Cryptosystems**
Division:	**Computer Science**
Department:	**Department of Mathematics**
Faculty:	**Faculty of Science**

Degree: **Ph.D.** Year: **2016**

Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

We use the following standard notations with a short explanation.

Notation	**Explanation**
$\mathbb{R}$	The set of real numbers.
Z	The set of integers.
Z^n	$\{(a_1, a_2, \ldots, a_n) : a_1, a_2, \ldots, a_n \in Z\}$.
$\gcd(x, y)$	The greatest common divisor of the two integers x and y.
Z_m	$Z_m = \{0, 1, \ldots, m-1\}$.
Z_m^*	$Z_m^* = \{x \in Z_m : \gcd(x, m) = 1\}$.
$a \mid b$	b is divisible by a.
$a \nmid b$	b is not divisible by a.
$x \equiv y \pmod{m}$	$m \mid (x - y)$.
$\phi(n)$	The Euler's phi function.
$dim(L)$	The dimension of lattice L.
$det(L)$	The determinant of lattice L.
$\|g(x)\|$	$\sqrt{\sum_i a_i^2}$ the norm of $g(x)$, where $g(x) = \sum_i a_i x^i$.
$\|(v_0, v_1, \ldots, v_{k-1})\|_\infty$	$\max\{\|v_0\|, \|v_1\|, \ldots, \|v_{k-1}\|\}$.
$\pi(n)$	The number of primes less than or equal to n.
$f * g$	the multiplication of two polynomials f and g.
$\|x\|$	The absolute value of x.
$\|A\|$	The cardinality of set A.
$\lfloor a/b \rfloor$	The round of a/b to the nearest integer less than or equal to a/b.
$\lceil a/b \rceil$	The round of a/b to the nearest integer greater than or equal to a/b.
$\lfloor a/b \rceil$	The round of a/b to the nearest integer to a/b.