UNIVERSITI PUTRA MALAYSIA

PERFORMANCE ANALYSIS AND IMPROVEMENT OF RABIN PRIMITIVE BASED CRYPTOSYSTEMS

ZAHARI BIN MAHAD

IPM 2014 14

PERFORMANCE ANALYSIS AND IMPROVEMENT OF RABIN PRIMITIVE BASED CRYPTOSYSTEMS

By

ZAHARI BIN MAHAD

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

February 2014

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

PERFORMANCE ANALYSIS AND IMPROVEMENT OF RABIN PRIMITIVE BASED CRYPTOSYSTEMS

By

ZAHARI BIN MAHAD

February 2014

Supervisor : Muhammad Rezal Bin Kamel Ariffin, PhD
Department : Institute for Mathematical Research

In this study, we analyze the performance of a new cryptosystem called AA_β Public Key Cryptosystem. The encryption process for the AA_β cryptosystem is easy and fast as operations involved only add and multiply operations. While in the decryption process, it involves the mathematical solution method using Chinese Remainder Theorem that produces four different answers where only one correct answer need to be determined by user.

The AA_β cryptosystem is constructed based on the mathematical problem of solving the Square Root Modulo and Integer Factorization problem. Results from the study and analysis found that AA_β cryptosystem have speeds exceeding RSA and ECC cryptosystem encryption process. While the decryption process, AA_β have speeds exceeding RSA and ECC. But when the sizes of prime number increase to 2048-bits, ECC is faster than AA_β.

Through research and analysis, we have found a new feature in AA_β cryptosystem can be enhanced which can result in increased speed on the decryption process. Therefore, in this study, we will define an amended structure of the AA_β cryptosystem by improving existing features resulting in increased speed in the decryption process. With this new definition, we still maintain safety features available on AA_β cryptosystem to avoid being attacked by enemies.

Finally, we amend the Rabin cryptosystem utilizing the encryption strategy of the AA_β algorithm and run experiments to gauge its efficiency.

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

ANALISIS PENCAPAIAN DAN PENAMBAHBAIKAN SISTEMKRIPTO BERASASKAN PRIMTIF RABIN

Oleh

ZAHARI BIN MAHAD

Februari 2014

Penyelia : Muhammad Rezal Bin Kamel Ariffin, PhD
Institut : Institut Penyelidikan Matematik

Penyelidikan ini mengkaji dan menganalisis prestasi satu sistemkripto baru yang diberi nama Sistemkripto Kekunci Awam AA_{β}. Proses penyulitan bagi sistemkripto-AA_{β} adalah mudah dan laju memandangkan operasi-operasi yang terlibat hanyalah operasi tambah dan darab. Manakala bagi operasi penyahsulitan pula, ianya melibatkan kaedah penyelesaian bermatematik menggunakan Chinese Remainder Theorem yang menghasilkan empat jawapan yang berlainan dan hanya satu sahaja jawapan yang betul.

Sistemkripto-AA_{β} yang dibangun berasaskan kepada permasalahan bermatematik payah kepada Punca Kuasa Dua Bermodulo dan Pemfaktoran Integer. Hasil daripada kajian dan analisis yang dijalankan mendapati bahawa sistemkripto-AA_{β} mempunyai kelajuan melebihi sistemkripto RSA dan ECC dalam proses penyulitan. Manakala bagi proses penyahsulitan pula, AA_{β} mempunyai kelajuan yang melebihi RSA dan ECC. Apabila saiz nombor perdana meningkat kepada 2048-bit, ECC adalah lebih laju berbanding AA_{β}.

Melalui kajian dan analisis yang dijalankan, kami telah menemui ciri baru pada sistemkripto-AA_{β} yang boleh diperbaiki yang mana mengakibatkan kelajuan pada proses penyahsulitan bertambah. Justeru dalam kajian ini, kami akan menakrifkan semula struktur sistemkripto- AA_{β} dengan menambahbaik ciri yang sedia ada sehingga mengakibatkan meningkatnya kelajuan dalam proses penyahsulitan. Berdasarkan penakrifan baru ini, kami masih mengekalkan lagi ciri-ciri keselamatan sedia ada pada sistemkripto-AA_{β} bagi mengelak daripada diserang oleh musuh.

Akhirnya, kami membuat penambahbaikan terhadap sistem-kripto Rabin menggunakan strategi penyulitan daripada AA_{β} algoritma dan seterusnya menjalankan eksperimen untuk mengukur tahap kecekapannya.

ACKNOWLEDGEMENTS

First of all praise to the almighty ALLAH S.W.T for His blesses and merciful those enable me to enrich my knowledge. I am sincerely grateful to my supervisor, Assoc. Prof. Dr. Muhammad Rezal Kamel Ariffin, for his patience and kindness for supervising me and his willingness to share his knowledge. Sincere appreciation to my co-supervisors, Assoc. Prof. Dr. Mohd. Rushdan Md. Said for giving advice on my research.

To my lovely wife Mrs. Nor Hafizah Mohd and my dearest son Muhammad Asyraf Ziqri, a lot of thanks and love for giving me soul, energy and moral boast to complete this journey. To my parents, family and lecturers, thank you very much for giving continuous moral support. Also to my friends, thanks for supporting me along this journey.

I wish to thank Universiti Putra Malaysia especially Institute for Mathematical Research for providing good research environment. Last but not least, a lot of appreciation to Ministry of Higher Education (MOHE) Malaysia for encouragement and financial support.

Thanks for this amazing journey.May Allah S.W.T blessing all of you. Wassalam.

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
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamad Rushdan Bin Md Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

_____

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

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.: _____

Declaration by Members of Supervisory Committee

I hereby 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:	_____	Signature:	_____
Name of Chairman of Supervisory Committee:	Assoc. Prof. Dr. Muhammad Rezal Bin KamelAriffin	Name of Chairman of Supervisory Committee:	Assoc. Prof. Dr. Mohamad Rushdan Bin Md Said

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advance Encryption Standard
DEHP	-	Diophantine Equation Hard Problem
DES	-	Data Encryption Standard
DLP	-	Descrete Log Problem
ECC	-	Elliptic Curve Cryptography
ECDLP	-	Elliptic Curve Discrete Logarithm Problem
ECDSA	-	Elliptic Curve Digital Signature Algorithm
gcd	-	Greatest Common Divisor
IFP	-	Integer Factorization Problem
RSA	-	Rivest-Shamir-Adlemen

CHAPTER 1

INTRODUCTION

In this modern era of the internet and telecommunication, security and privacy are the most common and essential words that we came across daily. It is because confidentiality has become one of the necessities of social life. Hence, this has created a need for a more secure communication channel for data transfers. In this context, several questions need to be considered. How can we transmit a message secretly without an unauthorized person obtaining knowledge about the message? How can the sender ensure that the message is transmitted to the intended receiver? How can the receiver ensure that the message is coming from the intended sender? The answer to the above questions is to ensure the communication channel is secure against adversary. One of the practical methods for performing information security is by utilizing cryptography.

Cryptography is a study of secret writing by altering the readable information into a different representation that unreadable [Samuel and Wagstaff, 2003]. Cryptography can be used to provide security for sensitive and confidential data from unauthorized user. It is about securing communication through insecure channel. An example of an insecure channel communication is the internet. Internet is the worldwide network channel used by the international community to share information with different interests and intentions. Based on Merkle, communication over the internet can be considered as communication over an insecure channel since an adversary may compromise it [Merkle, 1978]. Hence, there is a need to communicate securely over an insecure channel like the internet. The answer lies in cryptography.

Cryptography can be divided into symmetric-key cryptography and asymmetric-key cryptography. In symmetric-key cryptography, only one key is used to encrypt and decrypt data. To implement this type of cryptography, the key should be distributed and agree on the secret key before transmission between entities. The goal of the symmetric-key cryptography is to provide privacy between two parties that wish to communicate privately and on the same time an adversary knows nothing about the contents of the communication. The symmetric-key cryptography also called as private-key cryptography. The security of the symmetric-key cryptography is relies on the secret key. As long as the key remains secret means the communication remains secret. Examples of symmetric-key cryptography algorithms are RC2, DES, 3DES, RC5, Blowfish and AES, which use certain size of keys. The advantages of the symmetric-key cryptography are the key size for symmetric-key cryptosystem is smaller than the key size of asymmetric-key cryptography and in terms of the practical computational speed of its underlying operations, the symmetric-key cryptography is faster than asymmetric-key cryptography. However, the disadvantage of the symmetric-key cryptography is the key distribution problem between entities and authentication issues which the identity of both entities cannot be verified.

Another type of cryptography is called as asymmetric-key cryptography. In asymmetric-key cryptography, a pair of keys which are a public key and a private key is used for each entity. The public key is used for encryption process and the private key is used for

decryption process. Asymmetric-key cryptography is also known the public-key cryptography. The security of the asymmetric-key cryptography is relies on the hard mathematical problem of the algorithm. Examples of well known hard mathematical problem are Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP) and Elliptic Curve Discrete Logarithm Problem (ECDLP).Examples of asymmetric-key cryptography algorithms are RSA, Rabin, El-Gamal and ECC, which use certain size of keys. As an advantage, the disadvantages of the symmetric-key cryptosystem aresolvable by using the asymmetric-key cryptography. However, the disadvantage of the asymmetric-key cryptography is the practical computational speed is relative slow when compared to symmetric-key cryptosystem.

1.1 RSA Cryptosystem

The RSA algorithm is named after its inventors Ron Rivest, Adi Shamir and Len Adlemen [Rivest, Shamir and Adlemen, 1978]. It can be used for both public key encryption and digital signatures. As for the world renowned RSA cryptosystem, the inability to find e-th root of the ciphertext C modulo N from the congruence relation $C \equiv M^e \pmod N$ coupled with the inability to factor $N = pq$ for large primes p and q is its fundamental source of security [Rivest *et al.*, 1978]. Up to now, the most efficient algorithm for determining the proper factors of a given large number is the Quadratic Sieve with running time of $O(e^{\sqrt{(\log N)\cdot(\log\log N)}})$ where the running time is depends on the size of the integer N. In the RSA, case of the size of the product of two prime numbers p and q should be of at least 1024 bits where the size of two prime numbers p and q is 512 bits respectively. The RSA cryptosystem has a textbook complexity order of $O(n^3)$ or via Fast Fourier Transform $(n^2 \log n)$ for encryption and decryption operation. We denote n as the minimum security parameter of RSA algorithm.

The RSA cryptosystem uses computations in $\mathbb{Z}_N$, where N is the product of two distinct odd primes$p$ and q, of roughly equal size, k bits, and thegeneration of random exponent, e. It holds that $de \equiv 1 \pmod{\emptyset(N)}$, where $\emptyset(N) = (p-1)(q-1)$. The pair$(N, e)$ become public keys and d become a private key. This is illustrated in Algorithm 1.1.1.

Algorithm 1.1.1: RSA key generation
INPUT: The size k bits of the prime numbers.
OUTPUT: A public key pair (e, N) and private key (d).

1. Generate two random prime number k-bit size, p and q
2. Compute $N = p \cdot q$.
3. Compute $\emptyset(N) = (p-1)(q-1)$.
4. repeat
   Pick random integer e,
   until $\gcd\big(e, \emptyset(N)\big) = 1$.
5. Compute $d \equiv e^{-1} \bmod(\emptyset(N))$.
6. Return public key (N, e) and private key (d).

Algorithm 1.1.2: RSA encryption
INPUT: The public key (N, e) and the plaintext M.
OUTPUT: The ciphertext C.
1. Read plaintext, $M \in N$.
2. Compute $C \equiv M^e \bmod(N)$.
3. Return ciphertext, C.

Algorithm 1.1.3: RSA decryption
INPUT: The private key (d) and the ciphertext C.
OUTPUT: The plaintext M.
1. Read ciphertext, C.
2. Compute $M \equiv C^d \bmod(N)$.
3. Return plaintext, M.

The encryption and decryption operations are given in Algorithm 1.1.2 and Algorithm 1.1.3 respectively. To show that encryption and decryption are inverse operations, since$de \equiv 1 \ (\mathrm{mod}\emptyset(N))$, we have that

$$de = 1 + t\emptyset(N)$$

for some integer $t \geq 1$. Suppose that $M \in \mathbb{Z}_N$, then we have

$$\begin{aligned}(M^e)^d &\equiv M^{1+\, t\emptyset(N)}(\mathrm{mod}N)\\ &\equiv M^1 \cdot M^{t\emptyset(N)}(\mathrm{mod}N)\\ &\equiv M \cdot 1^t(\mathrm{mod}N)\\ &\equiv M(\mathrm{mod}N)\end{aligned}$$

as desired.

1.2 Rabin Cryptosystem

The Rabin cryptosystem is named after its inventor, Micheal O. Rabin in 1979 [Rabin, 1979]. It has been developed in an effort to improve the already existing RSA cryptosystem, by presenting a cryptographic solution whose security was mathematically proven to be based on the difficulty of the Integer Factorization Problem (IFP) coupled with the square root modulo problem. It is said to be an optimal implementation of RSA with the fix encryption exponent $e = 2$. However, the situation of a 4-to-1 mapping during decryption has deterred it from being utilized. Mechanisms to overcome the problem to ensure its possible implementation have been proposed like redundancy in the message method by Menezes *et al.* in 1996, extra bits method by Kurosawa *et al.* in 2001 and Williams's method by Williams in 1980. However these solutions either still have a possible decryption failure or lose their computational advantages. The Rabin cryptosystem has a textbook complexity order of $O(n^2)$ or via Fast Fourier Transform $O(n \log n)$ for encryption operation and complexity order of $O(n^3)$ or via Fast Fourier Transform $O(n^2 \log n)$ for decryption operation. We denote n as the minimum security parameter of Rabin algorithm.

The Rabin cryptosystem uses computations in $\mathbb{Z}_N$, where N is the product of two distinct odd primes p and q that satisfy the condition $p, q \equiv 3 \pmod 4$, of roughly equal size, k bits, and the exponent, $e = 2$. The pair (N, e) become public keys and p and q become a private keys. This is illustrated in Algorithm 1.2.1.

Algorithm 1.2.1: Rabin key generation
INPUT: The size k bits of the prime numbers.
OUTPUT: A public key pair (e, N) and private key pair (p, q).
1. Generate two random prime number k-bit size, p and q, that satisfy $p \equiv q \equiv 3 \pmod 4$.
2. Compute $N = pq$.
3. Return public key (N, e) and private key pair (p, q).

Algorithm 1.2.2: Rabin encryption
INPUT: The public key (N, e) and the plaintext M.
OUTPUT: The ciphertext C.
1. Read plaintext, $M \in N$.
2. Compute $C \equiv M^2 \bmod(N)$.
3. Return ciphertext, C.

Algorithm 1.2.3: Rabin decryption
INPUT: The private key pair (p, q) and the ciphertext C.
OUTPUT: The plaintext M.
1. Read ciphertext, C.
2. Computes the square roots of C modulo the primes p and q,

$$\pm M_p \equiv C^{\frac{p+1}{4}} \pmod p$$
$$\pm M_q \equiv C^{\frac{q+1}{4}} \pmod q$$

3. By using the Chinese Remainder Theorem to compute the original message.

$$M \equiv M_p q q^{-1} + M_q p p^{-1} \pmod N$$
$$M \equiv -M_p q q^{-1} + M_q p p^{-1} \pmod N$$
$$M \equiv M_p q q^{-1} - M_q p p^{-1} \pmod N$$
$$M \equiv -M_p q q^{-1} - M_q p p^{-1} \pmod N$$

4. From 4 possibilities M, recipient somehow determines the correct message.
5. Return plaintext, M.

The encryption and decryption operations are given in Algorithm 1.2.2 and Algorithm 1.2.3 respectively. The details of the Rabin cryptosystem and its improvement methods will be described in Chapter 6.

1.2.1 Security Reduction for Rabin

We put forward here a known security reduction involving the Rabin cryptosystem. Suppose $N = pq$ is the product of 2 large primes and we know the 4 solutions

$$x \equiv \pm a, \pm b \; of \; x^2 \equiv y (\mathrm{mod}\, N)$$

From this argument we can see that either $x \equiv b (\mathrm{mod}\, p)$ and $x \equiv -b (\mathrm{mod}\, q)$. This means, $p|(a-b)$ but $q \nmid (a-b)$. This means, $\gcd(a-b, N) = p$ and we have factored N. Then finding any two solution a and b such that $a \not\equiv \pm b (\mathrm{mod}\, N)$ is computationally equivalent to factoring N.

Proposition 1.2.1 *Suppose $N = pq$ is the product of 2 large primes. The product $N = pq$ is able to be factored if and only all 4 square roots of $x^2 \equiv y (mod\, N)$ are known.*

Proof.
$\Rightarrow$
If the product $N = pq$ is factored then all 4 square roots of $x^2 \equiv y (\mathrm{mod}\, N)$ can be found via the Chinese Remainder Theorem.

$\Leftarrow$
If any two solution a and b such that $a \not\equiv \pm b (\mathrm{mod}\, N)$ are found, then we have either $\gcd(a \pm b, N) = p$ or $\gcd(a \pm b, N) = q$.■

As such, any asymmetric scheme based upon the Rabin primitive would inherit the above characteristics.

1.2.2 Rabin Primitive

We classify any asymmetric scheme that utilizes the square root problem together with the difficulty to factor an integer N as a scheme that is built upon the Rabin primitive concept.

1.3 AA_{β} Cryptosystem[Ariffin*et al*, 2013]

In 2013, Ariffin *et al.* introduced a new asymmetric cryptosystem based on the Rabin primitive that is it depended on the hardness of factoring integers of the shape $N = p^2q$ (instead of $N = pq$) and solving square roots modulo $N = p^2q$, known as AA_{β}. This cryptosystem uses a combination of modular linear and modular squaring in their scheme. The hardness of factoring $N = p^2q$ has been used in many systems such as the Okamoto-Uchiyama's scheme [Okamoto, 1998] and the Schmidt-Samoa' system [Schmidt, 2006]. However, both schemes use large encryption exponent. It will cause the complexity order for encryption operation to be $O(n^3)$. For example, the encryption operation for Okamoto-Uchiyama's scheme is $C \equiv g^M h^r \pmod N$ and Schmidt-Samoa' scheme is $C = M^N \pmod N$.

In the work by Ariffin *et al.* in 2013, they managed to show how to efficiently design an asymmetric cryptosystem based on the hardness of factoring $N = p^2q$ where p and q are unknown parameters. They also show that in the AA_β scheme the situation of a 4-to-1 mapping during decryption does not exist which a great advantage over Rabin's cryptosystem. The AA_β cryptosystem has a complexity order faster than RSA and ECC for speed of encryption operation. However, for decryption operation, its speed is better than RSA and is marginally behind ECC. Due to its construction utilizing simple mathematical structure, the AA_β cryptosystem has low computational requirements and computing power to deploy secure communication procedures efficiently. It is also the reason why AA_β cryptosystem had speeds faster than RSA and ECC. There are five reasons or motivation in designing AA_β cryptosystem by Ariffin *et al.* in 2013:

i. Shorter key length. If possible shorter than ECC 160-bits.
ii. Speed. To have speed of complexity order $O(n^2)$ or by using FFT implementation of $O(n \log n)$ for both encryption and decryption operation.
iii. Able to increase data size to be transmitted asymmetrically. That is, not to be restricted in size because of the mathematical structure.
iv. To be IND-CCA2 secure in the standard model.
v. Simple mathematical structure for easy implementation.

We will now illustrate the key generation, encryption and decryption operation of AA_β cryptosystem in Algorithm 1.3.1, Algorithm 1.3.2 and Algorithm 1.3.3 respectively.

Algorithm 1.3.1: $\boldsymbol{AA_\beta}$ key generation
INPUT: The size $\boldsymbol{k}$ bits of the prime numbers.
OUTPUT: A public key tuple$(\boldsymbol{k, A_1, A_2})$ and private key tuple$(\boldsymbol{p, q, d})$.

1. Generate two random and distinct $\boldsymbol{k}$-bit strong primes $\boldsymbol{p}$ and $\boldsymbol{q}$, such that $\boldsymbol{p, q \equiv 3 \pmod 4}$ where $\boldsymbol{2^k} < p, q < \boldsymbol{2^{k+1}}$.
2. Choose random $\boldsymbol{d}$ such that $\boldsymbol{d} > (\boldsymbol{p^2 q})^{\frac{4}{9}}$.
3. Compute integer $\boldsymbol{e}$ such that $\boldsymbol{ed \equiv 1 \pmod{pq}}$ and add multiples of $\boldsymbol{pq}$ until $\boldsymbol{2^{3k+4}} < e < \boldsymbol{2^{3k+6}}$ (if necessary).
4. Set $\boldsymbol{A_1 = p^2 q}$. We have $\boldsymbol{2^{3k}} < \boldsymbol{A_1} < \boldsymbol{2^{3k+3}}$.
5. Set $\boldsymbol{A_1 = e}$.
6. Return public key tuple $(\boldsymbol{k, A_1, A_2})$ and private key tuple $(\boldsymbol{p, q, d})$.

Algorithm 1.3.2: $\boldsymbol{AA_\beta}$ encryption
INPUT: The public key tuple $(\boldsymbol{k, A_1, A_2})$ and the message $\boldsymbol{M}$.
OUTPUT: The ciphertext $\boldsymbol{C}$.

1. Message is an integer $\boldsymbol{M = m_1 \cdot 2^{2k-1} + m_2}$ with the following condition for the pair $(\boldsymbol{m_1, m_2})$, $\boldsymbol{2^{4k}} < \boldsymbol{m_1} < \boldsymbol{2^{4k+1}}$ and $\boldsymbol{2^{2k-2}} < \boldsymbol{m_2} < \boldsymbol{2^{2k-1}}$.
2. Compute $\boldsymbol{C = A_1 m_1 + A_2 m_2{}^2}$.
3. Return ciphertext $\boldsymbol{C}$.

Algorithm 1.3.3: $\boldsymbol{AA_{\beta}}$ decryption
INPUT: The private key tuple $(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{d})$ and the ciphertext $\boldsymbol{C}$.
OUTPUT: The message $\boldsymbol{M}$.

1. Compute $\boldsymbol{W \equiv Cd \pmod{pq}}$.
2. Proceed to solve $\boldsymbol{W}$ as in Chapter 2, Lemma 2.2.12 to obtain a list $\boldsymbol{m_{2_i}}$for $\boldsymbol{i = 1, 2, 3, 4}$.
3. For $\boldsymbol{i = 1, 2, 3, 4}$ compute $\boldsymbol{m_{1_i} = \frac{C - m_{2_i}{}^2 A_2}{A_1}}$.
4. Sort the pair $(\boldsymbol{m_{1_i}, m_{2_i}})$ for integer $\boldsymbol{m_{1_i}}$.
5. Return the message $\boldsymbol{M = m_1 \cdot 2^{2k-1} + m_2}$.

The AA_{β} cryptosystem has a complexity order of $O(n^2)$ or via Fast Fourier Transform $O(n \log n)$ for encryption operation and complexity order of $O(n^3)$ or via Fast Fourier Transform $O(n^2 \log n)$ for decryption operation. We denote n as the minimum security parameter of AA_{β} algorithm. The details of mathematical structure proof of AA_{β} cryptosystem will be described in Chapter 2.

1.4 Asymptotic Notation – Running times of algorithm

Efficiency of the algorithm can be measured in terms of the complexity of algorithm. But, the whole idea of complexity is to measure the behavior of the algorithm when n, the number of bits input is very large. Let us review some standard notation for relating the rate of growth of functions [Shoup, 2005]. This notation will be useful in discussing the running time of algorithms.

Definition 1.4.1 *Suppose x is a variable taking positive integer and let g denote a real-valued function in x that is positive for all sufficiently large x. Let f denote any real-valued function in x. Then:*

- $f = O(g)$ *means that* $|f(x)| \leq cg(x)$ *for some positive constant c as* $x \to \infty$ *(read, "f is big-O of g").*
- $f = \Omega(g)$ *means that* $f(x) \geq cg(x)$ *for some positive constant c as* $x \to \infty$ *(read, "f is big-Omega of g").*
- $f = \Theta(g)$ *means that* $cg(x) \leq f(x) \leq dg(x)$ *for some positive constant c and d as* $x \to \infty$ *(read, "f is big-Theta of g").*
- $f = o(g)$ *means that* $f/g \to 0$ *as* $x \to \infty$ *(read, "f is little-o of g").*
- $f \sim g$ *means that* $f/g \to 1$ *as* $x \to \infty$ *(read, "f is asymptotically equal to g").*

For the following definitions, let $A, B \in \mathbb{Z}$ and a is the number of bit length of A in base 2, while b is the number of bit length of B in base 2.

Definition 1.4.2 *Computing* $A + B$ *or* $A - B$ *where* $A > B$ *has time complexity* $O(a)$ *or* $O(\log(A))$ *where* a *is the number of digits of A in base two.*

Definition 1.4.3 *Computing* $A \cdot B$ *or* A/B *has time complexity* $O(a \cdot b)$ *or* $O(\log(A) \cdot \log(B))$. *When* $b = O(a)$, *the time complexity is* $O(a^2)$ *or* $O(\log(A)^2)$.

Definition 1.4.4 *Computing Euclidean and Extended Euclidean* $A = Bq + r$ *has time complexity identical to that for computing* $A \cdot B$*, that is* $O(a \cdot b)$ *or* $O(\log(A) \cdot \log(B))$*. When* $b = O(a)$*, the time complexity is* $O(a^2)$ *or* $O(\log(A)^2)$*.*

Definition 1.4.5 *Computing modular multiplication* $A \cdot B \pmod N$ *it is typical and assumed unless otherwise stated that* $a = O(n)$ *and* $b = O(n)$*. It follows that the time complexity is* $O(n^2)$ *or* $O(\log(N)^2)$*.*

Definition 1.4.6 *Computing modular exponentiation* $A^B \pmod N$ *with* $B > 0$ *requires at least* $\log_2(B)$ *modular multiplications and less than* $\frac{3}{2} \cdot \log_2(B)$ *using square and multiply. It thus has time complexity* $O(n^2 \cdot b)$ *or* $O(\log(N)^2 \cdot \log(B))$*. When* $b = O(n)$*, the time complexity is* $O(n^3)$ *or* $O(\log(N)^3)$*.*

1.5 Research Motivation

Since AA_β cryptosystem is a new cryptosystem, to determine whether it is on a par with well-known as RSA and ECC cryptosystem or not, we need to carry out a comparative analysis based on the performance of the RSA, ECC and AA_β. Then, from that we will know how good and efficient AA_β compared to RSA and ECC as claimed by Ariffin *et al.*. This comparative analysis is important to determine the practicality of AA_β cryptosystem that will be used in the future as one of the preferred public key systems.

Currently, from Algorithm 1.3.3 AA_β decryption operation, in the second step we need to find a solutions for square roots of W modulo the primes p and q,

$$\pm M_p \equiv W^{\frac{p+1}{4}} \pmod p$$
$$\pm M_q \equiv W^{\frac{q+1}{4}} \pmod q.$$

Then, from four solutions $+M_p, -M_p, +M_q$ and $-M_q$ above, by using the Chinese Remainder Theorem we will have four solutions for equation $V^2 \equiv W \pmod{pq}$ which are

$$m_{2_1} \equiv M_p q q^{-1} + M_q p p^{-1} \pmod{pq}$$
$$m_{2_2} \equiv -M_p q q^{-1} + M_q p p^{-1} \pmod{pq}$$
$$m_{2_3} \equiv M_p q q^{-1} - M_q p p^{-1} \pmod{pq}$$
$$m_{2_4} \equiv -M_p q q^{-1} - M_q p p^{-1} \pmod{pq}$$

With four values of m_2, we will find the value of m_1 by computing $m_{1_i} = \frac{C - {m_{2_i}}^2 A_2}{A_1}$ from $i = 1,2,3,4$. Finally, we need to determine which pair of m_{1_i} and m_{2_i} are an integer. From that, we will get back the original plaintext. As we can see, in order to find the value of m_1, we need to compute $m_{1_i} = \frac{C - {m_{2_i}}^2 A_2}{A_1}$ for four time. Therefore, it is essential if we can reduce the number of step to find the value of m_1 by computing

$m_{1_i} = \frac{C - m_{2_i}{}^2 A_2}{A_1}$ from four times to three, two or just once if possible. By doing that, the time to complete the decryption operation can be decreased and automatically the speed can be increased.

According to Ariffin *et al.*, the AA_{β} cryptosystem is a redesign of Rabin cryptosystem which overcome the decryption failure problem. Therefore, we conjecture that the methods utilized by Ariffin *et al.* to efficiently designing AA_{β}, can also be utilized for the Rabin cryptosystem to overcome its decryption failure.

1.6 Problem Statements

Four main questions lead us to the research objectives:

i. Is the AA_{β} public key cryptosystem practically implementable or not?
ii. How fast is AA_{β} public key cryptosystem compared to RSA and ECC cryptosystem?
iii. How do we enhance the AA_{β}? That is, to reduce the complexity time of AA_{β} encryption/decryption time?
iv. Can we overcome Rabin cryptosystem decryption failure using mechanisms from the AA_{β} cryptosystem?

1.7 Research Objectives

This research is conducted to achieve the following objectives:

i. To justify whether the AA_{β} public key cryptosystem is practically implementable or not,
ii. To provide a comparative performance analysis of the AA_{β} public key cryptosystem against well known asymmetric cryptosystem like RSA and ECC,
iii. To enhance the performance of running time of the AA_{β} decryption process with the mathematical proof and
iv. To overcome the Rabin cryptosystem decryption failure using similar mechanism from the AA_{β} cryptosystem.

1.8 Scope and Limitation of the Study

In our research, we are intending to cover two scopes. Firstly, the practical implementation and comparative performance analysis of the AA_{β} public key cryptosystem against the most popular public key cryptosystem like RSA and ECC. We will provide the details about the designing and implementation protocol to conduct the experiment to achieve the purposes of the first scope. As the conclusion for the first scope worked, we will provide analysis of the results. The second scope of our research, we will enhance the running time performance of the AA_{β} decryption process and enhance the Rabin cryptosystem to overcome decryption failure. In this work, we will provide the mathematical proof on how the enhancement is going to work.

1.9 Overview of the Thesis

We organize this thesis into seven chapters. In Chapter 2, we will present our literature review on the research study and mathematical background to construct the AA_β public key cryptosystem. In Chapter 3, we will describe the research methodology on the comparative analysis among AA_β, RSA and ECC has been conducted. Next, we will describe the comparative performance analysis of AA_β public-key cryptosystem with RSA and ECC cryptosystem in Chapter 4. In Chapter 5, we will describe an enhancement of the AA_β decryption procedure. In Chapter 6, we will introduce the new efficient method of Rabin cryptosystem. In Chapter 7, we conclude the thesis by summarizing all the works and results obtained and provide some suggestions for future works in the final chapter of this thesis.

REFERENCES

Abu, N.A., Zahari, N.A. and Zakaria, I.Z. The Simulation of 256-bit Elliptic Curve Cryptosystem.

Al-Kayali, Ahmed Khaled, M. 2004.Elliptic Curve Cryptography and Smart Cards.*SANS Institute*.

Ariffin, M. R. K., 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*, Vol.7(S): 19-37.

Creado, O.M., Wang, Y., Wu, X., Le, P.D. 2009. Probabilistic encryption - A practical implementation.In *Proceedings of the Fourth International Conference on Computer Sciences and Convergence Information Technology*, 1130-1136.IEEE Computer Society, Los Alamitos CA USA.

Creado, O.M., Wang, Y., Wu, X., Le, P.D. 2009. Probabilistic encryption - A comparative analysis against RSA and ECC.In *Proceedings of the Fourth International Conference on Computer Sciences and Convergence Information Technology*, 1123-1129.IEEE Computer Society, Los Alamitos CA USA.

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

Digital Signature, Web02 from*http://en.wikipedia.org/wiki/Digital_signing*

Feistel, H. 1973. Cryptography and Computer Privacy.*Scientific American*, vol. 228(5): 15-23.

Feistel cipher, Web01 from *http://en.wikipedia.org/wiki/Feistel_cipher*

Galbraith, S.D. 2012. Mathematics of Public Key Cryptography.In *The RSA and Rabin Cryptosystem*, 507– 541.Cambridge University Press 2012.

Gilbert, S. V. 1926. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, XLV: 109–115.

Giry, D. 2009. Cryptographic Key Length Recommendations.BlueKrypt - NIST, [cited July 10, 2009],*http://www.keylength.com/en/4/.*

Goldwasser, S. and S. Micali. 1984. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28(2): 270-299.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008a.An introduction to cryptography.In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 1– 6. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008b.The ElGamal public key cryptosystem. In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 68–71. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008c.Integer Factorization and RSA. In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 113–188. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008d.Elliptic Curves and Cryptography. In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 279–348. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008e.Discrete logarithms and Diffie-Hellman. In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 59–104. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008f. Hash functions. In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 466–468. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008g.An introduction to cryptography.In *An Introduction to Mathematical Cryptography* (eds. S. Axler and K. A. Ribet), 1– 58. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008h.An introduction to cryptography.In *Integer Factorization and RSA* (eds. S. Axler and K. A. Ribet), 113– 188. New York: Springer Science+Bussiness Media.

Hoffstein, J., Pipher, J. and Silverman, J. H. 2008i.An introduction to cryptography.In *Elliptic Curves and Cryptography* (eds. S. Axler and K. A. Ribet), 279– 348. New York: Springer Science+Bussiness Media.

Hoffstein, J., Lieman, D., Pipher, J. and Silverman, J. H. Web04. 2006. NTRU: A Public Key Cryptosystem. http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU1

Katz, J. and Lindell, Y. 2008. AES - The Advanced Encryption Standard. In *Introduction To Modern Cryptography*, 185-187. CRC Press.

Koblitz, N. 1987.Elliptic Curve Cryptosystems.*Mathematics of Computation* 48: 203–209.

Kurosawa, K., Itoh, T., and Takeuchi, M. 1994.Public Key Cryptosystem Using a Reciprocal Number with the Same Intractability as Factoring a Large Number.*CRYPTOLOGIA XII*, 225 – 233.

Lenstra, A.K. and E.R. Verheul, 2001.Selecting Cryptographic Key Sizes.*Journal of Cryptology*, 14(4): 255-293.

Mark, S. and Richard, M. L. 2007.Feistel Cipher. In *Applied Cryptanalysis*, 131 – 132.

Menezes, A., Oorschot, P. and Vanstone, S. 1997. Number-theoretic reference problem. In *Handbook of Applied Cryptography* (ed. K. Rosen), 87–132. CRC Press.

Menezes, A.J., van Oorschot, P.C. and Vantone, S.A. 1996a, *Handbook of applied cryptography,* CRC Press 1996.

Menezes, A.J., van Oorschot, P.C. and Vantone, S.A. 1996b. Handbook of applied cryptography.In *Public Key Encryption*, 283– 319.CRC Press 1996.

Merkle, R. C. 1978. Secure Communications over Insecure Channels. *Communications of the ACM21 (4)*: 294–299.

Mersin, A. 2007. The Comparative Performance Analysis of Lattice Based NTRU Cryptosystem with Other Asymmetrical Cryptosystems. Master thesis.Izmir Institute of Technology.

Rabin, M. 1979. Digitalized signature as intractable as factorization.*Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science*.

Rivest, R. L., Shamir, A. and Adleman, L. 1978.A method for obtaining digital signatures and public-key cryptosystems.*Commun. ACM* 21: 120–126.

Rosen, K. H. 2005. Primes and greatest common divisors.In *Elementary Number Theory and Its Applications*, 5th edn. (ed. K. Guardino), 67–133. Pearson.

RSA Laboratories, Web03 from*http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and-disadvantages.htm*

Samuel, S., Wagstaff, Jr. 2003. Random Number Generation.In *Cryptanalysis of Number Theoretic Ciphers*, 211-218.CRC Press.

Samuel, S., Wagstaff, Jr. 2003. Terminology in Cryptography.In *Cryptanalysis of Number Theoretic Ciphers*, 3-12.CRC Press.

Shannon, C. E. 1949. Communication Theory of Secrecy Systems.*Bell System Technical Journal*, vol.28-4: 656-715.

Stallings, W. 2005a.Classical encryption techniques.In *Cryptography and Network Security Principles and Practices,* 4th edn. (ed. T. Dunkelberger), 28–56. Prentice Hall.

Stallings, W. 2005b.Introduction.In *Cryptography and Network Security Principles and Practices*, 4th edn. (ed. T. Dunkelberger), 6–25. Prentice Hall.

Tata, E. 2007.Elliptic Curve Cryptography, An Implementation Guide. In *Anoop MS*.

Trappe, W. and Washington, L. C. 2005a.Basic number theory. In *Introduction to Cryptography with Coding Theory*, 2nd edn., 63–112. Pearson Prentice Hall.

Trappe, W. and Washington, L. C. 2005b.Overview of cryptography and its applications. In *Introduction to Cryptography with Coding Theory*, 2nd edn., 1–12. Pearson Prentice Hall.

Williams, H. C., 1980. A Modification of the RSA Public Key Encryption Procedure.*IEEE Trans. Inf. Theory 26, no. 6*.