UNIVERSITI PUTRA MALAYSIA

CRYPTANALYSIS OF RSA AND ITS VARIANTS USING CONTINUOUS MIDPOINT SUBDIVISION ANALYSIS AND LATTICES

WAN NUR AQLILI BINTI WAN MOHD RUZAI

IPM 2021 1

CRYPTANALYSIS OF RSA AND ITS VARIANTS USING CONTINUOUS MIDPOINT SUBDIVISION ANALYSIS AND LATTICES

By

WAN NUR AQLILI BINTI WAN MOHD RUZAI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

May 2021

DEDICATIONS

To the Stars of my Universe:

Mak & Abah
Aqilah, Atikah, Alya
Family, Teachers, Friends
...

من جد وجد

‘Whoever strives shall succeed’

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

CRYPTANALYSIS OF RSA AND ITS VARIANTS USING CONTINUOUS MIDPOINT SUBDIVISION ANALYSIS AND LATTICES

By

WAN NUR AQLILI BINTI WAN MOHD RUZAI

May 2021

Chairman : Prof. Muhammad Rezal Kamel Ariffin, PhD
Institute : Mathematical Research

The RSA cryptosystem developed in 1978 is the earliest public-key cryptosystem most widely deployed in securing digital information. One of the security features of RSA is based on the assumption that factoring its modulus $N = pq$ is an infeasible task to be done in polynomial time. However, most successful cryptanalysis (or often called ‘attack’) against RSA and its variants are not based on this integer factorization problem. Instead, these attacks manipulate the additional information from the RSA parameters being used. Practically for decades, the RSA cryptosystem has been generalized in various ways to improve its efficiency in terms of encryption and decryption time and its security.

This study concentrates on algebraic cryptanalysis via the application of classical methods such as the Diophantine approximation and lattice basis reduction. Accordingly, five new cryptanalysis methods are developed to show that the modulus $N = pq$ of RSA and some of its variants can be factored in polynomial time under certain specified conditions. It is expected from this study to outline several new conditions required to design a secure RSA and its variant cryptosystems.

The main contribution of this thesis is a strategy called the ‘continuous midpoint subdivision analysis’ (CMSA) is developed to find the vulnerabilities of RSA and some of its variants. In the first attack, CMSA is applied upon an interval containing the Euler’s totient function, and together with continued fractions on the RSA key relation, the upper cryptanalytic bound of private exponent d is raised exponentially. As in the second attack, a similar strategy is conducted upon an interval containing the modified Euler quotient along with continued fractions on the modified key relation of some variants of RSA cryptosystems. Note that, in the third attack, our strategy is considered for the case when the prime factors p and q are of arbitrary bit-size (i.e. the primes are said to be unbalanced primes). A new weak RSA key equation structure that solves the factoring problem under certain specified conditions in polynomial time is proposed in the fourth attack. This attack combines the continued fractions and Coppersmith's theory on finding the small solutions of modular univariate polynomial equations. Whilst in the last attack, the k instances of RSA moduli with a special-structured of the key equations can be factored simultaneously in polynomial time using the lattice basis reduction technique. Note that our cryptanalytic works extend the bound of insecure RSA decryption exponents of some previous literature.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KRIPANALISIS TERHADAP SISTEMKRIPTO RSA DAN VARIANNYA MELALUI KAEDAH ANALISIS BERTERUSAN TERHADAP SUB-BAHAGIAN TITIK TENGAH DAN KEKISI

Oleh

WAN NUR AQLILI BINTI WAN MOHD RUZAI

Mei 2021

Pengerusi: Prof. Muhammad Rezal Kamel Ariffin, PhD
Institut: Penyelidikan Matematik

Sistemkripto RSA yang telah dibangunkan pada tahun 1978 adalah merupakan sistemkripto kunci awam terawal dan digunakan dengan meluas untuk memastikan keselamatan maklumat digital pengguna. Salah satu daripada ciri keselamatan sistemkripto RSA adalah ia bergantung kepada masalah pemfaktoran integer; iaitu berdasarkan anggapan bahawa memfaktorkan modulus $N = pq$ adalah tugas yang amat sulit untuk diselesaikan dalam masa polinomial. Walau bagaimanapun, kebanyakan kripanalisis atau ‘serangan’ yang dijalankan terhadap RSA dan variannya bukan bertumpu kepada masalah pemfaktoran integer tetapi memfokuskan untuk memanipulasi struktur matematik atau aliran kerja pelaksanaan skim tersebut. Secara praktikalnya selama berdekad-dekad, sistemkripto RSA telah ditambahbaik dengan matlamat untuk meningkatkan keupayaannya dari segi kecekapan dan keselamatan.

Kajian tesis ini tertumpu kepada serangan yang dibangunkan melalui aplikasi kaedah klasik seperti hampiran Diophantus dan kekisi asas terturun. Sebagai hasilnya, tesis ini telah berjaya menghasilkan lima serangan baharu yang menunjukkan bahawa modulus $N = pq$ boleh difaktorkan dalam masa polinomial tertakluk kepada syarat tertentu. Adalah dijangkakan dapatan hasil kajian ini dapat dijadikan garis panduan untuk membina sistemkripto RSA dan variannya yang selamat.

Sumbangan utama tesis ini adalah membangunkan strategi baharu yang disebut sebagai ‘analisis berterusan terhadap sub-bahagian titik tengah’ (CMSA). Dalam serangan pertama, kaedah CMSA telah diaplikasikan terhadap selang yang mengandungi fungsi fi Euler bersama dengan kaedah pecahan lanjar yang mendorong kepada penemuan parameter rahsia sistemkripto RSA. Dalam serangan kedua dan ketiga, kaedah CMSA digunakan ke atas selang yang mengandungi fungsi Euler terubahsuai disertakan dengan kaedah pecahan lanjar yang telah mendorong parameter rahsia bagi sistemkripto varian RSA ditemui. Kami mengkhususkan serangan kedua untuk kasus apabila nombor perdana p dan q mempunyai saiz bit yang sama manakala serangan ketiga untuk kasus apabila nombor perdana tersebut mempunyai saiz bit yang tidak seimbang. Selanjutnya, serangan keempat telah membuktikan kelemahan baharu dalam parameter awam sistemkripto RSA yang boleh membawa kepada pemfaktoran N. Akhir sekali, kami membangunkan serangan terhadap sistem persamaan kunci RSA yang diubahsuai. Kami ingin menekankan bahawa kesemua serangan yang dibangunkan berjaya mengatasi batas atas bagi eksponen rahsia yang selamat berbanding dengan sesetengah kajian yang telah dijalankan.

ACKNOWLEDGEMENTS

Alhamdulillah.

All the praises and thanks are to Allah, the Lord of *'Alamin*, on whom we ultimately depend for sustenance and guidance. Thank you Allah for giving me the strength to do this research and the determination to complete this thesis against all the odds.

I enormously thank my supervisor, Prof. Dr. Muhammad Rezal Kamel Ariffin who has patiently given me guidance, assistance, and motivation on doing this research from the beginning until its completion. I acquired a lot of knowledge and learned many new things from him along my doctorate journey. Thank you kindly to my co-supervisors, Dr. Muhammad Asyraf Asbullah and Dr. Mohamat Aidil Mohamat Johari for their continuous interests and feedbacks on my works. I am thankful to meet many great figures in the cryptographic community during this journey, especially Prof. Abderrahmane Nitaj who has greatly influenced this research work.

My special thanks are to my *Al-Kindian* mates – Hanisah Adenan, Dr. Normahirah, Tea Boon Chian, Dr. Saidu Isah, Zahari Mahad, Rasyid Redha, Siti Nabilah, Dr. Amir Hamzah, and Wan Zariman for their opinions and helps in lots of academic discussions that make my studies much more manageable. And also to all my girlfriends for always share the positive energy in doing the research at INSPEM, UPM. I am lucky to have them around to go through this journey together, as it is vital to know that there is another person going through the same struggles as you, who understands your concerns, and is always there to support each other. Thanks for being in my corner.

My appreciation goes to Universiti Putra Malaysia for supporting me financially under Graduate Research Fellowship (GRF) scheme. And also to INSPEM's staff that are dedicated to assisting me in administrative processes pertaining to my studies. I really appreciate them.

I am forever grateful to my family, *Mak*, Rokhiyah Shamsudin, *Abah*, Wan Mohd Ruzai Yusof, and my *soulsisters*, Aqilah, Atikah, and Alya for always be there through my ups and downs. Thank you for showering me with your eternal love unconditionally. *Kakak* loves all of you *Lillahi Taala*.

Eternally grateful.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Muhammad Rezal bin Kamel Ariffin, PhD
Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairman)

Muhammad Asyraf bin Asbullah, PhD
Senior Lecturer
Centre of Foundation Studies for Agriculture Science
Universiti Putra Malaysia
(Member)

Mohamat Aidil bin Mohamat Johari, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 14 October 2021

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature:________________________ Date:________________________

Name and Matric No: Wan Nur Aqlili binti Wan Mohd Ruzai, GS48533

Declaration by members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ______________________________
Name of
Chairman of
Supervisory
Committee: Muhammad Rezal bin Kamel Ariffin

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Muhammad Asyraf bin Asbullah

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Mohamat Aidil bin Mohamat Johari

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

CF	Continued Fractions
CMSA	Continuous Midpoint Subdivision Analysis
DHKE	Diffie-Hellman Key Exchange
EC	Elliptic Curve
GNFS	General Number Field Sieve
IFP	Integer Factorization Problem
LLL	Lenstra-Lenstra-Lovász
PKC	Public-Key Cryptography
QS	Quadratic Sieve
RSA	Rivest Shamir Adleman
SVP	Shortest Vector Problem
$\mathbb{R}$	The set of real numbers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{Z}$	The set of integers
$\mathbb{Z}^+$	The set of positive integers
$\mathbb{Z}_k$	The set of positive integers less than k
$\mathbb{Z}_k^*$	The set of positive integers less than k and co-prime to k

CHAPTER 1

INTRODUCTION

1.1 Cryptography Around Us

The past decade has seen a rapid proliferation in the field of communication via digital platforms. Since the mid-1990s, the Internet has greatly influenced culture, commerce, and technology, including the rise of near-instant communication by email, instant messaging, two-way interactive video calls, telephony (Voice over Internet Protocol or VoIP), and the World Wide Web (WWW) with its social networking services, discussion forums, blogs, and online shopping sites. Thus, the execution of information transfer over multiple channels in our daily life has demanded an efficient exchange of secure information. This prime need for information security has led to the emergence of a variety of cryptographic algorithms to implement security in different dimensions and for various purposes.

As technology progressed and commercial opportunities arose through the digital platform, the field of cryptology turns into a valuable means when security begins to matters. The terminology cryptology refers to the study of cryptography and cryptanalysis. Literally, cryptography is the science, practice, and study of techniques for secure communication in the presence of third parties (usually called adversaries). In other words, cryptography is the conversion of information from a readable state to total gibberish. Cryptography can be directly used to achieve these information security objectives such as data confidentiality, integrity, authentication, and non-repudiation. Confidentiality ensures the content of data is accessible only to those authorized to have it. Integrity prevents unauthorized modification or alteration of data. Authentication ensures the entities in the communication to identify each other. At the same time, non-repudiation precludes an entity from denying previous commitments or actions. Hence, the ultimate objective of cryptography is to address these four areas in both theories and practice adequately.

Cryptanalysis has co-evolved together with cryptography, and the evidence can be traced through history. The notable work of Al-Kindi (801-873 AD) entitled *Manuscript on Deciphering Cryptographic Messages* has given rise to the birth of cryptanalysis through the invention of the frequency analysis technique. Consequently, new ciphers are being designed to replace old broken designs, and new cryptanalytic techniques are invented to crack the improved schemes.

In practice, cryptography and cryptanalysis can be viewed as two sides of the same coin – secure cryptography requires design against possible cryptanalysis. A well-known cryptographer Adi Shamir once said, “cryptography is a never-ending struggle between code makers and code breakers.”

Before proceeding to the next section, let us acknowledge some motivation words from the winner of *ACM Turing Award 2015*, Martin Hellman once said:

> "...The way to get to the top of the heap in terms of developing original research is to be a fool, because only fools keep trying. You have an idea number 1, you get excited, it flops, you get idea number 2, it also flops, then you get idea number 99, it also flops. Only a fool would be excited with the 100th idea, but it might take 100 ideas before one really pays off. Unless you are foolish enough to be continually excited, you won't have the motivation, you won't have the energy to carry through. God rewards fools..."

1.2 Public Key Cryptography

In the mid-1970s, all cipher systems adopted symmetric key algorithms in which the same cryptographic key is used during encryption and decryption processes. The key must be kept secret at all costs from unauthorized parties. Inevitably, the key must be exchanged between the communicating parties in advance before using the system via some secure channel. However, the implementation of symmetric cryptography causes a chaotic situation, especially in a large network system, as every communication needs a unique designated key. This situation is referred to as the key distribution problem. Moreover, the term symmetric cryptography is often called private-key cryptography.

It was not until 1976 that the notion of asymmetric cryptography emerged in the public sphere within the seminal work of Whitfield Diffie and Martin Hellman. Since then, it has shed light on how to solve the key distribution problem. The idea is to use distinct keys that are mathematically related in the encryption and decryption processes between two communicating parties. The scenario can be described as although everyone in the world knows the public key to encrypt messages, but only the legitimate recipient is able to decrypt messages. The term asymmetric cryptography is also sometimes referred to as public-key cryptography.

The formal definition of public-key cryptography (PKC) as mentioned in Hinek (2009) is recalled as follows.

Definition 1.1 *A public-key cryptosystem is a system that consists of five-tuple* $(\mathscr{K},\mathscr{P},\mathscr{C},\mathscr{E},\mathscr{D})$ *which meets the following conditions:*

1. $\mathscr{K}$ *is called a keyspace which consists of finite set of possible keys.*

2. $\mathscr{P}$ *is finite set of possible plaintexts.*

3. *$\mathscr{C}$ is a finite set of possible ciphertexts.*

4. *For each $K \in \mathscr{K}$, there exists an encryption rule $enc_K \in \mathscr{E}$ and its corresponding decryption rule $dec_K \in \mathscr{D}$. Each $enc_K : \mathscr{P} \to \mathscr{C}$ and $dec_K : \mathscr{C} \to \mathscr{P}$ are functions such that $dec_K(enc_K(M)) = M$ for each plaintext $M \in \mathscr{P}$.*

5. *Both $enc_K(M)$ and $dec_K(enc_K(M))$ are easy to calculate for every key $K \in \mathscr{K}$ and every plaintext $M \in \mathscr{P}$.*

6. *Each easily computable algorithm equivalent to dec_K is computationally infeasible to derive from enc_K for almost each key $K \in \mathscr{K}$. Simply said, it is hard to decrypt without dec_K.*

7. *The decryption rule dec_K is privately kept whilst the encryption rule enc_K is publicly known.*

One of the important features of PKC is to use a trapdoor one-way function which ensures the conditions 4–7 of Definition 1.1 are satisfied. This trapdoor function is auxiliary information that enables the inverse function to be easily computed. In the case of PKC, the decryption rule dec_K is said to be a trapdoor information in the set $\mathscr{D}$. Such function can be formally defined and illustrated as follows.

Definition 1.2 *(Trapdoor One-Way Function)(Menezes et al., 1996) An invertible function $f : A \to B$ is a one-way function if for $a \in A$ and $b \in B$, it is easy to compute $b = f(a)$ but it is hard to compute $a = f^{-1}(b)$. Whilst f is called a trapdoor one-way function if given some information on $f^{-1}(b)$, it is easy to compute $a = f^{-1}(b)$.*

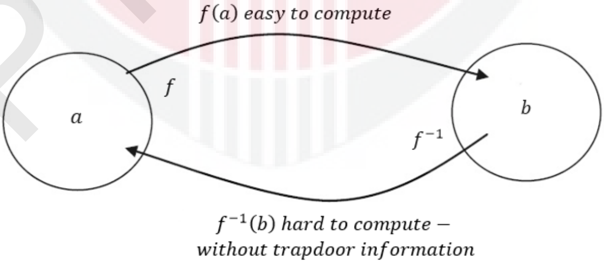

Figure 1.1: Illustration of a trapdoor one-way function

Note that, the phrase 'easy' or 'hard' to compute depends on the context of time complexity of an algorithm to solve a certain mathematical cryptographic hard problem. Hence, the standard concepts of computational complexity of mathematical problems are defined as follows.

Definition 1.3 *(Computationally Secure)(Menezes et al., 1996) An algorithm is considered computationally secure if it cannot be broken with available resources, either current or future.*

Definition 1.4 *(Time Complexity)(Sipser, 2012) Time complexity of an algorithm is a measuring tool to quantify the amount of time needed to execute the algorithm and is commonly expressed using big-$\mathcal{O}$ notation.*

Definition 1.5 *(Big-$\mathcal{O}$ Notation)(Sipser, 2012) Let $m(x)$ and $n(x)$ be defined on $X \subset \mathbb{R}$. One writes $m(x) = \mathcal{O}(n(x))$ as $x \to \infty$ if and only if there exists $x_0 \in \mathbb{R}$ and $B \in \mathbb{R}^+$ such that for all $x \geq x_0$,*

$$\left| \frac{m(x)}{n(x)} \right| \leq B.$$

As a note, big-$\mathcal{O}$ notation can be analogously described in L-notation, defined as

$$L_n[\alpha, c] = e^{\big(c+o(1)\big)(\ln n)^{\alpha}(\ln\ln n)^{1-\alpha}}$$

where α is a constant $0 \leq \alpha \leq 1$ and c is a positive constant. L-notation is mostly used to express the complexity of number theoretic problems such as the integer factorization and discrete logarithms problems.

Based on Definition 1.5, we can describe particular type of time complexities of an algorithm given n as the size of the input of an algorithm.

Definition 1.6 *(Sedgewick and Wayne, 2011) The number of digits (bits) in the binary representation of a positive integer n is the integral part of $\log_2 n + 1$ (i.e. $\lfloor \log_2 n \rfloor + 1$).*

Definition 1.7 *(Polynomial Time)(Papadimitriou, 2003) An algorithm is said to be solvable in polynomial time if the time required to complete the algorithm is $\mathcal{O}(n^k)$ where $k > 0$ and n is the size of the input.*

Definition 1.8 *(Sub-exponential Time)(Papadimitriou, 2003) An algorithm is said to be solvable in sub-exponential time if the time required to complete the algorithm is $\mathcal{O}(2^{n^{\varepsilon}})$ where $0 < \varepsilon < 1$ and n is the size of the input.*

Definition 1.9 *(Exponential Time)(Papadimitriou, 2003) An algorithm is said to be solvable in sub-exponential time if the time required to complete the algorithm is $\mathcal{O}(2^{n^k})$ where $k > 0$ and n is the size of the input.*

From the above definitions, it means that an algorithm with polynomial time complexity is considered ‘fast’ and an algorithm with exponential time complexity is considered ‘slow’. Similarly, an algorithm with sub-exponential time is ‘slow’ but better than exponential time. Therefore, if a problem cannot be solved in polynomial time, then it is a ‘hard’ problem. Practically, a ‘hard’ problem should take the best computers available billions of years to solve; whilst an ‘easy’ problem is one that can be solved very quickly.

1.3 Cryptanalysis of Public Key Cryptography

The terminology cryptanalysis is used to describe the study of mathematical techniques for attempting to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. That is, cryptanalysis is simply referred to as an attack.

The term cryptanalyst refers to someone who engages in cryptanalysis. The ultimate goal of the cryptanalyst is to gain as much information as possible about the original plaintext (unencrypted data) if they are given some ciphertext (encrypted data).

Although the security strength of a cryptosystem can be directly reduced by an attack, it may become a guiding principle for cryptographic practitioners to implement better cryptosystems in the future. Knudsen (1998) has classified various implications of an attack according to the amount and quality of private information that was revealed as follows.

- **Total break.** The scenario when the adversary retrieves the private key used in any cryptosystem i.e. $D_k(C) = P$.
- **Global deduction.** The scenario when the adversary finds an alternative algorithm which is equivalent to $D_k(C) = P$ without knowing k.
- **Local deduction.** The scenario when the adversary discovers the plaintext of an intercepted ciphertext.
- **Information deduction.** The scenario when the adversary discovers some information about the key or plaintext. The information could be a few bits of the key, some information about the form of the plaintext, and so forth.

In this thesis, we show the implication of information deduction attack which leads to a total break attack upon RSA and its variant cryptosystems within polynomial time.

Essentially, the security of a cryptosystem is quantified in terms of “bits of security”. One can think of this as a function of the number of steps needed to break a system by the most efficient attack. For example, a system with 112 bits of security would take 2^{112} steps to break, which would take the best computers available today billions of years. Therefore, according to Barker (2016), algorithms approved by the National Institute of Standards and Technology (NIST) should provide at least 112 bits of security.

1.4 Mathematical Preliminaries

This section provides the mathematical components requisite for a better understanding of the subject, which also aided us to construct the attacks presented in this thesis.

We begin with some notations that are frequently used in our work. We use $\mathbb{R}, \mathbb{Q}$ and $\mathbb{Z}$ to denote the set of real numbers, rational numbers and integers, respectively. Precisely, we use $\mathbb{Z}^+$ to denote the set of positive integers; $\mathbb{Z}_k$ to denote the set of positive integers less than k; and $\mathbb{Z}_k^*$ to denote the set of positive integers less than k and co-prime to k.

Definition 1.10 *(Divisibility)(Hoffstein et al., 2008) Let $a, b \in \mathbb{Z}$ and $b \neq 0$. If there exists $k \in \mathbb{Z}$ such that $a = bk$, then b divides a. This is denoted by $b|a$.*

Definition 1.11 *(Division Algorithm)(Hoffstein et al., 2008) Let $a, b \in \mathbb{Z}^+$. Then, a divided by b has unique integers called a quotient q and a remainder r such that $a = b \cdot q + r$ with $0 \leq r < b$.*

Definition 1.12 *(Greatest Common Divisor)(Hoffstein et al., 2008) A positive integer d is called the greatest common divisor (gcd) of two integers a and b where d is the largest integer dividing a and b. This is denoted by $gcd(a, b) = d$.*

Definition 1.13 *(Prime and Composite)(Hoffstein et al., 2008) An integer $p \geq 2$ is simply called a prime number if it is divisible only by 1 and p itself. If an integer $N > 1$ and not a prime, then it is called a composite number. An integer 1 is neither prime nor composite. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, \cdots$.*

Definition 1.14 *(Co-prime integers)(Hoffstein et al., 2008) Two integers a and b are said to be relatively prime or simply called co-prime integers if $gcd(a, b) = 1$.*

Definition 1.15 *(Congruence Relation)(Hoffstein et al., 2008) Let $a, b, N \in \mathbb{Z}$ and $N \neq 0$. We say $a \equiv b \ (mod\ N)$ if $\frac{a-b}{N} = k \in \mathbb{Z}$.*

Theorem 1.1 *(Fundamental Theorem of Arithmetic)(Riesel, 2012) For every integer $N > 1$, then N can be represented as*

$$N = \prod_{j=1}^{k} p_j^{\alpha_j}$$

where p_j are k distinct prime factors of N for each order $\alpha_j \geq 1$ such that $p_j^{\alpha_j}$ is unique regardless of its ordering.

Example 1.1 $2 = 2^1,\ 3 = 3^1,\ 4 = 2^2,\ 5 = 5^1,\ 6 = 2^1 3^1, \cdots,\ 12 = 2^2 3^1, \cdots,$ $504 = 2^3 3^2 7, \cdots, 1125 = 3^2 5^3, \cdots, 170217 = 3^2 18913, \cdots.$

From the above example, it is obvious that prime number made up every known integer in this universe.

1.5 Integer Factorization Problem

In this section, we define one of the oldest known hard problem that is adopted as a trapdoor one-way function in the RSA cryptosystem. This problem is derived from the classical Fundamental Theorem of Arithmetic; and is known as the integer factorization problem (IFP).

Definition 1.16 *(Integer Factorization Problem)(Menezes et al., 1996) Given that N is a positive integer. The IFP is a problem to identify the distinct primes p_k for $k = 1, 2, \cdots, \ell$ such that*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell},$$

and each $\alpha_k \geq 1$ for $k = 1, 2, \cdots, \ell$.

Consecutively, we redefine Definition 1.16 to suit the integer factorization problem for two large primes that can be specified as follows.

Definition 1.17 *(Yan, 2009) Given $N = pq$ where p and q are two distinct strong primes. The IFP is to find the unknown p and q.*

Definition 1.18 *(Euler's Totient Function)(Menezes et al., 1996) Given an integer $N > 1$, then the Euler's totient function of N counts the number of integer less than N that is co-prime to N and is denoted by the notation $\phi(N)$.*

Particularly, we will used the following theorem to compute $\phi(N)$.

Theorem 1.2 *(Menezes et al., 1996) Suppose* $N = \prod_{i=1}^{k} p_i^{a_i}$ *fulfills Theorem 1.1. Then*

$$\phi(N) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1).$$

Proposition 1.1 *(Menezes et al., 1996) If q is a prime number, then*

$$\phi(q) = q - 1.$$

1.5.1 Existing Factoring Algorithms

Practically, how hard is it to solve IFP? The question seems simple but for decades, mathematicians and cryptographers are still trying to find the best efficient algorithm to solve the IFP in polynomial time.

In this section, we list out some existing factoring algorithms that can solve the IFP. These algorithms can be categorized into (Menezes et al., 1996):

1. **General purpose factoring algorithm**
   - Targets any composite number without specific structures.
   - The running time depends solely on the size of composite number N.
   - Example of algorithms: Quadratic sieve, General number field sieve, and Continued fractions factorization.
2. **Special purpose factoring algorithm**
   - Targets some composite numbers with specific structures.
   - The running time depends on certain properties of the factors (i.e. smallest prime factor) of composite number N.
   - Example of algorithms: Trial division, Pollard's ρ algorithm, Pollard's $p-1$ algorithm, Elliptic curve algorithm, and Special number field sieve.

We summarize the time complexity of some known factoring algorithms in the next table. Note that, the parameters which determine the complexity time varies among algorithms.

Table 1.1: Time complexity of algorithms for solving IFP

Factoring Algorithm	**Time Complexity**	**Running Time**
General Number Field Sieve	$\mathcal{O}\left(e^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}}\right)$	Sub-exponential
Quadratic Sieve	$\mathcal{O}\left(e^{\left(1+o(1)\right)(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}}\right)$	Sub-exponential
Elliptic Curve	$\mathcal{O}\left(e^{\left(1+o(1)\right)(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}}\right)$	Sub-exponential
Continued Fractions	$\mathcal{O}\left(e^{\left(\sqrt{2}+o(1)\right)(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}}\right)$	Sub-exponential
Pollard's $p-1$	$\mathcal{O}\left(B \times \log B \times \log^2 n\right)$	Logarithmic
Trial Division	$\mathcal{O}(n^2\sqrt{N})$	Exponential

Thus far, the general number field sieve (GNFS) is the most efficient classical factoring algorithm known to factor integers greater than 10^{100}, as shown in Table 1.1. Heuristically, this algorithm runs in sub-exponential time with complexity $L_n\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right]$ (as written in L-notation). In practice, the second fastest algorithm is the quadratic sieve (QS) which runs in sub-exponential time with complexity $L_n\left[\frac{1}{2}, 1\right]$. QS algorithm is considered simpler than GNFS algorithm and still the fastest for integers below 100 decimal digits but not better than GNFS algorithm for integers with 110-120 digits. Elliptic curve (EC) is the third fastest known factoring method with the same expected running time as QS algorithm in the hardest case (i.e. when n is the product of the same-bit-size primes). However, QS is superior in practice since it uses single-precision operations instead of the multi-precision operations used by EC (Menezes et al., 1996). In the case of continued fractions (CF) factoring algorithm, it runs in sub-exponential time with complexity $L_n\left[\frac{1}{2}, \sqrt{2}\right]$. For the special purpose factoring algorithm such as Pollard's $p-1$ which runs in logarithmic time, larger value of smoothness bound B make the algorithm runs slower but practically to produce a factor when B maybe between 10^5 and 10^6 (Menezes et al., 1996). The most naive factoring algorithm is via trial division or brute-forcing the given large integer N to find one of the possible prime factor which runs in exponential time. Trial division algorithm only runs in polynomial time if N is sufficiently small.

The details of the factoring algorithms mentioned in Table 1.1 can be found mostly in Menezes et al. (1996), Pomerance (1982), and Pomerance (1996).

1.6 The RSA Cryptosystem

The introduction of asymmetric cryptography in the seminal work of Diffie and Hellman (1976) and consecutively the invention of the first practical asymmetric cryptosystem known as RSA by Rivest et al. (1978) are major breakthroughs within the lengthy history of secret communications. The acronym of RSA is due to the names of its inventors, namely Rivest, Shamir, and Adleman. Ever since its existence, RSA has been implemented as the default cryptosystem in most web browsers and is also the most commonly used feature to secure internet banking systems. RSA is embedded in millions of digital applications with the objectives to provide confidentiality, integrity, authenticity and to disallow repudiation.

RSA is made up of three constituents which are the key generation, encryption and decryption algorithms. In the RSA key generation, the algorithm is initiated by choosing two same bit, distinct, and strong primes p and q known as **RSA primes** which later are used to compute the **RSA modulus** $N = pq$. Then, the $\phi(N)$ function of N is computed where $\phi(N) = (p-1)(q-1)$. Both RSA primes and $\phi(N)$ are kept secret. Next, an integer e is selected such that $e < \phi(N)$ where $\gcd(e, \phi(N)) = 1$. Both N and e are called the **RSA public keys**. Conversely, an integer d is computed based on the modular relation $ed \equiv 1 \pmod{\phi(N)}$ or can be rewritten into the **RSA key equation** given by $ed - k\phi(N) = 1$ for an integer k. The algorithm keeps the **RSA private keys** tuple $(p, q, \phi(N), d)$.

Assume that Alice wants to communicate with Bob. The entire process of key generation is conducted by the recipient of a communication or Bob. The tuple (N, e) will be issued publicly for any entity who wishes to interact with Bob or will be sent via an insecure channel (internet) to the sender or Alice. In order to encrypt the plaintext message M, Alice will use Bob's public information (N, e) and compute $M^e \equiv C \pmod{N}$, and send C to Bob via insecure channel. Upon receiving C, Bob will use his private exponent d to decrypt back the message M by performing $C^d \equiv M \pmod{N}$.

Here, in brief, we put forward the construction algorithms of the RSA cryptosystem (Rivest et al., 1978).

Algorithm 1.1 RSA's Key Generation Algorithm

```
Input: $t$-bits size of chosen primes.
Output: RSA public keys $(N, e)$ and its respective private keys $(p, q, \phi(N), d)$.
1: Selects randomly two distinct primes $p$ and $q$ such that $2^t < p, q < 2^{t+1}$.
2: Calculates $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3: Chooses an integer $e$ which satisfies $e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
4: Calculates a respective integer $d$ such that $d \equiv e^{-1} \pmod{\phi(N)}$.
5: Keeps the private keys $(p, q, \phi(N), d)$ and publicizes the public keys $(N, e)$.
```

Algorithm 1.2 RSA's Encryption Algorithm

```
Input: The plaintext $M \in \mathbb{Z}_N^*$ and public tuple $(N, e)$.
Output: The ciphertext $C$.
Calculates $C \equiv M^e (\text{mod } N)$.
Sends ciphertext $C$.
```

Algorithm 1.3 RSA's Decryption Algorithm

```
Input: A ciphertext $C$ and the private tuple $(N, d)$.
Output: The plaintext $M$.
Calculates $M \equiv C^d (\text{mod } N)$.
Recovers back plaintext message $M$.
```

Before proceeding with the proof of correctness of RSA's decryption, we provide the classical Euler's theorem as follows.

Theorem 1.3 *(Euler's Theorem) If* $\gcd(\alpha, N) = 1$*, then* $\alpha^{\phi(N)} \equiv 1 \ (mod\ N)$ *given that* $\phi(N)$ *is the Euler's totient function.*

Proof. Refer to Hardy and Wright (1979). ■

Particularly from Theorem 1.3, when computing modulo such as N where N is the product of distinct primes, the exponent can be reduced to modulo $\phi(N)$.

With the aid of Euler's theorem, we show that the decryption process of RSA reverses its encryption process.

Theorem 1.4 *(RSA's Decryption Proof of Correctness)(Rivest et al., 1978) Let* $N = pq$ *be an RSA modulus and* $\phi(N)$ *be its Euler's totient function. Suppose that* $ed \equiv 1 \ (mod\ \phi(N))$*. For any integer* $0 < M < N$ *with* $\gcd(M, N) = 1$*, if* $M^e \equiv C \ (\text{mod } N)$*, then* $C^d \equiv M \ (\text{mod } N)$*.*

Proof. Since $ed \equiv 1 \ (\text{mod } \phi(N))$ for some integer t, then

$$C^d \equiv (M^e)^d \equiv M^{1+t\phi(N)} \equiv M \cdot (M^{\phi(N)})^t \equiv M \ (\text{mod } N). \tag{1.1}$$

From Theorem 1.3, we know that $(M^{\phi(N)})^t \equiv 1^t \equiv 1 (\text{mod } N)$ since $\gcd(M, N) = 1$. This completes the proof. ■

Thus, from (1.1), it is proven that for a given ciphertext C, we can always retrieve back its corresponding plaintext M.

1.6.1 Breaking RSA: In General

Essentially, the security of RSA relies on the hardness of the integer factorization problem of the shape $N = pq$ together with the modular e^{th} root problem and the difficulty of solving the key equation problem (Menezes et al., 1996). These hard problems are briefly defined as follows.

1. **Integer Factorization Problem (IFP) for Two Large Primes.**
   Given an RSA modulus $N = pq$. Then, the integer factorization problem is to find the prime factors p and q.
2. **Modular e^{th} Root Problem.**
   Given an RSA public key pair (N, e) where $N = pq$ and $e \geq 3$. Then, the modular eth root problem is to solve for an integer M from C which is related by $C \equiv M^e \pmod{N}$.
3. **Diophantine Key Equation Problem.**
   Given an RSA modulus $N = pq$ and $e \in \mathbb{Z}$ which satisfies the equation $ed - k\phi(N) = 1$ where $\phi(N) = (p-1)(q-1)$. Then, the key equation problem is to solve for integers $\phi(N), k$, and d.

Hence, in order to cryptanalyze or break RSA, either one of these hard problems needs to be solved. Practically, solving the IFP to retrieve the prime factors p and q is desired as the other hard problems of RSA also can be solved. This is supported by the following theorem.

Theorem 1.5 *(Hinek, 2009) If the RSA modulus $N = pq$ is factored, then the e-th root problem and the Diophantine key equation problem will be solved.*

Proof. Suppose that RSA modulus N can be factored feasibly, then p and q is known. Thus, $\phi(N) = (p-1)(q-1)$ can be computed easily. Once $\phi(N)$ is known, d can be solved since

$$d \equiv e^{-1} \pmod{\phi(N)}.$$

Consequently, M can be obtained by computing $M \equiv C^d \pmod{N}$. This leads to solve the e-th root problem. Also, this leads to solve the Diophantine key equation problem since $\phi(N), k$, and d are known. ■

In the next theorem, we show that by knowing the Euler's totient function of N will lead to solve the IFP of N.

Theorem 1.6 *(Hinek, 2009) If $\phi(N)$ is known, then N will be factored in polynomial time.*

Proof. Since $N = pq$ and $\phi(N) = (p-1)(q-1)$ are known, then we can have the following relation

$$\begin{aligned} N - \phi(N) + 1 &= pq - (p-1)(q-1) + 1 \\ &= p + q. \end{aligned}$$

From here, we can construct the polynomial

$$(X - p)(X - q) = X^2 - (p+q)X + pq. \tag{1.2}$$

Thus, by solving the roots of polynomial (1.2) completes the factorization of N

$$p, q = \frac{(p+q) \pm \sqrt{(p+q)^2 - 4pq}}{2}.$$

■

According to Theorem 1.6, we should consider the value of $\phi(N)$ as a part of RSA's private key to ensure the security of RSA modulus N.

1.7 Problem Statement

Although more than four decades of intensive research on the RSA cryptosystem, no devastating attacks (i.e. factoring algorithms that run in polynomial time) have been found so far. We are motivated to attack RSA and some of its variants based on the previous attacks on RSA. The main objective of the attacks launched on RSA and its variants is to find the weaknesses that make RSA and its variants insecure and, in the worst case, break the RSA and its variants (i.e. solve the hard mathematical problems embedded in the scheme). These attacks scrutinize the security of the RSA in order for RSA to remain relevant in practice. It is a fact that the vastness of the domains of its parameters and applications exposes the cryptosystem to more potential attacks and vulnerabilities. This research intends to discover these new attacks to be compiled for future criteria and conditions required to design a secure RSA and its variant cryptosystems.

1.8 Research Objectives and Methodology

We conduct a number of attacks on the RSA cryptosystem and some of its variant cryptosystems throughout this thesis. Thus, we put forward the objectives of every attack with their methodologies accordingly:

1. *To propose a new Diophantine approximations cryptanalysis of RSA.*

   Methodology: To achieve this objective, we introduce our strategy called the continuous midpoint subdivision analysis on the interval containing the Euler's totient function of an RSA cryptosystem. We prove that the unknown parameters d and k can be found among the convergents of the continued fractions expansion of certain public number. Afterwards, we solve for the prime factors of the modulus $N = pq$. At the end of this work, we will improve the upper cryptanalytic bound of the private exponent d as opposed to the previous results with similar approach.

2. *To propose a new Diophantine approximations cryptanalysis againts variants of RSA with modified Euler quotient.*

   Methodology: This objective can be achieved by conducting a continuous midpoint subdivision analysis upon an interval containing $(p^2-1)(q^2-1)$ together with continued fractions on the key relation of some variants of RSA. Each of these variants share a common key relation given by the key relation $ed - k(p^2-1)(q^2-1) = 1$ where e and d are the public and private keys respectively. We remark at the end of this work, we raise the security bound for d exponentially as opposed to the previous results with similar approach (i.e. via the continued fractions algorithm).

3. *To propose a new Diophantine approximations cryptanalysis againts variants of RSA with arbitrary bit-size prime factors.*

   Methodology: To achieve this objective, we propose a generalization of the method and strategy that has been discussed in the second objective. The motivation of the attack is based on the idea that our strategy also works on the case when the prime factors of modulus $N = pq$ of variants of RSA cryptosystem are unbalanced primes. That is, the primes p and q are of arbitrary bit size satisfying the relation $q < p < \lambda q$ where λ is a chosen parameter specifically $\lambda > 2$.

4. *To cryptanalyze RSA modulus with special-structured key equation.*

   Methodology: To achieve this objective, first we show that if e satisfies the Diophantine equation of the form $ex^2 - \phi(N)y^2 = z$ for appropriate values of x, y and z under certain specified conditions, then one is able to factor the RSA modulus N. The main idea is to find the unknown $\frac{y}{x}$ that can be found amongst the convergents of $\frac{\sqrt{e}}{\sqrt{N}}$ via continued fractions algorithm. Consequently, Coppersmith's theorem is applied to solve for prime factors p and q in polynomial time possible.

5. *To cryptanalyze simultaneously the k RSA moduli with special-structured key equation.*

   Methodology: We use the combination of simultaneous Diophantine approximation and lattice basis reduction via the LLL algorithm to retrieve the private parameters (x, y_i) or (x_i, y) that would render the factorisation of k RSA moduli $N_i = p_i q_i$ simultaneously in polynomial time possible.

1.9 Thesis Outline

This thesis covers eight chapters and is organized as follows.

Chapter 1 briefly describes on the progress of public key cryptography and its related components such as the integer factorization problem before proceeding with the details of textbook RSA cryptosystem. This chapter includes the concept of cryptanalysis upon a PKC and breaking the RSA in general, and also discusses some existing factoring algorithms in practice. Then, the research objectives together with their methodologies are presented in depth.

Chapter 2 introduces in detail the mathematical tools (i.e. the Diophantine approximation and lattice basis reduction) that will be used in subsequent chapters to construct our algebraic attacks. This chapter also provides some existing cryptanalytic works on RSA via continued fractions and Coppersmith's method. We also survey some variants of RSA with particular structure key equation and its algebraic cryptanalysis.

Chapter 3 introduces a method called the continuous midpoint subdivision analysis (CMSA) on the interval containing the Euler's totient function (i.e. $\phi(N) = (p-1)(q-1)$), along with continued fractions on the key relation of RSA with the aim to factor the RSA modulus. We also provide a working numerical example to illustrate our proposed attack.

Chapter 4 highlights the continuous midpoint subdivision analysis (CMSA) on the interval containing the modified Euler quotient function together with continued fractions on the modified key relation of some variants of RSA with the aim to factor its modulus. Note that, the variants of RSA that we consider utilized the modified key equation of the form $ed - k(p^2-1)(q^2-1) = 1$. We also provide numerical examples to illustrate our proposed attack. In this chapter, we consider the prime factors of modulus N to be balanced primes.

Chapter 5 generalizes the strategy that we propose in Chapter 4 by considering the case when the prime factors are of arbitrary sizes (i.e. $q < p < \lambda q$) or simply called unbalanced primes. We also include working examples to illustrate our generalized attack and as comparison with the previous results.

Chapter 6 presents a new weak RSA key equation structure that would render the factorization of modulus N using the combination of continued fractions and Coppersmith's method (via LLL algorithm) feasible in polynomial time. In this chapter, we provide a working example to illustrate our attack and a comparative analysis against some relevant literatures.

Chapter 7 considers the system of modified generalized RSA key equations that potentially contribute to solve the k instances of RSA moduli simultaneously from the given (N_i, e_i) for $i = 1, 2, \cdots, k$. Particularly, we propose two cryptanalytic works upon k instances of Diophantine equations of the form $e_i x^2 - y_i^2 \phi(N_i) = z_i$ and $e_i x_i^2 - y^2 \phi(N_i) = z_i$. Both attacks involve solving the simultaneous Diophantine approximations using lattice basis reduction techniques.

Chapter 8 summarizes all our results together with suggestions of potential future works that can be extended from this research.

REFERENCES

Ariffin, M. R. K., Abubakar, S. I., Yunos, F., and Asbullah, M. A. (2019). New Cryptanalytic Attack on RSA Modulus $N = pq$ Using Small Prime Difference Method. *Cryptography*, 3(1):1–25.

Barker, E. (2016). NIST Special Publication 800-57 Part 1 Revision 4; Recommendation for Key Management Part 1: General. *NIST, Tech. Rep.*

Bernstein, D. J., Chang, Y.-A., Cheng, C.-M., Chou, L.-P., Heninger, N., Lange, T., and Van Someren, N. (2013). Factoring RSA keys from certified smart cards: Coppersmith in the wild. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 341–360. Springer.

Blömer, J. and May, A. (2004). A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*, pages 1–13. Springer.

Boneh, D. and Durfee, G. (2000). Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$. *IEEE Transactions on Information Theory*, 46(4):1339–1349.

Bunder, M., Nitaj, A., Susilo, W., and Tonien, J. (2016). A new attack on three variants of the RSA cryptosystem. In *Australasian Conference on Information Security and Privacy*, pages 258–268. Springer.

Bunder, M., Nitaj, A., Susilo, W., and Tonien, J. (2017). A Generalized Attack on RSA Type Cryptosystems. *Theoretical Computer Science*, 704(3):74–81.

Bunder, M., Nitaj, A., Susilo, W., and Tonien, J. (2018). Cryptanalysis of RSA-Type Cryptosystems Based on Lucas Sequences, Gaussian Integers and Elliptic Curves. *Journal of Information Security and Applications*, 40:193–198.

Bunder, M. and Tonien, J. (2017). A New Attack on the RSA Cryptosystem Based on Continued Fractions. *Malaysian Journal of Mathematical Sciences*, 11(S3):45–57.

Castagnos, G. (2007). An Efficient Probabilistic Public-Key Cryptosystem Over Quadratic Fields Quotients. *Finite Fields and Their Applications*, 13(3):563–576.

Coppersmith, D. (1996). Finding a small root of a bivariate integer equation; Factoring with high bits known. In *Maurer U. (eds) Advances in Cryptology EUROCRYPT 96. EUROCRYPT 1996. Lecture Notes in Computer Science*, pages 178–189. Springer.

Coppersmith, D. (1997). Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *Journal of Cryptology*, 10(4):233–260.

De Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28.

Diffie, W. and Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

Elkamchouchi, H., Elshenawy, K., and Shaban, H. (2002). Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In *The 8th International Conference on Communication Systems, 2002. ICCS 2002.*, pages 91–95. IEEE.

Galbraith, S. D. (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press.

Hardy, G. H. and Wright, E. M. (1979). *An Introduction to the Theory of Numbers*. Oxford University Press.

Hinek, M. J. (2009). *Cryptanalysis of RSA and its Variants*. CRC Press.

Hoffstein, J., Pipher, J., Silverman, J. H., and Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*. Springer.

Knudsen, L. R. (1998). Block Ciphers — A Survey. In *State of the art in applied cryptography*, pages 18–48. Springer.

Kuwakado, H., Koyama, K., and Tsuruoka, Y. (1995). A New RSA-Type Scheme Based on Singular Cubic Curves $y^2 = x^3 + bx^2 \pmod{n}$. *IEICE Transactions on Fundamentals of Electronics*, 78(1):27–33.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534.

Maitra, S. and Sarkar, S. (2008). Revisiting Wieners attack–new weak keys in RSA. In *International Conference on Information Security*, pages 228–243. Springer.

May, A. (2009). Using LLL-reduction for solving RSA and factorization problems. In *The LLL Algorithm*, pages 315–348. Springer.

Menezes, A. J., Katz, J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Nemec, M., Sys, M., Svenda, P., Klinec, D., and Matyas, V. (2017). The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1631–1648. Association for Computing Machinery.

Nitaj, A. (2008). Another generalization of Wieners attack on RSA. In *International Conference on Cryptology in Africa*, pages 174–190. Springer.

Nitaj, A. (2013). Diophantine and lattice cryptanalysis of the RSA cryptosystem. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, pages 139–168. Springer.

Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and Bahig, H. M. (2014). New attacks on the RSA cryptosystem. In *International Conference on Cryptology in Africa*, pages 178–198. Springer.

Nitaj, A., Pan, Y., and Tonien, J. (2018). A generalized attack on some variants of the RSA cryptosystem. In *International Conference on Selected Areas in Cryptography*, pages 421–433. Springer.

Papadimitriou, C. H. (2003). *Computational Complexity*. John Wiley and Sons Ltd.

Peng, L., Hu, L., Lu, Y., and Wei, H. (2016). An improved analysis on three variants of the RSA cryptosystem. In *International Conference on Information Security and Cryptology*, pages 140–149. Springer.

Pomerance, C. (1982). Analysis and Comparison of Some Integer Factoring Algorithms. In *Mathematisch Centrum Computational Methods in Number Theory, Part 1*, pages 89–139. Math. Centrum.

Pomerance, C. (1996). A Tale of Two Sieves. *Notices of the AMS*, 43(12):1473–1485.

Riesel, H. (2012). *Prime Numbers and Computer Methods for Factorization*. Springer Science & Business Media.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126.

Schmidt, W. M. (1980). *Diophantine Approximation*. Springer-Verlag Berlin Heidelberg.

Sedgewick, R. and Wayne, K. (2011). *Algorithms (Fourth Edition)*. Addison-Wesley.

Sipser, M. (2012). *Introduction to the Theory of Computation*. Cengage Learning.

Tonien, J. (2018). *Continued Fractions and Their Applications*. Doctor of Philosophy, School of Mathematics and Applied Statistics, University of Wollongong.

Wiener, M. J. (1990). Cryptanalysis of Short RSA Secret Exponents. *IEEE Transactions on Information Theory*, 36(3):553–558.

Williams, H. (1980). A Modification of the RSA Public-Key Encryption Procedure (Corresp.). *IEEE Transactions on Information Theory*, 26(6):726–729.

Yan, S. Y. (2009). *Primality Testing and Integer Factorization in Public-Key Cryptography*. Springer.

Zheng, M., Kunihiro, N., and Hu, H. (2018). Cryptanalysis of RSA variants with modified Euler quotient. In *International Conference on Cryptology in Africa*, pages 266–281. Springer.

BIODATA OF THE STUDENT

Wan Nur Aqlili binti Wan Mohd Ruzai was born on 26 February 1990 in Sik, Kedah, Malaysia. She is the proud alumni of Sekolah Kebangsaan Sik, Sekolah Menengah Kebangsaan Sik, and MRSM Beseri as she completed her primary and secondary education here. She obtained her bachelor's degree in Mathematical Sciences from International Islamic University Malaysia in 2014. She then received a Master of Science (Mathematics) from Universiti Kebangsaan Malaysia in 2016. She has currently enrolled in a doctoral study at the Institute for Mathematical Research, Universiti Putra Malaysia in the area of Mathematical Cryptography. She actively joins the programs organized by her institute and acts as the treasurer of the INSPEM Student Society Club. Her research interest focuses on mathematical cryptography, algebraic cryptanalysis, and post-quantum cryptography. In her life, she always believes that anything is possible with a willing heart. The student can be reached via:

- Email: ************@gmail.com.my

LIST OF PUBLICATIONS

The following are the list of publications that arise from this study.

Wan Nur Aqlili Ruzai, Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Zahari Mahad, and Muhammad Asyraf Asbullah. (2021). Increment of Insecure RSA Private Exponent Bound Through Perfect Square RSA Diophantine Parameters Cryptanalysis, *Computer Standards & Interfaces*, Vol. 80, p. 103584.

Wan Nur Aqlili Ruzai, Muhammad Rezal Kamel Ariffin, Muhammad Asyraf Asbullah, Zahari Mahad, and Athirah Nawawi. (2020). On the Improvement Attack Upon Some Variants of RSA Cryptosystem via the Continued Fractions Method, *IEEE Access*, Vol. 8, pp. 80997-81006.

Wan Nur Aqlili Ruzai, Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin, Amir Hamzah Abd Ghafar and Mohamat Aidil Mohamat Johari(2021). An Attack on $N = p^2q$ as a Result When Some Information of Bits on the Multiple of the Prime Factors is Known. *Malaysian Journal of Mathematical Sciences*. (Accepted for Publication).

Muhammad Rezal Kamel Ariffin, **Wan Nur Aqlili Ruzai**, Muhammad Asyraf Asbullah, and Zahari Mahad. (2020). Cryptanalysis of RSA Cryptosystem via the Continued Midpoint Subdivision Analysis. *In the Proceeding of the* 7^{th} *International Cryptology and Information Security Conference 2020*, 9 - 10 June 2020, Malaysia, pp. 10 - 19.

Muhammad Rezal Kamel Ariffin, Amir Hamzah Abd Ghafar, **Wan Nur Aqlili Ruzai**, and Nurul Nur Hanisah Adenan. (2021). New Approach for Efficiently Computing Factors of the RSA Modulus. *In Soft Computing Approach for Mathematical Modeling of Engineering Problems*, 1 September 2021, CRC Press.

Wan Nur Aqlili Ruzai, Muhammad Rezal Kamel Ariffin, and Muhammad Asyraf Asbullah. (2019). On the Variants of RSA Cryptosystem and Its Related Algebraic Cryptanalysis, *In Seminar on Mathematical Sciences "Embracing Mathematical Diversity"*, 25 September 2019, Malaysia, pp. 67-81.

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : ________________

TITLE OF THESIS / PROJECT REPORT :

____

____

____

NAME OF STUDENT : ____

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

□	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
□	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☑	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

□ **PATENT** Embargo from_____________ until ______________
(date) (date)

Approved by:

________________________ ________________________

(Signature of Student) (Signature of Chairman of Supervisory Committee)
New IC No/ Passport No.: Name:

Date : Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]