UNIVERSITI PUTRA MALAYSIA

EXTENDING JOCHEMSZ-MAY ANALYTICAL STRATEGIES UPON INTEGER FACTORIZATION PROBLEM

NURUL NUR HANISAH BINTI ADENAN

IPM 2021 3

EXTENDING JOCHEMSZ-MAY ANALYTICAL STRATEGIES UPON INTEGER FACTORIZATION PROBLEM

By

NURUL NUR HANISAH BINTI ADENAN

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

February 2021

DEDICATIONS

Buat mak dan abah yang tercinta,
Coretan takkan mampu melahirkan rasa,
Pada Allah jua ku pohonkan doa,
Moga diampuni segala dosa,
Moga Allah kurniakan syurga,
Pada mak dan abah yang tiada gantinya.

Untuk Abg Sham dan Angah,
Kak Zai, Abg Hai, Yaya dan Uwais,
Terima kasih untuk setiap sokongan dan dorongan,
Telinga yang mendengar,
Tangan yang membantu,
Lidah yang menasihati,
Takkan ada galang ganti.

Tak lupa juga rakan seperjuangan,
Saksi jatuh dan bangun,
Duka dan ria,
Tangis dan gembira,
Teguh setia bersama.

Terima kasih kerna ada,
Terima kasih kerna percaya.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

EXTENDING JOCHEMSZ-MAY ANALYTICAL STRATEGIES UPON INTEGER FACTORIZATION PROBLEM

By

NURUL NUR HANISAH BINTI ADENAN

February 2021

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

The first public key cryptosystem namely RSA has been used extensively throughout the world since its invention in 1978. Since then, cryptanalytic research on this cryptosystem began with the purpose to enhance its security. In this thesis, we present three analytical attacks on the modulus $N = p^2q$ by utilizing Jochemsz-May strategy. We show that the modulus can be factored if the elements in the cryptosystem satisfy our conditions.

For the first attack, we utilize the modulus $N = p^2q$ where p and q are large balanced primes. Suppose there exists $e \in \mathbb{Z}^+$ satisfying $\gcd(e, \phi(N)) = 1$ where $\phi(N) = p(p-1)(q-1)$ and $d < N^{\delta}$ be its corresponding private exponent such that $d \equiv e^{-1} \mod \phi(N)$. From $ed - k\phi(N) = 1$, by utilizing the extended strategy of Jochemsz and May, our attack works when the primes share a known amount of Least Significant Bits (LSBs). This is achievable since we obtain the small roots of our constructed integer polynomial that consequently leads to the factorization of N. More specifically we show that N can be factored when the bound $\delta < \frac{2}{3} + \frac{3}{2}\alpha - \frac{1}{2}\gamma$. Our attack enhances the bound of some former attacks upon $N = p^2q$.

Next, we describe a cryptanalytic study on RSA with the modulus $N = p^2q$ with the existence of two key equations. Let $e_1, e_2 < N^{\gamma}$ be the integers such that $d_1, d_2 < N^{\delta}$ be their multiplicative inverses. Based on two key equations $e_1d_1 - k_1\phi(N) = 1$ and $e_2d_2 - k_2\phi(N) = 1$ where $\phi(N) = p(p-1)(q-1)$, our attack works when the primes share a known amount of LSBs and the private exponents share an amount of Most Significant Bits (MSBs). We apply the extended strategy of Jochemsz and May to find the small roots of a polynomial and show that if $\delta < \frac{11}{10} + \frac{9}{4}\alpha - \frac{1}{2}\beta - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 990\alpha - 180\beta + 64}$, then N can be factored. Our attack improves the bounds of some previously proposed attacks that makes the RSA vulnerable.

Lastly, we present an attack on RSA with the modulus $N = p^2q$. Let $e < N^{\gamma}$ be the public exponent satisfying the equation $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Our attack is applicable when some amount of LSBs of ap and bq are known. We use the extended strategy of Jochemsz and May as our main method to find the small roots of our polynomial and show that the modulus N can be factored if $\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{44}{45}\alpha - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(3\alpha - 3\beta + 1)(-84\alpha + 45\gamma + 39\beta - 28)}$. In this final segment of our research, we conclude that our approach via extending Jochemsz and May analytical strategies does not improve previous bounds. Hence, answers existing unknown outcome on this matter.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Sains

STRATEGI ANALITIK LANJUTAN JOCHEMSZ-MAY TERHADAP MASALAH PENGFAKTORAN INTEGER

Oleh

NURUL NUR HANISAH BINTI ADENAN

Februari 2021

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

Kunci umum pertama yang dikenali sebagai RSA telah digunakan di seluruh dunia sejak penciptaannya pada tahun 1978. Sejak itu, bermulanya penyelidikan kripanalitik terhadap sistem kripto ini bertujuan untuk menambah baik tahap keselamatannya. Dalam tesis ini, kami membentangkan tiga serangan secara analitik terhadap modulus $N = p^2q$ dengan menggunakan strategi Jochemsz-May. Kami menunjukkan bahawa modulus tersebut dapat difaktorkan sekiranya elemen-elemen dalam sistem kripto ini memenuhi syarat yang telah kami tetapkan.

Pertama, kami mengkaji serangan terhadap sistem kripto RSA yang menggunakan modulus $N = p^2q$ yang mana p dan q adalah suatu nombor perdana besar dan seimbang. Andaikan e adalah suatu nombor bulat positif dan memenuhi syarat $\gcd(e,\phi(N)) = 1$ yang mana $\phi(N) = p(p-1)(q-1)$ dan $d < N^{\delta}$ adalah eksponen rahsia sedemikian hingga $d \equiv e^{-1} \mod (\phi N)$. Daripada persamaan kunci RSA $ed - k\phi(N) = 1$, dengan menggunakan strategi lanjutan Jochemsz dan May, serangan kami berhasil apabila dua nombor perdana tersebut berkongsi bit keertian terkecil. Ianya mampu dicapai apabila kami memperoleh nilai punca yang kecil daripada pembinaan polinomial integer yang membawa kepada pengfaktoran N. Secara khususnya, kami membuktikan bahawa N mampu difaktorkan sekiranya batas $\delta < \frac{2}{3} + \frac{3}{2}\alpha - \frac{1}{2}\gamma$. Serangan kami berjaya mengatasi batas beberapa serangan terdahulu terhadap $N = p^2q$.

Seterusnya, kami memperihalkan berkenaan serangan terhadap RSA yang menggunakan modulus $N = p^2q$ dengan kewujudan dua persamaan kekunci. Andaikan $e_1, e_2 < N^{\gamma}$ menjadi nombor bulat sedemikian hingga $d_1, d_2 < N^{\delta}$ menjadi songsangan terhadap pendaraban mereka. Berdasarkan dua persamaan kekunci, $e_1d_1 - k_1\phi(N) = 1$ dan $e_2d_2 - k_2\phi(N) = 1$ di mana $\phi(N) = p(p-1)(q-1)$, serangan kami berhasil apabila nombor -nombor perdana berkongsi bit keertian terkecil dan eksponen rahsia berkongsi bit keertian terbesar. Kami mengaplikasikan strategi lanjutan Jochemsz-May untuk mencari nilai punca yang kecil daripada polinomial

dan menunjukkan jika $\delta < \frac{11}{10} + \frac{9}{4}\alpha - \frac{1}{2}\beta - \frac{1}{2}\gamma - \frac{1}{30}\sqrt{180\gamma + 990\alpha - 180\beta + 64}$, maka N boleh difaktorkan. Serangan kami telah berjaya menambah baik batas beberapa serangan yang dibentangkan sebelum ini.

Akhir sekali, kami membentangkan serangan terhadap RSA yang menggunakan modulus $N = p^2 q$. Andaikan $e < N^{\gamma}$ adalah eksponen umum yang memenuhi syarat persamaan $ed - k(N - (ap)^2 - apbq + ap) = 1$ di mana $\frac{a}{b}$ adalah anggaran $\frac{q}{p}$ yang tidak diketahui nilainya. Serangan kami berjaya dilaksanakan jika sejumlah bit keertian terkecil ap dan bq diketahui. Kami menggunakan strategi lanjutan Jochemsz dan May dalam mencari nilai punca yang kecil daripada polinomial dan menunjukkan bahawa N boleh difaktorkan sekiranya $\delta < \frac{91}{135} + \frac{29}{45}\beta - \frac{44}{45}\alpha - \frac{2}{3}\gamma - \frac{2}{135}\sqrt{2(3\alpha - 3\beta + 1)(-84\alpha + 45\gamma + 39\beta - 28)}$. Kesimpulannya, kami mendapati bahawa pendekatan kami melalui strategi lanjutan Jochemsz dan May secara analitik tidak meningkatkan batas daripada kajian yang sebelumnya.

ACKNOWLEDGEMENTS

Alhamdulillah.

All praises to Al Mighty Allah, by His permission, I finally managed to complete my thesis of Master Research in Mathematical Cryptography.

The first person that I would like to thank the most is my supervisor, Prof. Dr. Muhammad Rezal Kamel Ariffin for his willingness to accept me as one of his students. Thank you Prof. for all the guides, experiences and beneficial knowledge throughout my master journey. May Allay rewards your meritorious effort with success in this world and hereafter. Special thanks to my Co-Supervisor Dr Mohamat Aidil Mohamat Johari for his concerns in checking and giving feedback on my thesis.

Next, I want to express my gratitude to the most important people in my whole life, my parents, Adenan Bin Ismail and Ku Noreha Binti Ku Haris, and family for endless support and encouragement. Their morally and financially supports really help me in enduring the hardships in study. I could not ask for more.

I also would like to thank my friends, Wan Nur Aqlili Wan Mohd Ruzai, Nurnazhifa Ab Rahman, Normahirah Nek Abd Rahman, Tea Boon Chian, Rasyid Redha Mohd Tahir, Amir Hamzah Abd Ghaffar, Saidu Isah Abu Bakar, and also Dr. Muhammad Asyraf Asbullah and Encik Zahari Mahad for the indefinite help. Lastly, thank you to UPM for the sponsorship given to me during my study.

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

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

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: 06 May 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: Nurul Nur Hanisah binti Adenan, GS48915

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: Mohamat Aidil bin Mohamat Johari

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

CRT	Chinese Remainder Theorem
det	Determinant
gcd	Greatest Common Divisor
IFP	Integer Factorization Problem
LLL	Lenstra-Lenstra-Lovasz
LSB	Least Significant Bits
MSB	Most Significant Bits

Greek Symbol

$\mathbb{Z}$	Integer
$\mathbb{N}$	Natural Number
$\mathbb{R}$	Real Number

Subscripts

$\mathbb{Z}_N$	Integer within 0 and N
$\mathbb{Z}_{\phi(N)}$	Integer within 0 and $\phi(N)$

Superscript

$\mathbb{Z}^*$	Relatively Prime Integer
$\mathbb{Z}^+$	Positive Integer

CHAPTER 1

INTRODUCTION

1.1 Cryptography

The world of cryptography evolved since centuries ago and its application in communication is very significant considering it serves the purpose of having a secure channel and keeping the information sealed from the third party or adversary. Being in this digital world today, almost every transmission of data, transaction of money, conversation between two parties, etc involve the usage of the internet and thus the practice of cryptography becomes more essential.

Cryptography comprises of two branches which are symmetric cryptography and asymmetric cryptography. Encryption and decryption via symmetric cryptography uses only one key. Thus, the key needs to be kept secret between the sender and the receiver. The examples of symmetric cryptography are Advanced Encryption Standard (AES), Data Encryption Standard (DES), stream ciphers and block ciphers. For futher reading, reader may refer to (Katz and Lindell, 2020) and (Stinson and Peterson, 2018).

On the other hand, asymmetric cryptography uses two different keys to encrypt and decrypt the data. It is also known as public key cryptography. However, only the encryption key is publicized. Its decryption key must be kept secret. Diffie-Hellman Key Exchange was the first concept introduced by Diffie and Hellman (1976) that leads to the invention of other asymmetric crytosystem. The instance of cryptosystem that practice this type of cryptography are RSA(Rivest et al., 1978), El Gamal Cryptosystem (ElGamal, 1985), Rabin-p Cryptosystem (Asbullah and Ariffin, 2016), and Elliptic Curve Cryptography (ECC) .

Every of the cryptosystem needs to achieve four objectives of cryptography in order to ensure their cryptosystems are secure to be applied. The first objective is confidentiality which means unauthorised party cannot access the information. The second objective is authenticity; the source of the message must be validated to ensure the sender is properly identified. The third is integrity. One need to assure or pledge that the message was not modified during transmission whether by accidentally or intentionally. The last one is non-repudiation. A sender cannot deny that he has sent the message to the receiver.

1.2 Asymmetric Encryption

Assymetric encryption is composed by two different keys which known as public key and private key. We provide an appropriate definition as follows.

Definition 1.1 ***(Asymmetric Encryption)****(Diffie and Hellman, 1976). Let the message space be denoted as M, the ciphertext space be denoted by L, the key space be denoted by K, the plaintext be denoted by m and the ciphertex be denoted by c. Asymmetric encryption scheme is defined as follows.*

1. *Key generation algorithm K is a probabilistic algorithm that will generate a public key denoted as $e \in K$ and private key as $d \in K$ respectively.*
2. *Encryption algorithm E is a probabilistic algorithm that takes a message $m \in M$ and the public key e, to produce a ciphertext $c \in C$ as a function of $c = E_e(m)$.*
3. *Decryption algorithm D is a deterministic algorithm which is given the ciphertext and the private key d, will output m. That is, $m = D_d(c)$.*

Definition 1.2 ***(One-way Function and Trapdoor One-way Function)***
(Menezes et al., 2018). A one-way function is a function that only easy applied in one direction but not in vice versa. The inverse is very hard to compute. For $x \in X$ and $y \in Y$, let $f : X \longrightarrow Y$ be an invertible function. Then

1. *The computation of the value $y = f(x)$ is easy.*
2. *The computation of the value $x = f^{-1}(y)$ is hard.*

The computation of the inverse for one-way function $x = f^{-1}(y)$ would be easy with a trapdoor one-way function.

1.3 Integer Factorization Problem

The security of the RSA cryptosystem relies on the intractability of solving its hard problems. We include Integer Factorization Problem (IFP) in our section to emphasize the importance of this problem as it is the main strength that keeps the RSA secure until today. If the IFP is solvable, then the RSA cryptosystem is no more relevant to be used. Since this problem relates to the factorization of two large primes, thus we provide some essential definitions and theorems regarding this matter.

Definition 1.3 (Prime Number) *For an integer p such that $p \geq 2$, can be called as a prime if such number only divisible by 1 and itself.*

Definition 1.4 (Balanced Primes) *The primes p and q are considered balanced primes if they have the same bit size such that $q < p < 2q$.*

Theorem 1.1 (The Fundamental Theorem of Arithmetic)*(Hoffstein et al., 2008) Given $\{n \in \mathbb{Z} | n \geq 2\}$, the prime factorization of n is written as*

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

where $p_1 \dots p_k$ are distinct primes and $a_i \geq 1$ for $i = 1, \dots, k$. Regardless of its ordering, this expression is unique.

Definition 1.5 (Integer Factorization Problem)*(Menezes et al., 2018). Suppose $N \in \mathbb{Z}^+$. Then the integer factorization problem (IFP) is described as the problem to find the prime factorization of N such that $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ where p_i are distinct primes and $a_i \geq 1$.*

The researchers were intrigued by the IFP because this problem is seemingly easy to solve. Hence, many algorithms have been proposed with the aim to find the factorization of N. For instance, Trial Division, Pollards $p-1$ Factoring Algorithm, Factorization via Difference of Square, Quadratic Sieve Factoring, Elliptic Curve Method and Number Field Sieve Method(Hoffstein et al., 2008). We discuss in brief some of the algorithms in this section.

1.3.1 Pollard's $p-1$ Factoring Algorithm

In 1974, J. M. Pollard invented an algorithm to show that there exists insecure RSA modulus although it seemingly secure. Let $N = pq$ be the product of two primes. Suppose that there exists an integer L that comply to this condition

$$p-1 \text{ divides } L \qquad \text{and} \qquad q-1 \text{ does not divide } L.$$

This means that there exists integers h, i and j such that

$$L = h(p-1) \qquad \text{and} \qquad L = i(q-1) + j.$$

Assuming we choose an integer a and we want to compute a^L. From Fermat's Little Theorem, it proves that

$$a^L = a^{h(p-1)} = (a^{p-1})^h \equiv 1^h \equiv 1 (\text{mod } p)$$
$$a^L = a^{i(q-1)+j} = a^j (a^{q-1})^i \equiv a^j 1^i \equiv a^j (\text{mod } q)$$

which can be translate into

$$p | (a^L - 1) \quad \text{and} \quad q \nmid (a^L - 1).$$

Since $p|(a^L - 1)$, thus, we can retrieve the prime p through the following computation

$$p = \gcd(a^L - 1, N).$$

However, in order to find the integer L, the factor of $p-1$ must contain a lot of small primes. Thus, taking the product a few of the first small primes would give the multiple of $p-1$. Thus, one needs to ensure that the choice of the prime does not have these properties in order to resist Pollard's $p-1$ Factoring Algorithm.

1.3.2 Factorization via Difference of Square

This algorithm relies on the following mathematical relation

$$X^2 - Y^2 = (X+Y)(X-Y).$$

From the above equation, it can interpreted that the difference between two squares is equal to a product. It can be apply on the factorization of N. In order to factor N, we need to find an integer c such that $N + c^2 = b^2$ where b is also an integer. Thus,

$$N = b^2 - c^2 = (b+c)(b-c).$$

Example 1.1 *Given $N = 19519$, find an integer c such that the summation of N and b^2 is equal to perfect square.*

$$\begin{aligned}
19519 + 1^2 &= 19520 \\
19519 + 2^2 &= 19523 \\
19519 + 3^2 &= 19528 \\
19519 + 4^2 &= 19535 \\
19519 + 5^2 &= 19544 \\
19519 + 6^2 &= 19555 \\
19519 + 7^2 &= 19568 \\
19519 + 8^2 &= 19583 \\
19519 + 9^2 &= 19600 = 140^2 \qquad (\textit{square!})
\end{aligned}$$

Hence, we compute $19519 = 140^2 - 9^2 = (140-9)(140+9) = 131 \cdot 149$.

However, if the number N is a large number, then it is quite difficult to randomly choose the value c such that $N + c^2 = b^2$. Thus, the mathematical equation is altered into

$$kN = b^2 - c^2 = (b+c)(b-c).$$

Since the product $(b+c)(b-c) = kN$, thus we need to find $\gcd(N, b+c)$ and $\gcd(N, b-c)$ in order to factor N.

1.3.3 Quadratic Sieve Factoring

This method is known as the fastest algorithm in order to factor the modulus $N = pq$. However it is only retsricted to 300 bits long. The following definition describes the basis principle of this method (Katz and Lindell, 2008).

Definition 1.6 *Let $N \in \mathbb{Z}$ and there exists $x, y \in \mathbb{Z}$ such that $x^2 \equiv y^2 (\text{mod } N)$ and $x \not\equiv \pm y (\text{mod } N)$. This implies that $x^2 - y^2 (\text{mod } N) \not\equiv 0 (\text{mod } N)$ which means $N \nmid (x-y)$ and $N \nmid (x+y)$. Thus, $(x-y)$ must be relatively prime to N.*

1.3.4 Complexity and Running time of Current Known Strategies to Solve IFP

We summarize the complexity and running time of current stratergies to solve integer factorization problem through the following table.

Table 1.1: Complexity and running time of current algorithms to solve IFP

Algorithm	Complexity	Running Time
Trial Divisions	$\mathcal{O}(n^2\sqrt{N})$	Exponential
Pollard $p-1$ Factorization	$\mathcal{O}(K\log K\log^2 n)$	Logarithmic
Factorization via Difference of Square	$\mathcal{O}(\sqrt{N})$	Exponential
Quadratic Sieve Factoring	$\mathcal{O}(e^{(1+o(1))(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}})$	Sub-exponential
Elliptic Curve Method	$\mathcal{O}(e^{(1+o(1))(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}})$	Sub-exponential
Continued Fraction Method	$\mathcal{O}(e^{(\sqrt{2}+o(1))(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}})$	Sub-exponential
Number Field Sieve	$\mathcal{O}(e^{(\sqrt[3]{\frac{64}{9}}+o(1))\ln n^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}})$	Sub-exponential

1.4 RSA Cryptosystem

Secure communication up till the 70's was executed through symmetrical ways. In other word, the same key is used for encryption and decryption processes. Later in 1978, the first asymmetric cryptosystem went public and solved the problematic issue of distributing keys. This cryptosystem used different keys to encrypt and decrypt the data. It is known as the RSA cryptosystem(Rivest et al., 1978). The construction of the RSA algorithm comprises of key generation, encryption and decryption. During the key generation process, two large balanced primes p and q are generated and the number $N = pq$ is computed. Next, let e be a random integer that is coprime with $\phi(N)$ where $\phi(N) = (p-1)(q-1)$ is the Euler totient function and d be the multiplicative inverse of e mod $\phi(N)$. The security of the RSA relies on the difficulty on solving three hard problems which are factoring the large modulus N, solving the modular e^{th} root problem and solving the key equation $ed - k\phi(N) = 1$.

Definition 1.7 ***(Modular*** e^{th} ***Root Problem)****(Menezes et al., 2018) Suppose $N = pq$ and $e \geq 3$ be the odd integer. Then the modular e^{th} problem is finding $m \in \mathbb{Z}$ from c such that $c \equiv m^e \pmod{N}$.*

Definition 1.8 ***(Euler's*** ϕ ***Function)****(Menezes et al., 2018) Suppose the set $\{0,1,\cdots,N-1\}$ be the elements of residue system modulo N. This number of element in the set of residue system modulo N is called Euler's totient function and denoted as $\phi(N)$.*

Theorem 1.2 *(Menezes et al., 2018) If the prime factorization of N is $N = p_1^{r_1} p_2^{r_2} p_3^{r_3} p_4^{r_4} \cdots p_t^{r_t}$, then*

$$\phi(N) = \prod_{j=1}^{t} p_j^{r_j - 1}(p_j - 1).$$

Corollary 1.1 *(Menezes et al., 2018) If $N = pq$ then*

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

The RSA construction algorithm is defined as follows.

Algorithm 1.1 RSA Key Generation

Input: The bitsize k of the modulus
Output: A public key (N, e) and a private key (N, d)

1. Generate two large random and distinct primes p and q with $(k/2)$-bit size.
2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Choose a random integer e such that $\gcd(e, \phi(N)) = 1$.
4. Compute multiplicative inverse of e, $d \equiv e^{-1} \pmod{(\phi(N))}$.
5. Return the public key (N, e) and the private key (N, d).

Algorithm 1.2 RSA Encryption

Input: The public key (N, e) and the plaintext M
Output: The ciphertext C

1. Choose plaintext M with $M \in \mathbb{Z}_N^*$.
2. Compute $C \equiv M^e \pmod{N}$.
3. Return the ciphertext C.

Algorithm 1.3 RSA Decryption

Input: The private key (N, d) and the plaintext C
Output: The plaintext M

1. Compute $M \equiv C^d \pmod{N}$.
2. Return the message M.

Proof of Correctness for RSA Decryption

Proposition 1.1 *(Rivest et al., 1978). Suppose $N = pq$ be the RSA modulus and $\phi(N) = (p-1)(q-1)$. If $M \in \mathbb{Z}$ such that M and N are coprime, then $M^{\phi(N)} \equiv 1 \pmod{N}$.*

Proposition 1.2 *(Rivest et al., 1978). Let (N,e) be the public key pair while (N,d) be the respective private key. For $M \in \mathbb{Z}_N^+$ such that M and N are relatively prime and $C \equiv M^e \pmod{N}$. Then $M \equiv C^d \pmod{N}$.*

Proof. Suppose the RSA parameters consists of $N = pq$, $\phi(N) = (p-1)(q-1)$ and $ed \equiv 1 \pmod{\phi(N)}$. Hence, there exists $k \in \mathbb{Z}$ that satisfies $ed = 1 + k\phi(N)$. Thus we have

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(N)} \equiv M \cdot M^{k\phi(N)} \; (\text{mod } = \; N).$$

From Proposition 1.1, it follows that $M \cdot M^{k\phi(N)} \equiv M \pmod{N}$. Since $M < N$, then we have $C^d \equiv M \pmod{N}$. ■

1.5 Problem Statement

Multi-Power RSA $N = p^r q$ is one of the variant of the RSA. It has been implimented in order to make the cryptosystem more secure and more efficient. By using Chinese Remainder Theorem, the execution time for this type of modulus is faster compared to the standard one and thus lessen the cost. However, the exposure of some of the information on either the MSBs or LSBs of the private key might lead to the factorization of modulus N, specifically $N = p^2 q$.

1.6 Research Objective

In this section, we describe briefly the research objectives as follows.

1. To cryptanalyse the modulus $N = p^2 q$. We study the consequence when some of the information on the private key is leaked or exposed. Our attacks are divided into three distinct cases as follows.
   (a) The primes p and q share some known value of LSBs.
   (b) The primes p and q share some known value of LSBs with the existence of e_1, e_2 such that their corresponding multiplicative inverses d_1, d_2 share an amount of MSBs.
   (c) The LSBs of the multiple of the prime factors is known.

   With the information that we have, we form an integer multivariate polynomial. By utilizing Jochemsz-May technique, we find the roots of the polynomial and thus factor the modulus N (Jochemsz and May, 2006).

2. To find the bound of d that insecure from our attack. The implementation of Jochemsz May technique in our theorem may also find the bound of d that insecure from our attack. We find the bound for all of the three attacks and we make a comparison with the bound from the previous attacks.

1.7 Thesis Outline

This thesis consists of seven chapters and is structured as follows.

Chapter 1 is an introductory part to briefly explain the motivation of this research. It covers topics on cryptography, asymmetric encryption, the framework of the RSA cyptosystem, problem statement and objective of this research.

In Chapter 2 provides some crucial information on the previous attacks that we use as reference and instigate us to come out with our research problem.

Chapter 3 covers the methodology of our research. We present useful theorems, lemmas, and basic techniques that are needed throughout this thesis.

In Chapter 4, we describe our first result of our attack on the modulus $N = p^2q$. By considering the case where the primes of the modulus share some known amount of LSBs, we reformulate the lemma from Nitaj et al. (2014), and produce our lemma based on the condition that has been set. By using the strategy of Jochemsz-May technique, we manage to obtain a bound for d that is unsafe through our attack besides manage to prove that the modulus N is factorable based on Assumption 3 in Algorithm 6 . We also make a comparison of bound with some of the previous attacks.

In Chapter 5, we extend the first attack to the case where there exists two public parameters e_1, e_2 such that their corresponding private parameters d_1, d_2 share some amount of MSBs. By utilizing the strategy of Jochemsz-May technique, we obtain a bound for d that is insecure through our attack. Moreover, we also prove that the modulus N can be factored if Assumption 3 in Algorithm 6 is satisfied. We make a comparison of bounds with the previous attacks that also worked on the modulus $N = p^2q$.

In Chapter 6, we propose an attack on the modulus $N = p^2q$. we investigate the case when there exists an integer e that satisfies an equation $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Our attack works when some amount of LSBs of ap and bq is known. We utilize the strategy of Jochemsz-May technique to solve for the roots of the polynomial and thus factor the modulus N provided Assumption 3 in Algorithm 6 is satisfied. We also obtain an unsafe bound for d. We build a table of comparison of bound with some of the former attacks that also work on the modulus $N = p^2q$.

Finally in Chapter 7, we summarize all the contributions of our works and suggestion of 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.

Ariffin, M. R. K., Asbullah, M. A., and Abu, N. A. (2010). A new efficient asymmetric cryptosystem based on the square root problem. *Malaysian Journal Mathematical Sciences*, 10:19–37.

Ariffin, M. R. K. and Rahman, N. A. (2016). New weak finding upon RSA modulo of type $N = p^2q$. *Global Journal of Pure and Applied Mathematics*, 12(4):3159–3185.

Asbullah, M. A. and Ariffin, M. R. K. (2015). New attacks on RSA with modulus $N = p^2q$ using continued fractions. *Journal of Physics: Conference Series*, 622(1):12–19.

Asbullah, M. A. and Ariffin, M. R. K. (2016). Design of Rabin-like cryptosystem without decryption failure. *Malaysian Journal Mathematical Sciences*, 10:1–18.

Bahig, H. M., Nassr, D. I., Bhery, A., and Nitaj, A. (2020). A Unified Method for Private Exponent Attacks on RSA Using Lattices. *International Journal of Foundations of Computer Science*, 31(2):207–231.

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 Transformation Information Theory*, 46(4):1339–1349.

Boneh, D., Durfee, G., and Howgrave-Graham, N. (1999). Factoring $n = p^rq$ for larger r. In *Annual International Cryptology Conference*, pages 326–337. Springer.

Coppersmith, D. (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10:233–260.

Coron, J.-S. (2004). Finding small roots of bivariate integer polynomial equations revisited. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 492–505. Springer.

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

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Transaction on Information Theory*, 31(4):469–472.

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

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

Hoffstein, J., Pipher, J., and Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*, volume 1. Springer.

Howgrave-Graham, N. (1997). Finding small roots of univariate modular equations revisited. pages 131–142. Springer.

Jochemsz, E. and May, A. (2006). A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. pages 267–282. Springer.

Katz, J. and Lindell, Y. (2008). *Introduction To Modern Cryptography: Principles And Protocols.* Chapman And Hall / CRC Press.

Katz, J. and Lindell, Y. (2020). *Introduction to Modern Cryptography*. CRC Press.

Lenstra, A. K., Lenstra, H. W., and Lovasz, H. W. (1982). Factoring polynomials with rational coeffcients. *Mathematische Annalen*, 261:515–534.

Lu, Y., Zhang, R., Peng, L., and Lin, D. (2015). Solving linear equations modulo unknown divisors: revisited. *In International Conference on the Theory and Application of Cryptology and Inormation Security*, pages 189–213.

May, A. (2004). A secret exponent attacks on RSA-typer schemes with moduli $N = p^r q$. *In An International Workshop on Public Key Cryptography*, pages 218–230.

Menezes, A., Oorschot, P., and Vanstone, S. (2018). *Hanbook of applied cryptography*. CRC Press.

Nitaj, A. (2013). An attack on RSA using LSBs of multiples of the prime factors. *In International Conference on Cryptologyin Africa*, pages 297–310.

Nitaj, A., Ariffin, M. R. K., Nassr, D. I., and M., B. H. (2014). New attacks on the RSA cryptosystem. pages 178–198. Springer.

Qiao, G. and Lam, K.-Y. (1998). Rsa signature algorithm for microcontroller implementation. In *International Conference on Smart Card Research and Advanced Applications*, pages 353–356. Springer.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communication of the ACM*, 21(2):120–126.

Sarkar, S. (2014). Small secret exponent attack on RSA varian with modulus $N = p^r q$. *Designs, Codes, and Cryptography*, 73(2):383–392.

Shehu, S. and Ariffin, M. R. K. (2017). New attacks on prime power RSA $N = p^r q$ using good approximation of $\phi(N)$. *Malaysian Journal of Mathematical Sciences*, 11(S):121–138.

Stinson, R. and Peterson, M. (2018). *Cryptography Theory and Practice*. CRC Press.

Takagi, T. (2004). A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting. *IEICE Transactions on fundamentals of electronics, communications and computer sciences*, 87(1):94–101.

Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. *Journal IEEE Transactions on Information theory*, 36(3):553–558.

BIODATA OF STUDENT

Nurul Nur Hanisah binti Adenan was born in August 1993. Started her primary school at Sekolah Kebangsaan Sungai Lalang, she then continued her secondary school in Sekolah Menengah Kebangsaan Ibrahim. She pursued her next stage of study in Foundation of Science at Universiti Teknologi Mara. After graduating her degree in Bachelor Science(Hons) Major Mathematics from Universiti Putra Malaysia in 2016, she then pursued her Master of Science in Cryptography in Universiti Putra Malaysia. Her research field is in cryptanalysis on asymmetric cryptography specifically on the RSA cryptosystem.

The student can be reached through her supervisor,

Prof. Dr. Muhammad Rezal Kamel Ariffin
Institute for Mathematical Research
Email : rezal@upm.edu.my
Tel : +03-97696838

or through her email, hanisahadenan@gmail.com.my.

LIST OF PUBLICATIONS

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

Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin, Faridah Yunos, Siti Hasana Sapar, and Muhammad Asyraf Asbullah. (2021). Analytical Cryptanalysis Upon $N = p^2q$ Utilizing Jochemsz-May Strategy. *PLoS ONE*, 16(3), Article ID: e024888.

Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin, Siti Hasana Sapar, Amir Hamzah Abd Ghafar and Muhammad Asyraf Asbullah. (2021). New Jochemsz-May Cryptanalytic Bound For RSA System Utilizing Common Modulus $N = p^2q$. *Mathematics*, 9(4), 340.

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, Amir Hamzah Abd Ghafar, Wan Nur Aqlili Wan Mohd 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.

Abderahmanne Nitaj, Muhammad Rezal Kamel Ariffin, **Nurul Nur Hanisah Adenan**, Domenica Stefania Merenda and Ali Ahmadian. (2021). Exponential Increment of RSA Attack Range via Lattice Based Cryptanalysis, *Journal of Multimedia Tools and Applications*, (Accepted for Publication).

Abderahmanne Nitaj, Muhammad Rezal Kamel Ariffin, **Nurul Nur Hanisah Adenan** and Nur Azman Abu. (2021). Classical Attacks on a Variant of the RSA Cryptosystem, *In Proceeding of Seventh International Conference on Cryptology and Information Security in Latin America*, (Accepted for publication)

Abderahmanne Nitaj, Muhammad Rezal Kamel Ariffin, **Nurul Nur Hanisah Adenan** and Nur Azman Abu. (2021). Small Prime Difference Attack on a Cubic Pell Variant of RSA, *Cryptography and Communications*, (Submitted)

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : SECOND SEMESTER 2020/2021

TITLE OF THESIS / PROJECT REPORT :
EXTENDING JOCHEMSZ-MAY ANALYTICAL STRATEGIES UPON INTEGER FACTORIZATION PROBLEM

NAME OF STUDENT : NURUL NUR HANISAH BINTI ADENAN

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.]