UNIVERSITI PUTRA MALAYSIA

FACTORIZATION STRATEGIES OF N = pq AND N = p^rq AND RELATION TO ITS DECRYPTION EXPONENT BOUND

SAIDU ISAH ABUBAKAR

FS 2019 36

FACTORIZATION STRATEGIES OF $N = pq$ AND $N = p^r q$ AND RELATION TO ITS DECRYPTION EXPONENT BOUND

By

SAIDU ISAH ABUBAKAR

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

December 2018

DEDICATIONS

This research work is dedicated to the memory of my late brother Ibrahim Isah. May his gentle soul rest in peace.

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

FACTORIZATION STRATEGIES OF $N = pq$ AND $N = p^r q$ AND RELATION TO ITS DECRYPTION EXPONENT BOUND

By

SAIDU ISAH ABUBAKAR

December 2018

Chair: Associate Professor Muhammad Rezal Kamel Ariffin, PhD
Faculty: Science

The major RSA underlying security problems rely on the difficulty of factoring a very large composite integer N into its two nontrivial prime factors of p and q in polynomial time, the ability to solve a given Diophantine equation $ed = 1 + k\phi(N)$ where only the public key e is known and the parameters d, k and $\phi(N)$ are unknown and finally the failure of an adversary to compute the decryption key d from the public key pair (e,N). This thesis develops three new strategies for the factorization of RSA modulus $N = pq$ through analyzing small prime difference satisfying inequalities $|b^2 p - a^2 q| < N^\gamma$, $|b^i p - a^j q| < N^\gamma$ and $|b^j p - a^j q| < N^\gamma$ for $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$ which yield susceptible decryption exponent bounds of $d < \frac{\sqrt{3}}{\sqrt{2}} N^{\frac{3}{4}-\gamma}$, $d < \sqrt{\frac{a^j + b^i(b^i-2)}{2b^i}} N^{\frac{3}{4}-\gamma}$ and $d < \sqrt{\frac{a^j(b^{2j}-2)}{2b^j}} N^{\frac{3}{4}-\gamma}$ by taking the convergents of the continued fraction expansions of $\frac{e}{N - \lceil \frac{a^2+b^2}{ab} \sqrt{N} \rceil + 1}$, $\frac{e}{N - \lceil \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}} \sqrt{N} \rceil + 1}$ and $\frac{e}{N - \lceil \frac{a^j+b^j}{(ab)^{\frac{j}{2}}} \sqrt{N} \rceil + 1}$ respectively for $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$. It also reports a cryptanalysis attack via approximation of $\phi(N)$ given by $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil] + 1$ that leads to the break of modulus $N = pq$ with a decryption exponent bound $d < \sqrt{\frac{a^{i+1}+b^i}{2}} (\frac{N}{e})^{\frac{1}{2}} N^{0.375}$ found from the convergents of the continued fraction expansion of $\frac{e}{N*}$ where $N^* = N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$, for $i = 3, \ldots, j$.

This research work also focuses on successful factorization of t RSA moduli $N_s = p_s q_s$. By using good approximation of $\phi(N)$ and generalized key equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1,2,\ldots,t$. This method leads to simultaneous factoring of t RSA moduli $N_s = p_s q_s$ in polynomial time using simultaneous Diophantine approximation and lattice basis reduction techniques for unknown integers d, d_s, k, k_s, and z_s.

The thesis presents new cryptanalysis attack of factoring prime power modulus $N_s = p_s^r q_s$ for $r \geq 2$ in polynomial by taking the convergents of the continued fraction expansion of $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ which gives decryption exponent bound $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$.

Furthermore, this research work develops four successful cryptanalysis attacks of factoring t prime power moduli $N_s = p_s^r q_s$ by transforming equations $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1,2,\ldots,t$ into simultaneous Diophantine problem by using LLL algorithm to get the reduced basis (d, k_s) and (d_s, k) which can be used to calculate unknown parameters $\phi(N)$ and later simultaneously factor (p_s, q_s) in polynomial time. This research work also makes comparisons of its findings with existing literature. The bound of this research work was found to be better than the short decryption exponent bound within some of the existing literature.

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

KEJAYAAN BARU STRATEGI PEMFAKTORAN BAGI $N = pq$ DAN $N = p^r q$ DAN HUBUNGAN KEPADA BATAS EKSPONEN PENYAHSULITANNYA

Oleh

SAIDU ISAH ABUBAKAR

Disember 2018

Pengerusi: Profesor Madya Muhammad Rezal Kamel Ariffin, PhD
Fakulti: Sains

Asas keselamatan RSA yang utama bergantung kepada kepayahan memfaktorkan nombor gubahan N yang sangat besar kepada dua faktor perdananya iaitu p dan q dalam masa polinomial, keupayaan untuk menyelesaikan persamaan Diophantine yang diberikan $ed = 1 + k\phi(N)$ di mana hanya kekunci awam e diketahui dan parameter d, k dan $\phi(N)$ tidak diketahui dan akhirnya kegagalan pihak lawan untuk menghitung kekunci penyahsulitan d daripada pasangan kekunci awam (e,N). Tesis ini membangunkan tiga strategi baharu untuk memfaktorkan modulus RSA $N = pq$ dengan menganalisis perbezaan kecil nombor perdana yang memenuhi ketaksamaan $|b^2p - a^2q| < N^\gamma$, $|b^ip - a^jq| < N^\gamma$ dan $|b^jp - a^jq| < N^\gamma$ dimana $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$ yang menghasilkan eksponen penyahsulitan rentan yang dibatasi $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, $d < \sqrt{\frac{a^j+b^i(b^i-2)}{2b^i}}N^{\frac{3}{4}-\gamma}$ dan $d < \sqrt{\frac{a^j(b^{2j}-2)}{2b^j}}N^{\frac{3}{4}-\gamma}$ dengan mengambil penumpuan daripada pengembangan pecahan berselanjar oleh $\frac{e}{N-\lceil\frac{a^2+b^2}{ab}\sqrt{N}\rceil+1}$, $\frac{e}{N-\lceil\frac{a^j+b^i}{a^{\frac{j}{2}}b^{\frac{i}{2}}}\sqrt{N}\rceil+1}$ dan $\frac{e}{N-\lceil\frac{a^j+b^j}{(ab)^{\frac{j}{2}}}\sqrt{N}\rceil+1}$ masing-masing dimana $\frac{1}{4} \leq \gamma \leq \frac{1}{2}$. Ia juga melaporkan serangan analisis-kripto melalui penghampiran $\phi(N)$ yang diberikan oleh $N - \left\lceil \left(\frac{a^{\frac{i+1}{i}}+b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}}+b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}}\right)\sqrt{N}\right\rceil] + 1$ yang membawa kepada pemfaktoran modulus $N = pq$ dengan batasan eksponen penyahsulitan $d < \sqrt{\frac{a^{i+1}+b^i}{2}}(\frac{N}{e})^{\frac{1}{2}}N^{0.375}$yang ditemui dari penumpuan pengembangan pecahan berselanjar $\frac{e}{N*}$ dimana $N^* = N - \left\lceil \left(\frac{a^{\frac{i+1}{i}}+b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}}+b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}}\right)\sqrt{N}\right\rceil + 1$, untuk

$i = 3, \ldots, j$.

Kajian ini juga memberi tumpuan kepada kejayaan pemfaktoran terhadap t modulus-modulus RSA $N_s = p_s q_s$. Melalui penggunaan anggaran $\phi(N)$ yang terhampir dari persamaan kekunci umum dalam bentuk $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ dan $e_s d_s - k\phi(N_s) = z_s$ untuk $s = 1, 2, \ldots, t$. Kaedah-kaedah tersebut membawa kepada pemfaktoran secara serentak t modulus-modulus RSA t dalam masa polinomial menggunakan teknik penghampiran serentak Diophantus dan teknik penurunan asas kekisi untuk integer anu d, d_s, k, k_s, dan z_s.

Tesis ini persembahkan serangan analisis-kripto baharu terhadap pemfaktoran modulus $N_s = p_s^r q_s$ untuk perdana berkuasa $r \geq 2$ dalam masa polinomial melalui perhitungan penumpuan pengembangan berselanjar $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ yang memberikan eksponen penyahsulitan dibatasi $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$. Seterusnya, kajian ini membangunkan empat serangan analisis-kripto yang berjaya memfaktorkan t moduli $N_s = p_s^r q_s$ dengan mengubah persamaan $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k\phi(N_s) = z_s$ dan $e_s d_s - k\phi(N_s) = z_s$ untuk $s = 1, 2, \ldots, t$ kepada masalah persamaan serentak Diophantus dengan menggunakan algoritma LLL untuk mendapatkan penurunan asas kekisi (d, k_s) dan (d_s, k) yang boleh digunakan untuk mengira parameter anu $\phi(N)$ dan seterusnya memfaktorkan (p_s, q_s) secara serentak dalam masa polinomial. Kajian ini juga membuat perbandingan diantara penemuannya dengan kesusasteraan yang sedia ada. Batas eksponen penyahsulitan yang terhasil dari kajian ini didapati lebih baik daripada batas eksponen pendek penyahsulitan dalam kesusasteraan sedia ada.

ACKNOWLEDGEMENTS

All the praises and thanks be to Allah, the Lord of the 'Alamin (mankind, jinns and all that exists) who gave me the courage, wisdom, ability, strength and health to witness and accomplished this hard earned degree. My sincere appreciation goes to Associate Professor Dr. Muhammad Rezal Kamel Ariffin who chaired my supervisory committee for taking the pains to go through the manuscripts of this thesis despite his numerous/tight academics and administrative schedules, his guidance, constructive criticisms and helpful suggestions make this research work a successful one. I pray to Allah (S.W.T) to grants him his heart desires as words are too small to pay for his immense contributions in this journey. I also want to extend my gratitudes to members of the supervisory committee in persons of Dr. Faridah Yunos for her valuable advice and useful suggestion and Dr. Muhammad Asyraf Asbullah whose inputs in improving the quality of this research work can not be denied. In fact, he nurtured me into the area during my first year of research. May your dreams be fulfilled .

I would like to extend my appreciations to my parents for their support, encouragements and prayers. Also worthy to mention are my brothers and sisters in persons of Murtala Isah, Bello Isah Abubakar, Nura Bello Abubakar, Abubakar Isah, Naziru Bello, Aminu Bello Danjariri, Hajiya Rukayya, Amina Isah, Safiya Bello, Saratu Isah and many whose names are not mentioned who always remember me in their prayers and make calls to hear from me.

I have been very fortunate to meet and associate with friends in persons of Amir Hamzah Abd Ghafar, Zahari Mahad, Tea Boon Chian, Wan Nur Aqlili Wan Muhd Ruzai, Nurul Nur Hanisah Adenan and Muhammad Rasyid Redha Mohd Tahir . Thank you all for been friendly and your contributions during our Crypto-Discussions are appreciated.

Next, I would like to thank my employer Sokoto State University for given me this chance to further my study and also the Tertiary Eduction Trust Fund (TetFund) for providing grants throughout the period of the programme . I really appreciate your support and encouragement.

My gratitudes also goes to friends like Murtala Suleiman, Usman Aliyu Musa, Dr. Sadiq Shehu, my childhood friends and the entire Sokoto State University community for their supports and prayers.

Finally, special thank you goes to Hauwa'u Bashir Sada and her son Urwatu for been my partners and my best friends throughout the period of my study in Malaysia. I thank her for all the love and support and perhaps most importantly the patience she has always shown me. May Allah rewards all those who contributed in one way or the other toward making this work a successful one.

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

Muhammad Rezal Kamel Ariffin, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

Faridah bt. Yunos, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

Muhammad Asyraf Asbullah, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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: Saidu Isah Abubakar, GS 46378

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
Associate Professor Dr. Muhammad Rezal Kamel Ariffin

Signature: ______________________________
Name of Member of Supervisory Committee
Dr. Faridah bt. Yunos

Signature: ______________________________
Name of Member of Supervisory Committee
Dr. Muhammad Asyraf Asbullah

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

p	prime number
$\mathbb{Z}$	Set of integers
$\mathbb{R}$	Set of real numbers
$\mathbb{Q}$	Set of rational numbers
Min	Minimum
Max	Maximum
mod	Modulo
gcd	Greatest Common Divisor
LCM	Lowest Common Multiple
IFP	Integer Factorization Problem
LLL	Lenstra-Lenstra-Lovasz
RSA	Rivest-Shamir-Adleman
CRT	Chinese Remainder Theorem
DLP	Discrete Logarithm Problem
MSBs	Most Significant Bits

CHAPTER 1

INTRODUCTION

1.1 Cryptography

The importance of keeping information secret except to those who are authorized to have access to it cannot be overemphasized especially as information becomes an increasingly valuable commodity, and as communication revolution changes our society. The process of encoding messages, known as encryption will continue to play an increasing role in our everyday life. Nowadays, our phone calls bounce off satellites and our emails pass through computers and networks and both forms of communications can be intercepted with ease by unauthorized parties also known as an eavesdropper. Hence, jeopardizing our privacy. Similarly, as more and more business transactions are conducted over the internet, measures must be in place to protect companies and clients from eavesdroppers. The only way to ensure privacy of our communication is through encryption. The art of secret writing known as cryptography, will provide the locks and keys of the information age, as reported by Singh (2000).

Cryptography can also be considered as a science that applies complex mathematics and logic to design strong encryption schemes. The rapid increase of information transmitted through electronic means and need to provide security for these communications make cryptography an inevitable discipline in today's world. Cryptography is also considered to be the study of mathematical systems of solving two kind of security problems: privacy and authentication. A privacy system prevents the extraction of information by unauthorized parties from the message transmitted over a public channel, thus assuring the sender of the message that, it will only being access and read by the trusted party (intended recipient). An authentication system prevents the alteration of a message by insertion or deletion of a message into a public channel, assuring the receiver of the message of the legitimacy of its sender.

Basically, there are four goals of cryptography. These include: confidentiality/privacy, data integrity, authentication and non-repudiation. We will briefly discuss them as follows:

1. Confidentiality/Privacy: This is one of the goals of cryptography that refers to the process of keeping the content of information secret from all except those who are authorized to see/have it. Confidentiality denies an adversary access to information and ensures that only intended parties have access to the information. There are numerous approaches to providing privacy in communication channels ranging from physical protection of the content to design of mathematical algorithms which render data incomprehensible. One of the goals of Cryptography is

to ensure confidentiality in communications between entities which is considered as the central issue in the field of information security.

2. Data Integrity: This refers to the ability of the designed system to prevents data modification by an adversary and detect data manipulations by unauthorized parties in the communication channels. To ensure data integrity, one must be able to detect data manipulation which includes such thing as insertion, deletion and substitution.

3. Authentication: This can also be viewed as identification of parties and information involved in the communication. Entities entering into a communication should be able to identify each other and information transfered over a communication channel should be authenticated as to the origin, data content, time sent, etc.

4. Non-repudiation: This is a service which prevents an entity from denying previous commitments or actions. For instance, whenever disagreements arise when an entity denies being involve in a certain action, the need to resolve such controversies is necessary. The disputes can be resolved by engaging a trusted third party.

1.2 Cryptanalysis

Cryptanalysis can be defined as the science of revealing/knowing the content of a message by an adversary without the full knowledge of the key(s) involved in encrypting a message. Cryptanalysis can also be viewed as the study of ciphertexts, ciphers and cryptosystems with the sole aim of understanding how they work and finding their weaknesses that will render them insecure which can be achieved through the use of mathematical formulas to search for algorithms vulnerabilities. One of the main goal/motive of a cryptanalyst is to identify weaknesses or threats within cryptosystems. Professional cryptanalysts perform an important role in evaluating and validating the weaknesses of cryptosystems and any cryptosystem that withstand significant cryptanalysis is considered to be a secure system. Cryptanalysts also have many ways, procedures, techniques and in fact can use strong and powerful computing machines to mount a successful attack against the cryptosystems.

Some of the major types of cryptanalysis attacks can be categorized as follows:

1. Ciphertext Only Attack: This is a cryptanalytic attack in which the cryptanalyst has access to only encrypted message. The cryptanalyst does not know anything about the contents of the message and must work from known ciphertext collections only to mount an attack.

2. Known Plaintext Attack: This is a type of attack in which the cryptanalyst has some knowledge about the plaintext and its corresponding ciphertext which enables him to decrypt the encrypted message.

3. Chosen Plaintext Attack: This is another type of attack in which the attacker has access to both the ciphertext and its corresponding plaintext and can also select the plaintext to be encrypted.

4. Chosen Ciphertext Attack: In this type of attacks, the cryptanalyst can select different ciphertexts to be decrypted and also has access to the decrypted plaintext. This type of attack is generally applicable to attacks against public key cryptosystems.

5. Adaptive Chosen-Plaintext Attack: This is another cryptanalytic attack whereby the cryptanalyst has access to both the plaintext and its corresponding encryption and can also ammends the plaintext to suit his need in connection with the results of the previous encryptions.

6. Man-in-the-Middle Attack: This is a cryptanalytic attack which involves two parties communicating in a channel which is seems to be secured by the parties but it is being hijacked by an adversary by intercepting any message that passes through the channel and performs key exchanges with the trusted parties via the same channel which enables him to get access to the proper key that will lead to decryption of the encrypted message. The parties think that they are communicating via a secure channel without knowing that an adversary is reading their conversations.

7. Brute Force Attack: This is another attack in which an attacker keeps on testing all possible keys until he finds the correct one which reveals the expected plaintext. This type of attack is time-consuming.

Definition 1.1 (Cryptology) *Cryptology can be viewed as a broad term that encompasses both cryptography and cryptanalysis. It is the scientific study of cryptography and cryptanalysis. Cryptology can be defined as a branch of mathematics that focused on the practice of protecting sensitive information from an adversary by using mathematically intractable problems. Researcher who is involve in developing new ciphers and devising techniques of breaking others is considered to be cryptologist.*

1.3 Public Key Cryptography

A public-key cryptography is a cryptosystem that was first used/developed by Diffie and Hellman (1976), in order to provide a solution to the problem of key distributions which is considered to be the major drawback in symmetric encryption. The development of public key cryptography is considered to be the greatest and perhaps the only true revolution in the entire history of cryptography, Diffie and Hellman (1976). A public key encryption uses two different keys known as public and private keys in which a public key is used for encrypting messages while the private key is used for decrypting messages. The public key is always publish for public consumption while the private key is kept secret.

Definition 1.2 (Public-Key Cryptography) *(Hinek, 2009) A public-key cryptosystem can be defined as a five-tuple* $(\mathbb{P}, \mathbb{C}, \mathbb{K}, \mathbb{E}, \mathbb{D})$, *satisfying the following seven conditions:*

1. $\mathbb{P}$ *is a finite set of possible plaintexts.*
2. $\mathbb{C}$ *is a finite set of possible ciphertexts.*
3. $\mathbb{K}$ *is a finite set of possible keys.* $\mathbb{K}$ *is called the keyspace.*
4. *For each key in the keyspace* $\mathbb{K} \in \mathbb{K}$, *there is an encryption rule* $enc_K \in E$ *and a corresponding decryption rule* $dec_K \in D$. *Each* $enc_K : P \to C$ *and* $dec_K : C \to P$ *are functions such that* $dec_K(enc_K(m)) = m$ *for every plaintext* $m \in P$.
5. *For each key* $K \in K$ *and each plaintext* $m \in P$, *both* $enc_K(m)$ *and* $dec_K(enc_K(m))$ *are easy to compute.*
6. *For almost every key* $K \in K$, *each easily computable algorithm equivalent to* dec_K *is computationally infeasible to derive from* enc_K . *That is, it is difficult to decrypt without* dec_K .
7. *The encryption rule* enc_K *is made public and the decryption rule* dec_K *is kept private.*

A public-key cryptosystem can also be viewed as a cryptosystem that is made up of three efficiently computable algorithms: a key generation algorithm, an encryption algorithm, and a decryption algorithm. Here, the key generation algorithm defines the key space $\mathbb{K}$ and the encryption and decryption algorithms define the plaintext and ciphertext spaces $\mathbb{P}$ and $\mathbb{C}$ respectively.
The public key encryption plays an important role in information security by providing essential services such as confidentiality (privacy) and authentication of entities involved in communication channels which can be achieved through the use of digital signatures. The security of public key cryptosystems depend largely on the hardness (difficulty) of certain computational problems in mathematics and solving those computational problems require a substantial knowledge in areas of algebra, number theory and geometry.

1.4 Complexity Theory

In this section, we give brief definitions of some terms that will be used in this research which are related to computational problems.

Definition 1.3 *(Complexity Theory) This can be viewed as a branch of mathematics and theoretical computer science that is aimed at classifying computational problems which can theoretically be solved by computers in terms of their practical difficulties involved in finding their solutions. The most important resources to be considered by* *most computers while dealing with a computational problem is the time and space needed by an algorithm in running the given problem. The computational problem is specified by an input (of a certain form) and an output satisfying certain properties relative to input. An instance of a computational problem refers to a specific input and the number of bits required to represent an instance is termed as input size whereas the number of bits necessary to represent the output is known as outputsize. For more details see Galbraith (2012), Talbot and Welsh (2006).*

Definition 1.4 *(Algorithm) An algorithm can be defined as a well-defined step by step procedures that takes a variable input and terminates with an output. It can also be seen as a sequence of bit operations. The running time of an algorithm is the number of bit operations or step executed and it is usually measured in terms of the number of basic operations performed. The running of an algorithm will normally depends on the size of the input. An algorithm to solve a computational problem is called deterministic if it does not make use of any randomness. A deterministic algorithm should terminate after a finite number of steps. In cryptography, it is a tradition to consider an algorithm whose running time is bounded (typically by a polynomial in the input size).*

Definition 1.5 *(Asymptotic Complexity) The asymptotic complexity of a deterministic algorithm refers to the process of counting the number of bit operations performed by the algorithm expressed as the function of the input size. Upper bound on the complexity are represented using the "big O " notation. When giving complexity estimates using big O notation we implicitly assume that there is a countably infinite number of possible input to the algorithm.*

Definition 1.6 *(Worst-Case) The worst-case running time of an algorithm refers to the upper bound of the running time for any input, expressed as a function of the input size.*

Definition 1.7 *Let $h_1, h_2 : \mathbb{N} \to \mathbb{R}_{>0}$. Write $h_1 = O(h_2)$ if there are $c \in \mathbb{R}_{>0}$ and $N \in \mathbb{N}$ such that*

$$h_1(n) \leq ch_2(n)$$

for all $n \geq N$ where $\mathbb{R}_{>0}$ denotes set of positive real numbers.

Definition 1.8 *Let $h_1, h_2 : \mathbb{N} \to \mathbb{R}_{>0}$. Write $h_1 = o(h_2)$ if*

$$\lim_{n\to\infty} \frac{h_1(n)}{h_2(n)} = 0$$

Definition 1.9 *(Order notations) It is always difficult to derive the exact running time of an algorithm. In such situation, one is allowed to use approximations of the running time, and usually may only derive the asymptotic running time. That is, one studies how the running time of an algorithm increases as the size of the input increases without bound.*

1. *Asymptotic upper bound $f(n) = O(g(n))$ if there exists a positive constant c and a positive integer n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.*

2. *Asymptotic lower bound $f(n) = \Omega(g(n))$ if there exists a positive constant c and a positive integer n_0 such that $0 \leq cg(n) \leq f(n)$ for all $n \geq n_0$.*

3. *Asymptotic tight bound $f(n) = \Theta(g(n))$ if there exists a positive constants c_1 and c_2 and a positive integer n_0 such that $c_1 g(n) \leq f(n) \leq c_2 g(n)$ for all $n \geq n_0$.*

4. *$(o-notation)$ $f(n) = o(g(n))$ if for any given positive constant $c > 0$ there exists a constant $n_0 > 0$ such that $0 \leq f(n) < cg(n)$ for all $n \geq n_0$. For more details on complexity theory see Galbraith (2012), Menezes and Vanstone (2001), and Talbot and Welsh (2006).*

Definition 1.10 *(Worst case asymptotic complexity) Let A be a deterministic algorithm and let $t(n)$ be a bound on the running time of A on every problem of input size n bits. Then the following holds*

1. *A is polynomial-time if there exists an integer k such that*

$$t(n) = O(n^k).$$

2. *A is superpolynomial-time if $t(n) = \sigma(n^c)$ for all $c \in \mathbb{R}_{>1}$.*

3. *A is exponential-time if there is a constant $c_1 > 1$ such that*

$$t(n) = O(c_1^n).$$

4. *A is subexponential-time if $t(n) = O(c^n)$ for all $c \in \mathbb{R}_{>1}$.*

Definition 1.11 *(One-Way Function) A function $g : \{0,1\}^* \to \{0,1\}^*$ is called a one-way function if it satisfies the following two conditions:*

1. *Easy to compute: There exists a (deterministic) polynomial-time algorithm A such that on input x algorithm A output $g(x)$ (i.e;$A(x) = g(x)$);*

2. *Hard to invert: For every probabilistic polynomial-time algorithm A', every positive polynomial $p(\cdot)$ and all sufficiently large n'*

$$pr[A'(g(U_n), 1^n) \in g^{-1}(g(U_n))] < \frac{1}{p(n)}.$$

where U_n denotes a random variable uniformly distributed over $\{0,1\}^n$. Hence, the probability in the second condition is taken over all the possible internal coin tosses of A', with uniform probability distribution.

It should be noted that, one does not require A' to output a specific pre-image $f(x)$; any element in the set $f^{-1}(f(x))$ will do. In situation where f is one-to-one, the string x is the only pre-image of $f(x)$ under f, but in general there may be other pre-images. For more details on one-way function see Oded (2001).

Definition 1.12 *(Trapdoor One-way Function) A trapdoor one-way function also refers to collections of those functions that can be computed easily in a forward direction but it is hard to find their inverses except with some secret information. Mathematically, a trapdoor one-way function is a family of invertible functions f_k, such that*

1. *$y = f_k(x)$ easy to compute if k and x are known.*
2. *$x = f_k^{-1}(y)$ easy to compute if k and y are known.*
3. *$x = f_k^{-1}(y)$ infeasible to compute if y are known but k is not known.*

Thus, the development of a practical public-key scheme depends largely on discovery of a suitable trapdoor one-way function, Stallings (2005). Most of the public-key cryptosystems hardness are considered to be trapdoor-one-way function; for examples discrete log problem, integer factorization problem, etc.

1.5 Primality Testing

Prime numbers has many applications in today's world as it has been used in setting up some parameters of certain cryptographic protocols. This makes prime numbers to have more applications in public key cryptography. Primality testing refers to the procedures and techniques adopted in order to determine whether a given random number (large) is a prime or not. There are many algorithms for primality testing, but in this section, we will give two probabilistic algorithms for primality testing which are: Solovay-Strassen algorithm and Rabin-Miller algorithm. Before discussing these algorithms in details, we give the following definitions:

Definition 1.13 (Legendre Symbol) *Let p be an odd prime and x be an integer such that the $\gcd(x,p) = 1$. Then the Legendre symbol, $\left(\frac{x}{p}\right)$, is defined by*

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \textit{if } x \textit{ is a quadratic residue} \bmod p \\ -1, & \textit{if } x \textit{ is a quadratic non–residue} \bmod p \end{cases}$$

Definition 1.14 (Jacobi Symbol) *Let x be an integer and $n > 1$ be an odd positive integer. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots, p_k^{\alpha_k}$, then the Jacobi symbol, $\left(\frac{x}{n}\right)$, is defined by*

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)^{\alpha_1} \left(\frac{x}{p_2}\right)^{\alpha_2} \cdots \left(\frac{x}{p_k}\right)^{\alpha_k}$$

where $\left(\frac{x}{p_i}\right)$ *for* $i = 1,2,\ldots,k$ *is the Legendre symbol for the odd prime* p_i*. The Jacobi symbol turns to Legendre symbol if n is an odd prime instead of an odd positive integer.*

Both Legendre and Jacobi symbols have certain properties. More details can be found in Song (2002), Wang et al. (2016).

1.5.1 Solovay-Strassen Algorithm

This is one of the probabilistic algorithms for primality testing that uses Jacobi function in testing whether or not a given random number p is prime. The method has the following steps:

Algorithm 1.1 Solovay-Strassen algorithm

```
Randomly select a number $x$ that is less than $p$.
Compute the greatest common divisor (gcd) of $x$ and $p$. If gcd $(x,p) \neq 1$, then $p$ must be a composite number and the test fails. Return "$p$ is a composite number."
Compute $j = x^{\frac{p-1}{2}} \pmod{p}$.
Compute the Jacobi symbol $\left(\frac{x}{p}\right)$.
If $j \neq \left(\frac{x}{p}\right)$, then $p$ is not a prime number and $p$ is prime if $j = \left(\frac{x}{p}\right)$
If $p$ passes the test, randomly select another $x$ and repeat steps $1-5$, if $p$ passes all the test $t$ times, then the largest probability that $p$ is a composite is $\frac{1}{2^t}$ where the number $t$ can be determined based on the security requirements.
```

1.5.2 Rabin-Miller algorithm

This is also another probabilistic algorithm which is considered to be simple and also widely used algorithm for primality testing. Firstly, let p be the number to be examined, then we compute a positive integer k and an odd integer m such that $p = 2^k m$. Then perform the following steps:

Algorithm 1.2 Rabin-Miller algorithm

```
Randomly select a number $c < p$.
Initialize the number of steps$j = 0$ and let $z \equiv c^m \pmod{p}$.
If $z = 1$ or $z = p-1$, then $p$ is probably a prime, and passes the test.
Increase the variable of number of steps by one, if $j < k$ and $z \neq p-1$, set $z \longrightarrow z^2$.
If $z = 1$, then $p$ is not a prime. If $z = p-1$, then $p$ is a probable prime, otherwise repeat step 4.
If $j = k$ and $z \neq p-1$, then $p$ is not a prime
[Exit] Terminate the algorithm.
```

1.6 Integer Factorization Problem (IFP)

Integer Factorization Problem (IFP) started during ancient Greece and many algorithms were developed as a result of the advent of computers which can factor very large numbers into their prime factors. It can also be defined as given a large positive integer N, then its prime factorization can be written as $N = p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$ where p_i are defined to be pairwise distinct primes and each $a_i \geq 1$. This means in another way, integer factorization problem refers to the study of algorithms that split a composite number N into a non-trivial prime factors say a and b such that $N = ab$. The integer factorization problem plays a significant role in modern communication as the security of many cryptographic protocols such as RSA public-key, encryption, RSA digital signature scheme and the Rabin public key encryption rely on the intractability of integer factorization problem. This means if someone can find two prime factors of a very large composite integer N in polynomial time, then this implies that any design cryptosystem whose intractability relies on integer factorization problem is consider to be insecure.

There are many methods and algorithms developed for factoring very large composite integers N ranging from classical methods of trial division, Pollard ρ to modern factoring algorithms of quadratic sieve, elliptic curve method and number field sieve but there is no known deterministic polynomial-time algorithm for integer factorization problem. This section will discuss briefly some of these factoring methods and their algorithms where necessary. For more details on integer factorization methods see Cohen (1996), Song (2002) and Hoffstein et al. (2008).

1.6.1 Trial Division Method

This is consider to be one of the oldest factoring method that brute force a given composite integer into its prime factors by keeps on dividing with small primes up to the square root of the given composite integer. This simply means given a composite integer N, trying small primes $p_1, p_2, \ldots, p_k$ where $p_k \approx \sqrt{N}$, if a prime p_k is found to divide N, then it leads to factorization of the integer N. To test for every integer less than $\lfloor N \rfloor$ is of time complexity $O(\sqrt{N}) = O(2^{N/2})$ which is exponential time. The complexity time of division is $O(N^2)$. Hence, the complexity time of trial division is $O(N^2 2^{N/2}) = O(N^2\sqrt{N})$ Hoffstein et al. (2008). In what follows, we present an algorithm that tries to factor an integer $N > 1$ using trial division by all possible divisors of N.

Algorithm 1.3 Trial Division Method of factoring a composite integer $N > 1$

```
1: [Initialization] Input $N$ and set $a \leftarrow 0, \quad b \leftarrow 2$.
2: [$N = 1$?] If $N = 1$, then go to step 5.
3: [Compute remainder] $q \leftarrow \frac{N}{b}$ and $r \leftarrow N \pmod{b}$. If $r \neq 0$, go to step 4. $a = a+1, p_a \leftarrow b, N \leftarrow q$, go to step 2.
4: [Factor found?] If $q > b$, $\quad$ *then* $\quad b \leftarrow b+1$, go to step 3
5: $a \leftarrow a+1; p_a \leftarrow N$
6: [Exit] Terminate the algorithm.
```

1.6.2 Pollard's ρ Factoring Method

Pollard's ρ method was introduced in 1975 by John M. Pollard which is aimed at finding a relatively small factors of an integer N, Pollard (1975). The method uses an iteration of the form

$$x_o = \text{random } (0, N-1),$$
$$x_i \equiv f(x_{i-1}) \pmod N$$

where x_0 is a random starting value, N is the number to be factored, and $f \in \mathbb{Z}[x]$ is a polynomial with integer coefficients, usually is chosen to be $f(x) = x^2 \pm a$ with $a \neq -2, 0$. Then starting from some initial value x_0, a random sequence $x_1, x_2, \ldots$ is computed modulo N as follows:

$$\begin{array}{rcl} x_1 & = & f(x_0), \\ x_2 & = & f(f(x_0)) = f(x_1), \\ & \vdots & \\ x_i & = & f(f(_{i-1})). \end{array}$$

Let d be nontrivial divisor N such that d is smaller than N. Since there are relatively few congruent classes modulo d (namely, d of them) , probably, there exists some integers x_i and x_j that lie in the same congruence class with modulo d but belong to different class modulo N which can be written as follows:

$$x_i \equiv x_j \pmod d$$
$$x_i \not\equiv x_j \pmod N$$

Since $d \mid (x_i - x_j)$ and $N \nmid (x_i - x_j)$, then it follows that the gcd $(x_i - x_j, N)$ is a nontrivial factor of N. The possibility exists that when a gcd greater than 1 is obtained, it may turn out also to be equal to N but this happens in a very rare case. The complexity of the algorithm has an expected running time of $O(p^{1/2}(\log N)^2)$. In what follows, we present the Pollard's ρ algorithm of factoring an integer $N > 1$ and using a polynomial $f(x) = x^2 + 1$ as presented by Song (2002).

Algorithm 1.4 Pollard's ρ Method of factoring a composite integer $N > 1$

```
1: [Initialization] Choose a seed, $x_0 = 2$, a generating function $f(x) = x^2 + 1 \pmod{N}$. Choose also a value for $t$ not much bigger than $\sqrt{d}$, perhaps $t < 100\sqrt{d}$
2: [Iteration and computation] Compute $x_i$ and $y_i$ as follows
       $x_1 = f(x_0),$
       $x_2 = f(f(x_0)) = f(x_1),$
       $\vdots$
       $x_i = f(f(_{i-1})).$

       $y_1 = x_2 = f(x_1) = f(f(x_0)) = f(f(y_0))$
       $y_2 = x_4 = f(x_3) = f(f(x_2)) = f(f(y_1)),$
       $y_3 = x_6 = f(x_6) = f(f(x_3)) = f(f(y_2))$
       $\vdots$
       $y_i = x_{2i} = f(f(y_{i-1})).$
   and simultaneously compare $x_i$ and $y_i$ by computing the $d = \gcd(x_i - y_i, N)$
3: [Factor Found?] If $1 < d < N$, then $d$ is a nontrivial factor of $N$, print $d$, and go to step 5.
4: [Another Search?] If $x_i = y_i \pmod{N}$ for $i$ or $i \geq \sqrt{t}$, then go to step 2 to choose a new seed and a new generator and repeat.
5: [Exit] Terminate the algorithm.
```

1.6.3 Pollard's $p-1$ Factoring Method

The Pollard's $p-1$ algorithm was invented by J.M. Pollard (1974) . It is a special-purpose algorithm, this means that it is only suitable for integers with specific types of factors. Suppose that we are given the product of two distinct prime numbers $N = pq$ and our task is to find the prime factors p and q. Assume that by luck or hard work or some other method, we manage to find an integer L with the following properties

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

This means that there are integers i, h, and j with $j = q-1$ satisfying

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

Now, we choose a random integer a and compute a^L modulus p. From Fermat's little theorem we can write

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

which showed that

$$p \text{ divides } a^L - 1 \quad \text{and} \quad q \text{ does not divide } a^L - 1$$

Observed that since $p|N$ and we showed that $p|(a^L - 1)$, then one can recover p through the following simple computation

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

But one may ask, how can we find L that is divisible by $p-1$ and not by $q-1$? Pollard consider that if $p-1$ is to be the product of several small primes, then we can make use of the first few primes, and calculate the product of those primes and the result is multiple of $p-1$.

Similarly let $p|N$ such that is a product of many small primes. Then there exists an integer $L = B!$ such that $p-1|B!$ for some not-too-large value of B. This shows that $B! = (p-1)j$ for some integer j. Hence, we can compute the following relation

$$b \equiv a^{B!} \equiv (a^{p-1})^j \equiv 1 \pmod{p}$$

which gives $p = \gcd(a^{B!} - 1, N)$. In practice, one might simply choose $a = 2$. If the $\gcd(a^{B!} - 1, N)$ happens to be equal to 1, then we try the next value of B. And if happens to be number between 1 and N, then we have found a nontrivial factor of N.

Algorithm 1.5 Pollard's $p-1$ factorization of composite integer $N > 1$

```
1: Input $N = pq$ as a compute integer to be factored.
2: Choose an integer $a > 1$. Often 2 is used.
3: Choose a bound $B$.
4: Compute $a^{B!} - 1$ modulo $N$.
5: Compute $d = \gcd(a^{B!} - 1, N)$.
6: Check if $1 < d < N$.
7: If yes, we have found a nontrivial factor of $N$.
8: If no, loop again at Step 3 with $(B+h)$ for $h = 1,2,3,4,\ldots$ until we compute the
   gcd in step 3 such that $1 < d < N$.
```

Remark 1.1 *Note the following*

- *To compute $a^{B!} - 1$ is not feasible. Even if $a = 2$ with moderate values of B say $B = 100$, hence to compute the number $2^{100!}$ has more than 10^{157} digits, which is more than the number of particles in the universe.*

- *We need to compute* $\gcd(a^{B!}-1,N)$*. Then it suffices to calculate* $a^{B!}-1 \pmod{N} = \mu$ *and evaluate* $\gcd(\mu,N)=p$*. Thus we do not want to work with numbers which is greater or larger than N.*

- *Also,* $a^{(n+1)!} \equiv (a^{B!})^{n+1} \pmod{N}$*. Then, we can efficiently compute* μ

Remark 1.2 *It takes at most* $2\log_2\ j$ *steps in order to compute* $a^j \pmod{N}$ *using fast exponentiation algorithm. In other words, we can say that, the running time of computing* $a^j \pmod{N}$ *is in* $O(\log j)$ *steps. Then, to compute* $a^{B!} \pmod{N}$*, it takes approximately* $2n\log_2(n)$ *steps for some reasonable large values of n . One can choose p and q in such a way that both* $p-1$ *and* $q-1$ *can not be expressed into small primes decompositions which make the Pollard's* $p-1$ *method to fail, Hoffstein et al. (2008).*

Remark 1.3 *Note that the Pollard* $p-1$ *method of factoring is not useful to all numbers, it works if at least one of* $p-1$ *or* $q-1$ *factors entirely into the product of small prime powers. This means* $p-1$ *is even, so we can pull off a factor of* 2*. But the quantity* $\frac{1}{2}(p-1)$ *behave more or less like random number of size approximately* $\frac{1}{2}p$ *which is consider to be a hard problem. Also, to avoid Pollard's* $p-1$ *method, one can choose p and q in such a way that both* $p-1$ *and* $q-1$ *can not be expressed as a product of small prime powers.*

1.6.4 Elliptic's Curve Method

This is another method of splitting a composite integer into its prime factors invented by Lenstra (1987) that uses elliptic curves. This method uses the idea of Pollard's $p-1$ method except that the multiplicative group is replaced by the group of points in a random elliptic curve. If we can choose a random group G with order g close to p, we may be able to perform computation similar to that involved in Pollard's $p-1$ algorithm but working with G rather than F_p. The factors of an integer N can be found if all prime factors of g are less than the bound B otherwise we make a new choice of g and repeat the process until a factor is found. The running time of this method is $O(e^{\sqrt{(2+0(1))\log p \log\log p}})$ which is subexponential and works substantially faster for small p. Let $N > 1$ be a composite integer with $\gcd(N,\ 6) = 1$, the algorithm below tries to find a nontrivial factor of N.

Algorithm 1.6 Elliptic Curve Method of factoring a composite integer $N > 1$

```
1: [Choose an Elliptic Curve] Select a random pair $(E,P)$, where $E$ is an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}/N\mathbb{Z}$, and $P(x,y) \in E(\mathbb{Z}/N\mathbb{Z})$ is a point on $E$. That is choose $a, x, y \in \mathbb{Z}/N\mathbb{Z}$ at random, and set $b \leftarrow y^2 - x^3 - ax$. If $\gcd(4a^3 + 27b^2, N) \neq 1$, then $E$ is not an elliptic curve, then start over by choosing a new pair $(E,P)$ and repeat the process.
2: [Choose an integer $k$] Select a positive integer that is divisible by many prime powers, say $k = \text{lcm } (1, 2, \ldots, B)$ or $k = B!$ for a suitable bound $B$ (as $B$ becomes larger, the chances of producing a successful factor increases but the time taking will be long).
3: [Compute $kP$] Compute the point $kP \in E(\mathbb{Z}/N\mathbb{Z})$ by using the following formula to compute $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2) \bmod N$:
       $(x_3, y_3) = (\lambda^2 - x_1 - x_2 \pmod{N}, \ \lambda(x_1 - x_3) - y_1 \pmod{N}),$
   where
       $\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} \pmod{N}, & \text{if } P_1 = P_2 \\ \frac{y_1 - y_2}{x_1 - x_2} \pmod{N}, & \text{otherwise} \end{cases}$
   The computation of $kP \pmod{N}$ can be done in $O(log\ k)$ doubling and additions
4: [Compute gcd] If $kP \equiv O_E$ ( $(\bmod N)$), then set $m_2 = z$ and compute $d = \gcd(z,\ N)$, else go to step1 to make a new choice for $a$ or even for a new pair $(E,\ P)$.
5: [Factor Found?] If $1 < d < N$, then $d$ is a nontrivial factor of $N$, output $d$ and go to step 7.
6: [Start Over?]If $d$ is not a nontrivial factor of $N$ and want to try more elliptic curve, then go to step 7 and repeat the procedures again, else go to step 7.
7: [Exit] Terminate the algorithm.
```

1.6.5 Factorization via Difference of Squares

One of the most powerful factorization methods known today begins with the simplest identities

$$x^2 - y^2 = (x + y)(x - y)$$

The formula above says that a difference of squares is equal to a product. In order to factor a number N, we look for an integer b such that quantity $N + b^2$ is a perfect square, say equal to a^2. That is $N + b^2 = a^2$, then

$$N = a^2 - b^2 = (a + b)(a - b)$$

which yield the factorization of N.

However if N is large, then it is unlikely that a randomly chosen value of b will give $N+b^2$ into a perfect square. We want to give a clever method of selecting b. An important thing to consider is that we don't want to write N itself as a difference of two squares. It is sufficient to write some multiple kN of N as a difference of two squares, since

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

Hence to show that the factors of N are separated from the right-hand side of the equation, that is, N has a nontrivial factor in common with each of $a+b$ and $a-b$. It is then very easy to recover the successful factorization of integer N by evaluating $\gcd(N,\ a+b)$ and $\gcd(N,\ a-b)$. Thus, the running time of this method is given as $O(\sqrt{N})$. Since $N \approx 2^{2n}$, then $O(\sqrt{N}) = O((2^{2n})^{1/2}) = O(2^n)$ which is exponential. The multiples of N are the numbers that are congruent to 0 modulo N , so rather than searching for a difference of squares $a^2 - b^2$ that is a multiple of N, we may instead search for distinct numbers a and b such that

$$a^2 \equiv b^2 \pmod{N}.$$

In practice it is not feasible to search directly for integers a and b that satisfy the above congruence relation. We give some steps that will aid the factorization of a composite integer $N > 1$.

Algorithm 1.7 Factorization of $N > 1$ via Difference of Squares Method

```
1: [Relation Building] Find many integers $a_1, a_2, a_3, \dots, a_r$ with the property that the
   quantity $c_i \equiv a_i^2 \pmod{N}$ factors as a product of small primes.
2: [Elimination] Take a product $c_{i1}c_{i2}\dots, c_{is}$ of some of the $c_i$'s so that every prime
   appearing in the product appears to an even power. Then $c_{i1}, c_{i2}, \dots, c_i^{\prime}s = b^2$ is a
   perfect square.
3: [gcd Computation] Let $a = a_{i1}a_{i2}\dots, a_{is}$ and compute the greatest common divisor
   $d = \gcd(N, a-b)$. Since
       $a^2 = (a_{i1}a_{i2}\cdots a_{is})^2 \equiv a_{i1}^2 a_{i2}^2 \cdots a_{is}^2 \equiv c_{i1}c_{i2}\cdots c_{is} \equiv b^2 \pmod{N},$
   there is a reasonable chance that $d$ is a nontrivial factor of $N$ . If $1 < d < N$ is a
   nontrivial factor of $N$, then go to step 4, else make a new choice and go to step 1
   and repeat the process.
4: [Exit] Terminate the algorithm.
```

For other methods on integer factorization refer to Hoffstein et al. (2008), Song (2002), and Cohen (1996).

The following table gives a summary of the running time of some of the integer factorization problems:

Table 1.1: Running Time of Algorithms for Solving IFP

Algorithm	Running Time	Remark
Trial Divisions	$O(n^2\sqrt{N})$	Exponential
Pollard $p-1$ Factorization Algorithm	$O(\log m)$	Logarithmic
Factorization Via Difference of square	$O(\sqrt{N})$	Exponential
Quadratic Sieve Factoring	$O(\sqrt{n \cdot \log n})$	Subexponential
Pollard ρ Method	$O(p^{1/2}(\log n)^2)$	Subexponential
Continued Fraction Method	$O(c^{\sqrt{\log p \log\log p}})$	Subexponential
Number Field Sieve	$O(e^{((c+0(1))\sqrt[3]{\log n}\sqrt[3]{(\log\log n)})})$	Subexponential
Elliptic Curve Method	$O(e^{\sqrt{(2+0(1))\log p \log\log p}})$	Subexponential

1.6.6 Modulus $N = pq$

This section presents the RSA modulus whose hardness relies on the difficulty of solving the integer factorization problem. Let $N = pq$ be an RSA modulus where a composite integer N is the product of two large random prime numbers p and q of the same bit size. Let (e,N) be the public key tuple where the parameter e is used for encryption and let d be a private exponent used for decryption. Then the parameters e and d are related in the form $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N)$ is known as Euler's totient function defined as $\phi(N) = (p-1)(q-1)$. The above modular relation can be written as $ed = 1 + k\phi(N)$ for $k \in \mathbb{Z}$ known as key equation with only one known parameter e and three unknown parameters d, k and $\phi(N)$.

This RSA modulus suffers from various attacks such as common modulus attacks, small public exponent attacks, short decryption exponent attacks, side channel attacks, Boneh and Durfee lattice attack, partial key exposure attacks and many more which can be found in Hinek (2009).

This research work focuses on constructing new strategies of factoring moduli $N = pq$ and $N = p^r q$ for $r \geq 2$ in polynomial time and in relation to short decryption exponent attacks. As such, it will briefly report some attacks that factor the modulus $N = pq$ efficiently as a result of using short decryption exponents.

The first to report about an attack upon short decryption exponents was by Wiener (1990). He showed that the modulus $N = pq$ can be factored efficiently into its prime factors p and q if the short decryption exponent $d < \frac{1}{3}N^{\frac{1}{4}}$ using continued fraction method.

Varheul and van Tilborg extended the boundary of the Wieners attack by exhaustive search for the short decryption exponent d using continued fraction method. In their findings, they showed that the cost of exhaustive search for d having modulus $N = pq$ is $2r+8$ when extending the Wiener's boundary to r bits where $r = \ln_2 \frac{d}{N^{0.25}}$ with a complexity of about $\ln_2(N)2^{2r}$ which yielded the results in polynomial time, Verheul and van Tilborg (1997).

In 1999, Boneh and Durfee proposed a heuristic attack on the modulus $N = pq$ using lattice construction technique which factored the modulus into its prime factors with an improved bound of short decryption exponent $d < N^{0.292}$, see (Boneh and Durfee (1999)). B. D. Weger also reported an attack on $N = pq$ where he showed that the modulus is insecure if the prime difference $|p-q| < N^{\gamma}$ for $\frac{1}{4} \le \gamma \le \frac{1}{2}$ using continued fraction method, de Weger (2002). Maitra and Sarkar proved that the $N = pq$ can be factored in polynomial if $|2q-p| \le \frac{N^{\gamma}}{16}$ where $q < p < 2p$ and balanced primes, Maitra and Sarkar (2008). Another cryptanalysis attacks on $N = pq$ using ratio of primes was carried out by Chen's et al (2009) where they proved that the modulus $N = pq$ can be factored efficiently if $|ap-bq| = N^{\gamma}$ where $q < p < 2p$, (a,b) are small positive integers less than $\log N$ and $\frac{1}{4} \le \gamma \le \frac{1}{2}$.

Furthermore, Nitaj (2012) also reported attack on the modulus $N = pq$ using continued fraction method that improved the short decryption exponent bound to $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{0.25}$ which factor the modulus in polynomial time, **?** . Mu-En, Chien-Ming, Yue-Hsun and Hung-Min (2014) proposed another attack on $N = pq$ through exhaustive searching of MSBs of $p+q$ as many as possible which is equivalent to estimating $p+q$ as accurately as possible, Wu et al. (2014). The result of their findings reduced the cost of exhaustive search to $2r+2$ which is an extension of Wiener's boundary r bits and 2^6 faster than Verheul and van Tilborg (1997) attack. Other proposed attacks on modulus $N = pq$ can found in Hashimoto (2010) , Asbullah and Ariffin (2015), Bunder and Tonien (2017) and Akchiche and Khadir (2018).

1.6.7 Modulus $N = p^2q$

In order to make encryption and decryption work faster and more efficient, some proposed cryptosystem were developed with modulus $N = p^2q$ where p and q are prime factors of a composite number N. Fujioka and Miyaguchi (1991) was the first to used the modulus $N = p^2q$ for digital signature whose computational speed is faster than the original RSA scheme. Also in 1998, Okamoto and Uchiyama proposed a public key cryptography scheme whose security is considered to be as difficult as factoring an RSA modulus of the form $N = p^2q$ Okamoto and Uchiyama (1998). HIME(R) cryptosystem proposed a modulus of the form $N = p^2q$ where p and q are prime numbers which was found to be faster in decryption than the modulus $N = pq$ and the security of this cryptosystem is based on the hardness of factoring a composite integer $N = p^2q$, see Hitachi (2001). In 2013, Sarkar reported the use of short decryption exponent attack on prime power with modulus $N = p^2q$ which he showed that the cryptosystem is insecure if the bound $d < N^{0.395}$ and he successfully factored the prime power modulus $N = p^2q$ into its prime factors p and q, Sarkar (2013).

In 2013, Ariffin developed a new scheme based on the hardness of factoring integers of the form $N = p^2q$ (Ariffin et al. 2013). The Ariffin scheme uses a combination of modular linear and modular squaring. They showed that the decryption is 1-to-1 which is of great advantage over Rabin's cryptosystem. Its encryption speed has a complexity order faster than RSA and ECC. For decryption its speed is better than RSA and is marginally behind ECC. Also the scheme was constructed using a simple mathematical structure, and it has low computational requirements which enable communication devices with low computing power to deploy secure communication procedures efficiently, Ariffin et al. (2013). In 2015, Asbullah and Ariffin also showed that the prime power modulus of the form $N = p^2q$ can be successful factored by taking the term $N-(2N^{2/3}-N^{1/3})$ as a good approximation of $\phi(N)$ satisfying the key equation $ed-k\phi(N) = 1$, (Asbullah and Ariffin (2015)).

1.6.8 Modulus $N = p^rq$

The modulus $N = p^rq$ for $r \geq 2$ is known as the prime power modulus whose security depends on the difficulty of factoring the modulus N into its prime factors p and q of the same bit size. The first person to report the security threat for this type of scheme was Takagi in 1991 where he proved that the cryptosystem is insecure if the short decryption exponent $d \leq N^{\frac{1}{2(r+1)}}$ for $r \geq 2$, the modulus $N = p^rq$ can be factored efficiently using lattice based technique Takagi (1998). May (2004) reported an improvement on the bound of Takagi where he showed that the modulus $N = p^rq$ is insecure if the short decryption exponent $d < N^{max\{\frac{r}{(r+1)^2},\frac{(r-1)^2}{(r+1)^2}\}}$, May (2004) . More reports on factoring the modulus N can be found in Sarkar (2014), Lu and Lin (2014), Shehu and Ariffin (2017).

1.7 RSA Cryptosystem

The RSA key generation involves random selection of two distinct large prime numbers such that their product is represented as $N = pq$ and called the RSA modulus. The Euler totient function $\phi(N)$ is computed as $\phi(N) = (p-1)(q-1)$ and also choosing an integer $e < \phi(N)$ such that the $\gcd(e,\phi(N)) = 1$ and computing a short decryption exponent d such that the relation $ed \equiv 1 \bmod \phi(N)$ is satisfied. Then the pairs (e,N) and (d,p,q) are called the public and private keys respectively.

The encryption function is always computed by choosing a message $M \in \mathbb{Z}_N$ and computing the ciphertext $C = M^e \pmod N$ while the plaintext can also be recovered by computing the decryption exponent from an equation $M = C^d \pmod N$. The primes p and q in most cases are consider to have same bit length.

1.7.1 RSA Algorithm

In simpler terms, the RSA cryptosystem involves three processes of key generation, encryption, and decryption algorithms as presented in Algorithms 1.8, 1.9 and 1.10 below:

Algorithm 1.8 RSA key generation

```
Initialization: Input the size $n$ and $(e, N)$.
Choose two random and distinct $n - bit$ strong primes $(p, q)$.
**for each** pair of the form $(p, q)$ **do**
    $N := pq$
    $\phi(N) := (p-1)(q-1)$
**end for**
Choose a random integer $e$ such that $1 < e < \phi(N)$ and gcd$(e, \phi(N))$ = 1.
**if** $d$ is an integer **then**
    $ed \equiv 1 \pmod{\phi(N)}$.
**end if**
**return** the public key pair $(N, e)$ and the private key pair $(N, d)$.
```

Algorithm 1.9 RSA encryption

```
Initialization: Input the public key pair $(e, N)$ and the plaintext $M$.
Represents the plaintext message $M$ as integer such that $M < N$ and $\gcd(M, N) = 1$.
**for each** triplet of the form $(e, N, M)$ **do**
    $C := M^e \pmod{N}$
**end for**
**return** the ciphertext $C$.
```

Algorithm 1.10 RSA decryption

```
Initialization: Input the private key pair $(d,N)$ and the ciphertext $C$.
for each triplet of the form $(d,N,C)$ do
    $M := C^d \pmod N$
end for
return the message $M$.
```

Theorem 1.1 *(Euler's Theorem). Let $N = pq$ and $\phi(N) = (p-1)(q-1)$. For any integer M such that* $\gcd(M,N) = 1$*, then* $M^{\phi(N)} \equiv 1 \pmod N$.

Proof:
See Hoffstein et al. (2008)

1.8 AA_β Cryptosystem

This section will presents an enhanced AA_β cryptosystem algorithm of factoring $N = p^2q$ as proposed by Ariffin et al. (2013). The AA_β cryptosystem has key generation algorithm, encryption algorithm and decryption algorithm as outlined by Algorithms 1.11, 1.12, and 1.13.

Algorithm 1.11 AA_β key generation

```
Initialization: Input the size $n$ and $(e,N)$.
Choose two random and distinct $n-bit$ prime numbers $(p,q)$ such that the inequality $2^n < p,q < 2^{n+1}$ satisfying the relation $p,q \equiv 3 \pmod 2$ holds.
for each pair of the form $(p,q)$ do
    $N_2 := p^2q$
    $r_1 := 2^{3n+4}$
    $r_2 := 2^{3n+6}$
end for
Compute a random integer $N_1$ such that $r_1 < N_1 < r_2$
if $d$ is an integer then
    $N_1 d \equiv 1 \pmod{N_2}$.
end if
return the public key pair $(N_1,N_2)$ and the private key pair $(d,p)$.
```

Algorithm 1.12 AA_β encryption

```
Initialization: Input the public key pair $(N_1, N_2)$ and the plaintext $M, T$.
Represents the plaintext message $M$ as $2^{2n-2} < M < 2^{2n-1}$ such that $\gcd(M, N_2) = 1$.
Choose a plaintext $T$ such that $2^{4n} < T < 2^{4n+1}$
for each tuple of the form $(N_1, N_2, M, T)$ do
    $C := N_1 M^2 + N_2 T$
end for
return the ciphertext $C$.
```

Algorithm 1.13 AA_β decryption

```
Initialization: Input the private key pair $(d, p)$ and the ciphertext $C$.
for each triplet of the form $(d, p, C)$ do
    $Z \equiv C^d \pmod{N_2}$
    $M_p \equiv Z^{\frac{p+1}{4}} \pmod{p}$
    $W := \frac{Z - M_p^2}{p}$.
    $X \equiv \frac{W}{2M_p} \pmod{p}$
    $M_1 = M_p + Xp$
end for
if $M_1 < 2^{2n-1}$ then
    return $M := M_1$. Else return $M := p^2 - M_1$
    $T := \frac{C - N_1 M^2}{N_2}$.
end if
return the message $M, T$.
```

For proof of correctness for AA_β decryption, see Ariffin et al. (2013).

1.9 Takagi Cryptosystem

In this section, the key generation algorithm, encryption and decryption algorithms of the Takagi cryptosystem for factoring the modulus $N = p^r q$ for $r \geq 2$ will be presented in Algorithms 1.14, 1.15 and 1.16.

Algorithm 1.14 Takagi key generation

```
Initialization: Input the size $n$ and $(e,N)$.
Choose two random and distinct $n-bit$ strong primes $(p,q)$.
for each pair of the form $(p,q)$ do
    $N := p^r q$
    $\phi(N) := p^{r-1}(p-1)(q-1)$
end for
Choose a random integer $e$ such that $1 < e < \phi(N)$ and gcd$(e,p) = 1$.
if  $d$ is an integer then
    $ed \equiv 1 \pmod{\phi(N)}$.
end if
return the public key pair $(N,e)$ and the private key tuple $(d,p,q)$.
```

Algorithm 1.15 Takagi encryption

```
Initialization: Input the public key pair $(e,N)$ and the plaintext $M$.
Represents the plaintext message $M$ as integer such that $M < N$ and $\gcd(M,N) = 1$.
for each triplet of the form $(e,N,M)$ do
    $C := M^e \pmod{N}$
end for
return the ciphertext $C$.
```

Algorithm 1.16 Takagi decryption

```
Initialization: Input the private key pair $(d,p,q)$ and the ciphertext $C$.
for each tuple of the form $(d,p,q,C)$ do
    $M_q := C^d \pmod{q}$
    $M_p := C^d \pmod{p}$
end for
return the message $M$.
```

For the proof of correctness of the above algorithm, see Takagi (1998).

1.10 Problem Statement

The integer factorization problem has always been of mathematical interest. The problem of finding two prime factors of a large composite integer $N = pq$ has been considered to be a major challenge often which some of the public key cryptosystems security were built. Likewise the prime power modulus variant $N = p^r q$ relies on the difficulty of decomposing the given prime power modulus into its two prime factors. The complexity running time of most of the existing factoring methods are consider to be subexponential. However, in order to ensure the difficultness remain intact, it is the hope of this research to find new criteria upon primes to be avoided.

1.11 Research Questions and Hypothesis

This research work is aimed at finding new criteria upon primes to be avoided in order to ensure the difficultness of factoring either $N = pq$ or $N = p^r q$ remain intact. The research questions are as follows:

1. What is the relationship between improving short decryption exponent bound using small prime difference and the difficulty of factoring cryptosystem with modulus $N = pq$?

2. What makes t instances of a public key pair (N_s, e_s) with moduli $N_s = p_s q_s$ factorizable when there is an improvement on the bound d such that the generalized RSA key equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$, and $e_s d_s - k\phi(N_s) = z_s$ are satisfied ?

3. How can improving the bound of short decryption exponent for prime power with modulus of the form $N = p^r q$ make the scheme insecure and leads to the factorization of the modulus $N = p^r q$ in polynomial time?

4. What makes t instances of a prime power public key pair (N_s, e_s) with moduli $N_s = p_s^r q_s$ factorizable when there exists an improvement on the bound d such that the following generalized key equations $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$, and $e_s d_s - k\phi(N_s) = z_s$ hold?

1.12 Research Objectives and Methodology

The research objectives together with brief explanations of the methodology adopted are stated below:

1. To develop new cryptanalytic attack on the modulus $N = pq$ with relation to the bound of the decryption exponent d.

   Methodology: The method to be employed is aimed at finding a good approximation of $\phi(N)$ using information from public key pair (e,N). That is, by taking the convergents of the continued fraction expansions of $\frac{e}{N - \lceil \frac{a^2+b^2}{ab}\sqrt{N} \rceil + 1}$, $\frac{e}{N - \lceil \frac{a^j+b^i}{a^{\frac{j}{2}} b^{\frac{i}{2}}}\sqrt{N} \rceil + 1}$, $\frac{e}{N - \lceil \frac{a^j+b^j}{(ab)^{\frac{j}{2}}}\sqrt{N} \rceil + 1}$ and $\frac{e}{N^*}$ where $N^* = N - \left\lceil \left(\frac{a^{\frac{i+1}{i}} + b^{\frac{i+1}{i}}}{2(ab)^{\frac{i+1}{2i}}} + \frac{a^{\frac{1}{j}} + b^{\frac{1}{j}}}{2(ab)^{\frac{1}{2j}}} \right) \sqrt{N} \right\rceil + 1$, where $2 < j < i$ to find the right candidates among the convergents that can yields to the factorization of modulus $N = pq$ in polynomial time where a, b, i and j are small positive integers.

2. To develop a new cryptanalytic attack that can simultaneously and successfully factor t instances of the moduli $N_s = p_s q_s$ given public key pair (e_s, N_s) with

relation to $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$ and $e_sd_s - k\phi(N_s) = z_s$ for $s = 1,\ldots,t$.

Methodology: The method to be adopted can be formulated upon generalized key equations. It will then transform the generalized key equations into a simultaneous Diophantine approximations problem and apply lattice basis reduction techniques to find some unknown parameters, which can lead to finding t prime factors p_s and q_s of t instances moduli $N_s = p_sq_s$ in polynomial time.

3. To develop a new technique of factoring prime power modulus $N = p^rq$ for $r \geq 2$ by using good approximation of $\phi(N)$, the public key pair (e,N) and its relation with the bound of the decryption exponent d that will lead to the factorization of the modulus in polynomial time.

   Methodology: It will employ continued fraction method to search for a right and better candidate from convergents of the continued fraction expansion of approximation of $\phi(N)$ that can lead to the successful factorization of the prime power modulus $N = p^rq$ in polynomial time.

4. To develop a new cryptanalytic attack that can simultaneously and successfully factor t instances prime power moduli $N_s = p_s^rq_s$ given public key pair (e_s,N_s) with relation to $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$ and $e_sd_s - k\phi(N_s) = z_s$ for $s = 1,\ldots,t$ and $r \geq 2$.

   Methodology: The method to be adopted will be formulated upon generalized key equations. It will then transform the generalized key equations into a simultaneous Diophantine approximations problem and apply lattice basis reduction techniques to find some unknown parameters, which will enable us to find t prime factors p_s and q_s of t instances prime power moduli $N_s = p_s^rq_s$ for $r \geq 2$ in polynomial time.

1.13 Scope of the Research

This research work is aimed at developing new factorization strategies of $N = pq$ and $N = p^rq$ for $r \geq 2$ and relation to its short decryption exponent bound using continued fractions method. It is the hope of this research to find a better approximations of $\phi(N)$ through analyzing cases of small prime difference under certain restrictions on parameters to be used. The findings of this work is also expected to yield improve decryption exponent bound.

This research work will also explore new factorization strategies for moduli $N_s = p_sq_s$ and prime power moduli $N_s = p_s^rq_s$ for $s = 1,\ldots,t$ and $r \geq 2$ using generalized key equations. These proposed strategies are expected to simultaneously factor t moduli N_s

in polynomial time by applying simultaneous Diophantine approximations and lattice basis reduction method to obtain unknown positive integers (d, k_s) and (d_s, k).

1.14 Overview of the Thesis

In this section, a skeleton of the thesis compositions is briefly given as follows:

Chapter 1 gives introduction to cryptography and its goals, cryptanalysis and some types of attacks, definitions of some terms such as public key cryptography, complexity theory, primality testing, integer factorization problem and some reports on factoring modulus of the form $N = pq$, $N = p^2q$, $N = p^rq$, an overview of RSA, AA_β and Takagi cryptosystems through key generations algorithms, encryption and decryption algorithms and their proofs of correctness. The chapter also presents statement of the problem, research questions, research objectives and methodology adopted in accomplishing them. The section also put forwards scope of the research and finally present an overview of the thesis.

Chapter 2 presents some literature review on successful cryptanalytic attacks in relation to the bound of short decryption exponent upon the RSA modulus $N = pq$ using a good approximations of $\phi(N)$, attacks using small prime difference and successful cryptanalytic attacks on prime power modulus $N = p^rq$ for $r \geq 2$ based on the bound of the decryption exponent and successful factoring t instances RSA moduli $N_s = p_sq_s$ and also t instances of prime power RSA with moduli $N_s = p_s^rq_s$ for $s = 1, \ldots, t$.

Chapter 3 presents the results on new bounds for the decryption exponent that leads toward successful factorization by observing small prime difference. The chapter presents three cases. It also reports successful factorization of t instances of RSA moduli $N_s = p_sq_s$ by analyzing the generalized key equations given by $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$ and $e_sd_s - k\phi(N_s) = z_s$ for unknown parameters d, k_s, d_s, k and z_s where $s = 1, \ldots, t$.

In Chapter 4, this research reports another new decryption exponent bound that leads toward successful factorization of $N = pq$ in polynomial time using continued fraction method . It also presents four cryptanalysis attacks upon t instances of RSA generalized key equations of the shape $e_sd - k_s\phi(N_s) = 1$, $e_sd_s - k\phi(N_s) = 1$, $e_sd - k_s\phi(N_s) = z_s$ and $e_sd_s - k\phi(N_s) = z_s$ for unknown positive integers d, k_s, d_s, k and z_s where $s = 1, \ldots, t$. In all the attacks, it successfully factored the moduli $N_s = p_sq_s$ in polynomial time by transforming the above equations into a simultaneous Diophantine problem. It then applies lattice basis reduction method to find the values of the unknown parameters. These values aided the computation of t prime factors p_s and q_s simultaneously. The chapter gives numerical examples in all the attacks presented.

Chapter 5 presents new results regarding bounds for the decryption exponent that leads toward successful factorization of prime power modulus $N = p^r q$ where $r \geq 2$ using a good approximation of $\phi(N)$, given by $\Phi = N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} + 1$. It utilizes right candidate from the convergents of $\frac{e}{\Phi}$. The chapter also presents new successful attacks on t instances of the prime power moduli $N_s = p_s^r q_s$.

Finally, Chapter 6 concludes the thesis by summarizing the research findings and also suggests some future directions for researchers in this field to explore.

REFERENCES

Akchiche, O. and Khadir, O. (2018). Factoring RSA moduli with primes sharing bits in the middle. *Applicable Algebra in Engineering, Communication and Computing*, 29(3):245–259.

Ariffin, M., Asbullah, M. A., Abu, N. A., and Mahad, Z. (2013). A new efficient asymmetric cryptosystem based on the integer factorization problem of $N = p^2q$. *Malaysian Journal of Mathematical Sciences*, 7(S):19–37.

Asbullah, M. A. (2015). *Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-like Cryptosystem without Decryption failure*. PhD thesis, Universiti Putra Malaysia.

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

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. (1999). Cryptanalysis of RSA with private key $d < N^{0.292}$. In *Advances in Cryptology-Eurocrypt99, Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag.

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. and Tonien, J. (2017). A new attack on the RSA cryptosystem based on continued fractions. *Malaysian Journal of Mathematical Sciences:Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology*, 11(S):45–57.

Chen C.Y. Hsueh, C. and Lin, Y. (2009). A generalization of de Weger's method. *IEEE*, 1:344–347.

Cohen, H. (1996). *A Course in Computational Algebraic Number Theory*. Springer, Heidelberg; New York, third edition.

Courtois, N. T., Mourouzis, T., and Le, P. V. (2012). Extension of de Weger's attack on RSA with large public keys. In *SECRYPT*, pages 145–153.

Davenport, H. and Schmidt, W. (1970). Dirichlet's theorem on Diophantine approximation. ii. *Acta Arithmetica*, 4(16):413–424.

de Weger, B. (2002). Cryptanalysis of RSA with small prime difference. *Applicable Algebra in Enginering, Commnication and Computing AAECC*, 13:17–28.

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

Fujioka, A. Okamoto, T. and Miyaguchi, S. (1991). ESIGN: An efficient digital signature implementation for smart cards. In *Advances in Cryptology EUROCRYPT 91,Lecture Notes in Computer Science*, pages 446–457. Springer.

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press, New York.

Hardy, G. and Wright, E. (1965). *An Introduction to the Theory of Numbers*. Oxford University Press, New York.

Hashimoto, Y. (2010). On small secret key attack against RSA with high bits known prime factor. *IACR Cryptology ePrint Archive*, 2010:657.

Hinek, J. (2007). *On the Security of Some Variants of RSA*. Phd thesis, Universiti Waterloo, Ontario, Canada.

Hinek, M. (2009). *Cryptanalysis of RSA and Its Variants*. Chapman and Hall, Boca Raton London, New York.

Hitachi, L. (2001). Specification of HIME(R) cryptosystem. Technical report, Hitacchi.

Hoffstein, J., Pipher, J. C., Silverman, J. H., and Silverman, J. H. (2008). *An introduction to mathematical cryptography*, volume 1. Springer, New York.

Lenstra, W. (1987). Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673.

Lu, Y. Zhang, R. and Lin, D. (2014). New results on solving linear equations modulo unknown divisors and its applications. *IACR Cryptology eprint*, 1(1-4):343–354.

Lu, Y. Zhang, R. and Lin, D. (2015). Solving linear equations modulo unknown divisors: Revisited. In *Advances in Cryptology - ASIACRYPT 2015. Lecture Notes in Computer Science*, pages 189–213. Springer.

Maitra, S. and Sarkar, S. (2008). Revisiting wieners attack new weak keys in RSA. In *Lecture Notes in Computer ScienceInternational Conference on Information Security-ISC 2008*, pages 228–243. Springer.

May, A. (2004). Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In *Public Key Cryptography-PKC 2004*, pages 218–230. Springer.

Menezes, A.J. van Oorschot, P. and Vanstone, S. (2001). *Handbook of Applied Cryptography*. Chapman and Hal, London, fifth edition.

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., Nassr, D., and Bahig, H. (2014). New Attacks on the RSA cryptosystem. In *Progress in Cryptology AFRICACRYPT 2014. Lecture Notes in Computer Science*, volume 8469, pages 178–198. Springer.

Oded, G. (2001). *Foundations of cryptography : Basic tools*. Cambridge University Press.

Okamoto, T. and Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology EUROCRYPT'98, Lecture Notes in Computer Science*, pages 308–318. Springer.

Pollard, J. (1975). A Monte Carlo method for factorization. *BIT*, 15:331–334.

Rahman, N. A. and Ariffin, M. (2017). New vulnerability of RSA modulus type $N = p^2q$. *Malaysian Journal of Mathematical Sciences:Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology)*, 11(S):75–88.

Sarkar, S. (2013). Small secret exponent attack on RSA variant with modulus $N = p^2q$. In *Proceedings International Workshop on Coding and Cryptography -WCC 2013*, pages 215–222. Norway and INRIA.

Sarkar, S. (2014). Small secret exponent attack on RSA variant with modulus $N = p^rq$. *Des. Codes Cryptogr.*, 7(2):383–392.

Sarkar, S. (2016). Revisiting prime power RSA. *Discrete Applied Mathematics*, 203(C):127–133.

Shehu, S. and Ariffin, M. (2017). New attacks on prime power RSA $N = p^rq$ using good approximation of $\phi(N)$. *Malaysian Journal of Mathematical Sciences special issues:The 5th International Cryptology and Information Security Conference(New Ideas in Cryptology)*, 11(S):121–138.

Singh, S. (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor books, New York.

Song, Y. Y. (2002). *Number Theory for Computing*. Springer Science & Business Media, New York, second edition.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices*. Prentice Hall, Upper Saddle River, New Jersey, United States, fourth edition.

Takagi, T. (1998). Fast RSA-type cryptosystem modulo p^kq. In *Advances in Cryptology CRYPTO '98. CRYPTO 1998. Lecture Notes in Computer Science*, pages 318–326. Springer.

Talbot, J. and Welsh, D. (2006). *Complexity and Cryptography: An Introduction*. Cambridge University Press, New York.

Verheul, E. R. and van Tilborg, H. C. (1997). Cryptanalysis of less short RSA secret exponents. *Applicable Algebra in Engineering, Communication and Computing*, 8(5):425–435.

Wang, X., G., X., Wang, M., and Meng, X. (2016). *Mathematical Foundations of Public Key Cryptography*. CRC Press, Boca Rating London New York.

Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inform. Theory*, 36(3):553–558.

Wu, M.-E., Chen, C.-M., Lin, Y.-H., and Sun, H.-M. (2014). On the improvement of Wiener attack on RSA with small private exponent. *The Scientific World Journal*, 2014.

BIODATA OF STUDENT

Saidu Isah Abubakar was born on the 27th October, 1982 in Sokoto, Nigeria. He started his primary school in the year 1988 at Waziri Model Primary School, Sokoto which he completed in the year 1994. He proceeded with his secondary school which he completed in the year 2000 at Sultan Bello Secondary School, Sokoto. The student also obtained his Nigeria Certificate in Education (NCE) Maths/Computer Science at Shehu Shagari College of Education, Sokoto in the year 2004. He had his Bachelor of Science Degree in Education Mathematics and Master of Science Degree in Mathematics from Usmanu Danfodiyo University, Sokoto in 2008 and 2012 respectively. The student is enrolled as Ph.D student in Universiti Putra Malaysia (UPM) to study Mathematical Cryptography in February 2016. Happily married with children.

LIST OF PUBLICATIONS

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

Muhammad Rezal Kamel Ariffin, Saidu Isah Abubakar, Faridah Yonus and Muhammad Asyraf Asbullah, New Cryptanalytic Attack on RSA Modulus $N = pq$ Using Small Prime Difference Method, *Cryptography* 2019, 3(1), 2; https://doi.org/10.3390/cryptography3010002.

Abubakar, S.I, Ariffin, M.R.K and Asbullah, M.A (2018). A New Improved Bound for Short Decryption Exponent on RSA Modulus $N = pq$ Using Wener's Method. (Accepted for publication by MJMS).

Abubakar, S.I, Ariffin, M.R.K and Asbullah, M.A (2018).A New Simultaneous Diophantine Attack Upon RSA Moduli $N = pq$. (Accepted for publication by MJMS).

Abubakar, S.I, Ariffin, M.R.K, Faridah Yunos and Asbullah, M.A (2018) Diophantine Attack on Prime Power RSA with Modulus $N = p^r q$.

Abubakar, S.I, Ariffin, M.R.K, Faridah Yunos and Asbullah, M.A (2018) A New Small Secret Exponent Cryptanalysis attacks of Factoring RSA Modulus $N = pq$.

Abubakar, S.I, Ariffin, M.R.K, Faridah Yunos and Asbullah, M.A (2018) A New Technique of Factoring RSA Modulus $N = pq$.

UNIVERSITI PUTRA MALAYSIA
STATUS CONFIRMATION FOR THESIS/PROJECT REPORT AND COPYRIGHT
ACADEMIC SESSION: First Semester 2018/2019

TITLE OF THE THESIS/PROJECT REPORT:

FACTORIZATION STRATEGIES OF $N = pq$ AND $N = p^r q$ AND RELATION TO ITS DECRYPTION EXPONENT

NAME OF STUDENT: SAIDU ISAH ABUBAKAR

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 acces.

This thesis is submitted for:

□ PATENT Embargo from ___________until ___________.
(date) (date)

Approved by:

____
(Signature of Student)
New IC No/Passport No.:850523-10-5567
Date:

____
(Signature of Chairman of Supervisory Committee)
Name: **Associate Professor. Muhammad Rezal Kamel Ariffin**
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.]