CONTINUED FRACTIONS AND CRYPTOGRAPHIC APPLICATIONS

A DISSERTATION

SUBMITTED TO THE FACULTY OF SCIENCE,
UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG,
IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE
OF

MASTER OF SCIENCE
IN
MATHEMATICS

Submitted by

PRIYANKA SOOKRAJ (1092832)

Under the supervision of

DR. DARLISON NYIRENDA

SCHOOL OF MATHEMATICS
UNIVERSITY OF THE WITWATERSRAND
NOVEMBER, 2022

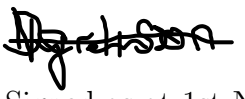
Declaration

I declare that this dissertation is my own, unaided work. It is being submitted for the degree of Master of Science at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.

Candidate signature:

Signed as at 1st November 2022.

Supervisor signature:



Signed as at 1st November 2022.

Acknowledgements

I have so much gratitude in my heart, which I would like to express. My journey towards writing up my dissertation would not have been possible without the angels, heroes and guides who shone their lights and helped me through the crests and troughs, in some way or another. First and foremost, I would like to express gratitude to my parents, who have supported and encouraged me from the very beginning. Nothing would have been possible without their love and guidance. I am also grateful to my brother, Nikhil and sister, Shakti for their motivation and for lending a listening ear whenever I needed it. I am extremely grateful to my supervisor, Dr Darlison Nyirenda for his valuable insights, probing questions, in-depth explanations, guidance and support that has helped me see my write-up to fruition. I am also extremely grateful to the University of the Witwatersrand for funding my studies via the Postgraduate Merit Award, as well as the National Research Foundation for granting a bursary to me in my second year of masters. I would also like to express gratitude to my coach, Jeremy Peters, my mentor, Faith Zottor and my guides, Renee Macaulay, Sashlin Reddy and Donald Miller, who have all been key sources of inspiration and from whom I have learnt so much from. Last, but not least, a special thanks goes out to my friends Jeanne Bamukunde, Sriya Beharie, Ruwayda Nicholson, Nokwanda Mnguni and Akua Afrane-Okese for being there for me, cheering me on and giving me solid advice whenever I needed it. All of you are my anchors and my pillars of strength. I greatly appreciate each and every one of you.

Abstract

In this dissertation, Michael J. Wiener's proposed attack on short secret exponents used in the RSA cryptosystem is studied and thus an application of continued fractions in the cryptanalysis is highlighted. Furthermore, some variants and improvements to the attack proposed by A. Dujella, M. Bunder and J. Tonien are studied.

Contents

Candidate's Declaration i

Acknowledgements ii

Abstract iii

Content iv

1 INTRODUCTION 1

2 PRELIMINARIES 3
2.1 Some important number theoretical theorems 3
2.2 The RSA cryptosystem 4
2.3 Finite continued fractions 6
2.4 Convergents 7
2.5 A cryptosystem based on continued fractions 18

3 WIENER'S ATTACK 20
3.1 Application of continued fractions 20
3.2 Wiener's algorithm 21
3.3 Wiener's algorithm applied to RSA 28

4 A VARIANT ON WIENER'S ATTACK 31
4.1 A further look at Wiener's attack 31
4.2 Verheul and Van Tilborg variant of Wiener's attack 34

5 IMPROVEMENT TO WIENER'S ATTACK 48
5.1 The method 48

6 CONCLUSION 61

A A code for Wiener's algorithm in SageMath 62

Chapter 1

INTRODUCTION

Cryptology is a 3000-year-old science of secret communications, initially important to just soldiers at war, secret government agencies, spies and secret lovers. Today, our computers, mobile devices, wi-fi security and machines have cryptology embedded within.

The two components of cryptology are cryptography (techniques for creating systems of secret writing) and cryptanalysis (techniques for breaking systems of secret writing). Over all these years that cryptography has existed, there have always been hackers who attempt to recover private messages not meant for their eyes. A formal term for such hackers would be cryptanalysts. Because of such attacks, cryptography also involves designing systems that are secure enough to convey secret messages via communication channels. For the past 2500 years, cryptologists have developed numerous types of cryptosystems to hide messages, followed by a rich vocabulary to describe them.

Codes and ciphers are at the heart of cryptography, in which algorithms for encryption, decryption and key-generation embody the cryptosystems in use. Cryptology was even considered to be a form of magic in the European middle ages [4], an art if you will, which required creativity and personal skill to mold. There were hardly any theoretical notions behind the creation of good codes back then. It was reserved just for talented artists who could create them.

However, in the late 20th century, the picture of cryptology rapidly transformed from being an art to a science, having many mathematical applications behind the array of algorithm constructions. Many of these mathematical applications stem from Number Theory, Algebra and Group Theory. Today, cryptography is a science that has the ability to secure systems used across the globe.

Furthermore, the field of cryptography encompasses so much more than just secret communications in this day and age. This field now also deals with message authentication, digital signatures, electronic auctions, protocols for exchanging secret keys, digital cash and more. Such systems of software protection methods employ encryption authentication and other tools to prevent thieves from extracting private information from stolen laptops and enforce access control in multi-user operating systems.

It is amazing to think that in the 1500s, encrypted messages were solely embedded in hand-written letters. These days, much of the cryptography in use is invisible. If you log in to a computer, you have cryptography in the form of a one-way hash function which protects your password behind the scenes, you have a symmetric key algorithm ensuring

safety whilst you finish your online transactions and there is public-key cryptography involved in setting up the encrypted network connection between you and your colleagues on that Microsoft Teams meeting. One could say that the magic of cryptography is still alive in its ability to make an impact without being seen.

In this dissertation, we unpack the magic. Today, we have thousands of implemented cryptosystems, such as RSA, Elgamal and the Goldwasser-Micali public key cryptosystem, to name a few. Particularly, the focus on the use of continued fractions in cryptanalysis of the RSA cryptosystem forms the basis of the study.

Chapter Two touches on preliminaries that provide tools to be used in the dissertation. Chapter Three focuses on a discussion of Wiener's algorithm for cryptanalysis of short RSA secret exponents [22]. Chapter Four discusses a variant to Wiener's attack [5]. Chapter Five focuses on a new attack on the RSA cryptosystem based on continued fractions [2].

Chapter 2

PRELIMINARIES

2.1 Some important number theoretical theorems

In this section, we look at some fundamental theorems [7], [15] that are key for Chapters 2 to 5. Note that (a, b) will denote the greatest common divisor of integers a and b.

The following theorem due to Fermat is called Fermat's Little Theorem.

Theorem 2.1.1 (Fermat).
Let p be a prime and a be any integer. Then $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.

Using Fermat's Little Theorem, we can prove the theorem below.

Theorem 2.1.2 (Euler).
Let p and q be distinct primes and let $G = (p-1, q-1)$. Then $a^{(p-1)(q-1)/G} \equiv 1 \pmod{pq}$ for all a satisfying $(a, pq) = 1$.

Proof: By assumption, we know that p does not divide a and that G divides $q-1$. Using Fermat's Little Theorem and the fact that $\frac{(q-1)}{G}$ is an integer gives

$$\begin{aligned} a^{(p-1)(q-1)/G} &= (a^{p-1})^{\frac{(q-1)}{G}} \\ &\equiv 1^{\frac{(q-1)}{G}} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

The exact same computation, reversing the roles of p and q, shows that

$$a^{(p-1)(q-1)/G} \equiv 1 \pmod{q}.$$

Thus $a^{(p-1)(q-1)/G} - 1$ is divisible by both p and q, hence it is divisible by pq. ■

Theorem 2.1.3 (Euler).
If m is a positive integer and a is an integer with $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof: Let $r_1, r_2, \ldots, r_{\phi(m)}$ denote the reduced residue system made up of the positive integers not exceeding m that are relatively prime to m. Then the set $ar_1, ar_2, \ldots, ar_{\phi(m)}$ is also a reduced residue system modulo m. Hence, the least positive residues of $ar_1, ar_2, \ldots, ar_{\phi(m)}$

must be the integers $r_1, r_2, \ldots, r_{\phi(m)}$. Consequently, if we multiply together all terms in each of these reduced residue systems, we obtain

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Thus,

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, we have $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

2.2 The RSA cryptosystem

With conventional secret-key cryptosystems, parties who would like to communicate must have their own secret keys. In public-key cryptosystems, the enciphering keys are made public for everyone to use. In a network of n individuals, each person produces a key and a directory of n keys is published. The RSA cipher system invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman is one of the most widely used public-key systems and is based on modular exponentiation. The procedure of RSA involves a public-private key generation, along with a designated encryption and decryption algorithm [18]. The following headings highlight the steps taken when making use of the RSA cryptosystem:

Public Key Generation: Suppose that Alice would like to make use of the RSA cryptosystem to receive private information from Bob. Firstly, Alice chooses two large prime numbers p and q. Then she proceeds to compute their product $n = pq$. Next, Alice computes the Euler totient function for n, namely

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

The Euler totient function represents the amount of numbers less than n and relatively prime to n. Alice then picks a number e at random, where $1 < e < \phi(n)$ and such that $(e, \phi(n)) = 1$. (Alice can determine if e and $\phi(n)$ are relatively prime by using the Euclidean Algorithm to compute the greatest common divisor of e and $\phi(n)$). The pair of numbers (e, n) is regarded as the public key, consisting of a modulus n and a public exponent e. Alice now publishes her public key (e, n) in a directory that is available to anyone who would like to send her a private message.

Private Key Generation: Since $(e, \phi(n)) = 1$, then e has a multiplicative inverse $(\text{mod } \phi(n))$, which we call d.
This means that $ed = 1 \pmod{\phi(n)}$ and so $d = e^{-1} \pmod{\phi(n)}$. The pair of numbers (d, n) is regarded as Alice's private key. As the name suggests, Alice does not share her private key (d, n) with anyone. Bob does the same computations and has his own pair of public and private keys.

Encryption: Suppose Bob wants to send a private message M to Alice. To encrypt a message in RSA, Bob needs to first convert the message M into a number, where $0 \leq M < n$. (Bob may need to break his message M into several parts in order to convert it to a number.) Bob then proceeds to retrieve Alice's public key (e, n) from the directory. Next, Bob computes $C = M^e \pmod{n}$. That is, he raises his message to the power e

and then reduces the product (mod n). The result is his ciphertext C. Bob sends this ciphertext C to Alice.

Decryption: To decrypt Bob's message, Alice uses her private key (d, n). Alice proceeds to compute $M = C^d \pmod{n}$ to retrieve the message that Bob sent.

Note: This decryption computation retrieves the message because of the following reasoning:

Firstly, recall Theorem 2.1.3, which states that if n is a positive integer and M is an integer with $(n, M) = 1$ then $M^{\phi(n)} \equiv 1 \pmod{n}$.
Secondly, note that since n is a product of two primes, the only possibility for (n, M) is $1, p, q$ or n, where the last case is precluded since we have assumed $0 \leq M < n$. The cases where $(n, M) = p$ or $(n, M) = q$ are analogous. So we have three cases to consider, namely $(n, M) = 1$ and $(n, M) > 1$.

Case 1: $(n, M) = 1$.
Since d is an inverse of e modulo $\phi(n)$, $ed \equiv 1 \pmod{\phi(n)}$. Then $ed = 1 + k\phi(n)$ for some integer k. Since $(n, M) = 1$, then by Theorem 2.1.3, $M^{\phi(n)} \equiv 1 \pmod{n}$. So for decryption, $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\cdot\phi(n)} \equiv M^1(M^{\phi(n)})^k \equiv M \cdot 1^k \equiv M \pmod{n}$.

Case 2: $(n, M) > 1$.
Assume that $(n, M) = p$. Then $p|M$ and so $M^{ed} \equiv 0 \equiv M \pmod{p}$.
That is, $M^{ed} \equiv M \mod p$. Now, $(n, M) = p$ with q a prime and $q \neq p$, implying that $(q, M) = 1$, so by Theorem 2.1.3, $M^{\phi(n)} \equiv 1 \pmod{q}$. So,
$M^{ed} \equiv M^{1+k\cdot\phi(n)} \equiv M^1(M^{\phi(n)})^k \equiv M \cdot 1^k \equiv M \pmod{q}$.
Furthermore, when $M = 0$, we have $(n, M) = (n, 0) = n > 1$, which then gives the same result as above.

At this point we have shown that $M^{ed} \equiv M \pmod{q}$ and $M^{ed} \equiv M \pmod{p}$. Thus by the Chinese Remainder Theorem, we have that $M^{ed} \equiv M \pmod{n}$.
It follows that $C^d \pmod{n} \equiv M^{ed} \equiv M \pmod{n}$ for Case 2 as well. A similar argument holds for $(n, M) = q$. ■

We now demonstrate the RSA cryptosystem with a short example

Example 1 Select two primes, $p = 5$ and $q = 11$. Compute $n = p \times q = 5 \times 11 = 55$. Compute $\phi(n) = (p-1)(q-1) = 4 \times 10 = 40$. Select e such that $(e, 40) = 1$. We choose $e = 7$. Determine d by computing $d = e^{-1} \pmod{40} = 7^{-1} \pmod{40}$, where $d < 40$. In this case $d = 23$ because $23 \times 7 = 161 = 1 \pmod{40}$. Publish the public key $(7, 55)$ and keep the private key $(23, 55)$ a secret. Using the public key, we proceed to encrypt a message, say $M = 3$. $C = 3^7 \pmod{55} = 42$. This is our ciphertext. Now, to decrypt, we take the ciphertext and undo the encryption $M = 42^{23} \equiv 3 \pmod{55}$. ■

The security of the RSA algorithm lies in two areas. First, while $n = pq$ is easy to compute, it is difficult to do the reverse when trying to determine what p and q are, given n. That leads to the other part of the security of RSA. The two prime numbers p and q must be very large primes such that their binary representations have about 500 bits or

more each. In Chapter 3, we will analyse how security is compromised when an attacker is able to retrieve p and q, as well as how attackers are able to retrieve a message by exploiting short public exponents and short RSA secret exponents.

2.3 Finite continued fractions

Definition 2.3.1 A finite continued fraction is an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

where $a_0, a_1, a_2, \ldots, a_n$ are all real numbers with $a_1, a_2, \ldots, a_n$ positive. The real numbers $a_1, a_2, \ldots, a_n$ are called the partial quotients of the continued fraction. We use the notation $[a_0; a_1, a_2, \ldots, a_n]$ to represent a finite continued fraction.

A continued fraction is called simple if $a_0, a_1, \ldots, a_n$ are all integers.

Remark 2.3.2 Every rational number can be expressed as a finite simple continued fraction and every simple finite continued fraction represents a rational number.

Let a and b be integers, such that $(a, b) = 1$. Set $f_0 = a/b$. Then the partial quotients are computed using the following formula: $a_i = \lfloor f_i \rfloor$, $f_{i+1} = 1/(f_i - a_i)$, for $i = 0, 1, \ldots, n-1$ and $a_n = f_n$. Note that the notation $\lfloor\ \rfloor$ denotes the floor function. For $i = 0, 1, \ldots, n-2$, f_{i+1} is not an integer. We stop when the value of f_{i+1} is a positive integer and this positive integer would be the last partial quotient. At the point where $i = n-1$, $f_n = 1/(f_{n-1} - a_{n-1})$, which is a positive integer and so gives the last partial quotient a_n. This recursive rule allows for the expansion into a continued fraction. For instance, we find that $89/23 = [3; 1, 6, 1, 2]$.

Remark 2.3.3 Continued fractions for rational numbers are not unique. From the identity

$$a_n = (a_n - 1) + \frac{1}{1},$$

we see that

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, \ldots, a_{n-1}, a_n - 1, 1],$$

whenever $a_n > 1$.

If $a_n = 1$, we have $\frac{1}{a_{n-1} + \frac{1}{a_n}} = \frac{1}{a_{n-1}+1}$ and we see that

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, a_2, \ldots, a_{n-2}, a_{n-1} + 1].$$

2.4 Convergents

Definition 2.4.1 The convergents of the finite simple continued fraction $[a_0; a_1, a_2, \ldots, a_n]$ are defined to be the numbers $C_k = [a_0; a_1, a_2, \ldots, a_k]$ for $k = 0, 1, 2, \ldots, n$.
C_k is called the kth convergent.
For $k < n$, these convergents may also be termed *partial convergents.*

If

$$\frac{r}{s} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}},$$

then

$$C_1 = a_1, \quad C_2 = a_1 + \tfrac{1}{a_2}, \quad C_3 = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}, \quad C_4 = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}.$$

Theorem 2.4.2 Let $a_0, a_1, a_2, \ldots, a_n$ be partial quotients of the finite simple continued fraction $[a_0; a_1, a_2, \ldots, a_n]$. Let the sequences $p_0, p_1, \ldots, p_n$ and $q_0, q_1, \ldots, q_n$ be defined recursively by

$$p_0 = a_0 \quad \text{and} \quad q_0 = 1,$$

$$p_1 = a_0 a_1 + 1 \quad \text{and} \quad q_1 = a_1,$$

$$p_k = a_k p_{k-1} + p_{k-2} \quad \text{and} \quad q_k = a_k q_{k-1} + q_{k-2} \text{ for } k = 2, 3, \ldots, n.$$

Then the kth convergent is given by $C_k = \dfrac{p_k}{q_k}$.

Proof: We use mathematical induction on k.
We firstly note that

$$C_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0 - 0} = \frac{p_0}{q_0},$$

$$C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1},$$

$$\begin{aligned} C_2 = [a_0; a_1, a_2] &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} \\ &= a_0 + \cfrac{1}{\cfrac{a_1 a_2 + 1}{a_2}} \\ &= \frac{a_0}{1} + \frac{a_2}{a_1 a_2 + 1} \end{aligned}$$

$$= \frac{a_0(a_1a_2+1)+a_2}{a_1a_2+1}$$
$$= \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1}$$
$$= \frac{a_2(a_0a_1+1)+a_0}{a_1a_2+1} = \frac{p_2}{q_2}.$$

We see that the theorem holds for $k=0$, $k=1$ and $k=2$.
Suppose that the theorem holds for a positive integer k, where $2 \leq k \leq n$, i.e.

$$C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}. \tag{2.1}$$

By how the p_j's and q_j's are defined, the real numbers p_{k-1}, p_{k-2}, q_{k-1} and q_{k-2} depend only on the partial quotients $a_0, a_1, \ldots, a_{k-1}$.

Consequently, we can replace the real number a_k by $a_k + \dfrac{1}{a_{k+1}}$ in (2.1), to obtain

$$\begin{aligned}
C_{k+1} &= [a_0; a_1, \ldots, a_k, a_{k+1}] \\
&= [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}] \\
&= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} \\
&= \frac{(\frac{a_k(a_{k+1})+1}{a_{k+1}})p_{k-1} + p_{k-2}}{(\frac{a_k(a_{k+1})+1}{a_{k+1}})q_{k-1} + q_{k-2}} \\
&= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\
&= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.
\end{aligned}$$

Hence, we see that $C_{k+1} = \dfrac{p_{k+1}}{q_{k+1}}$. ■

Applying what was proved in Theorem 2.4.2, the convergents of $[6; 7, 3, 1]$ are $C_0 = 6$, $C_1 = \frac{43}{7}$, $C_2 = \frac{135}{22}$, $C_3 = \frac{178}{29}$. Theorem 2.4.2 can be used to find the fraction associated with a given finite simple continued fraction expression.

Lemma 2.4.3 Let $C_k = \dfrac{p_k}{q_k}$ be the kth convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$, where $1 \leq k \leq n$. If $p_k = a_k p_{k-1} + p_{k-2}$ (as defined in Theorem 2.4.2), then the following relations hold:

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}, \tag{2.2}$$
$$p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k. \tag{2.3}$$

Proof: For (2.2), firstly recall from Theorem 2.4.2 that

$$p_1 = a_0a_1 + 1,\ p_0 = a_0,\ q_0 = 1,\ q_1 = a_1.$$

By mathematical induction on k, we have for $k = 1$,

$$p_1q_0 - p_0q_1 = (a_0a_1 + 1) \cdot 1 - a_0a_1 = a_0a_1 + 1 - a_0a_1 = 1 = (-1)^{k-1}.$$

Now assume that (2.2) holds for any integer k, where $1 \leq k \leq n-1$, i.e.

$$p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}.$$

Then

$$\begin{aligned} p_{k+1}q_k - p_kq_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= a_{k+1}p_kq_k + p_{k-1}q_k - a_{k+1}p_kq_k - p_kq_{k-1} \\ &= p_{k-1}q_k - p_kq_{k-1} \\ &= -(p_kq_{k-1} - p_{k-1}q_k) \\ &= -(-1)^{k-1} \\ &= (-1)^1(-1)^{k-1} = (-1)^k. \end{aligned}$$

Thus, we see that the result holds for $k+1$. Hence, the result is true for all $1 \leq k \leq n$.

For (2.3), observe that $p_k = a_kp_{k-1} + p_{k-2}$, and $q_k = a_kq_{k-1} + q_{k-2}$, for $k = 2, 3, \ldots, n$.

So,

$$\begin{aligned} p_kq_{k-2} - p_{k-2}q_k &= (a_kp_{k-1} + p_{k-2})q_{k-2} - (a_kq_{k-1} + q_{k-2})p_{k-2} \\ &= a_kp_{k-1}q_{k-2} + p_{k-2}q_{k-2} - a_kp_{k-2}q_{k-1} - p_{k-2}q_{k-2} \\ &= a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) \\ &= (1)^{k-2}a_k = (-1)^ka_k. \quad \blacksquare \end{aligned}$$

We utilise Lemma 2.4.3 in proving Theorem 2.4.4 below.

Theorem 2.4.4 The numerator and denominator of the kth convergent, p_k and q_k, are co-prime integers.

Proof: By definition, p_1, q_1, p_0 and q_0 are integers. By hypothesis, the a_k's are also integers for $1 \leq k \leq n-1$. For $1 \leq k \leq n-1$, as seen in Lemma 2.4.3, since p_k and q_k are as a result of combinations of multiplication and subtraction of a_k's, it must be that p_k and q_k are integers as well. Note that by (2.2) of Lemma 2.4.3, we have $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$. Since this is a linear combination of p_k and q_k, it is equal to ± 1. So it must be that (p_k, q_k) divides ± 1. Thus p_k and q_k are co-prime. $\blacksquare$

Corollary 2.4.5 Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$.

Then

$$(a)\ C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}\ (1 \le k \le n),$$

$$(b)\ C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}\ (2 \le k \le n),$$

$$(c)\ C_0 < C_2 < C_4 < C_6 < C_8 < \cdots < C_5 < C_3 < C_1.$$

Proof: From (2.2) of Lemma 2.4.3, we know that

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}. \tag{2.4}$$

Dividing both sides of (2.4) by $q_{k-1}q_k$ and then utilising the result from Theorem 2.4.2 gives

$$\frac{(-1)^{k-1}}{q_{k-1}q_k} = \frac{p_k q_{k-1} - p_{k-1}q_k}{q_{k-1}q_k} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = C_k - C_{k-1}.$$

This proves (a).

By Theorem 2.4.2, we know that

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}. \tag{2.5}$$

Using the fact that $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$ from Theorem 2.4.2, we see that the numerator on the extreme right of (2.5) is such that

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2} - a_k p_{k-2} q_{k-1} - p_{k-2} q_{k-2} \\ &= a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) = a_k (-1)^{k-2}. \end{aligned}$$

Now by (2.5), we know that
$C_k - C_{k-2} = \dfrac{a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1})}{q_k q_{k-2}}$. Since $(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = (-1)^k$, we must have
$C_k - C_{k-2} = \dfrac{a_k(-1)^k}{q_k q_{k-2}}$. This proves (b).

We now prove Corollary 2.4.5 (c).

From (b), we know that $C_k - C_{k-2} = \dfrac{a_k(-1)^k}{q_k q_{k-2}}$. This means that
$C_k - C_{k-2} > 0$ for every even k and on the other hand, $C_k - C_{k-2} < 0$ for every odd k.

Since $C_k - C_{k-2} < 0$ for every odd k, $C_k < C_{k-2}$ when k is odd, hence $C_1 > C_3 > C_5 > \ldots$. Similarly, $C_k - C_{k-2} > 0$ for every even k implies that $C_k > C_{k-2}$ when k is even and so $C_0 < C_2 < C_4 < \ldots$.

To show that every odd-numbered convergent is greater than every even-numbered conver-

gent, observe that from (a), we have $C_{2m} - C_{2m-1} = \dfrac{(-1)^{2m-1}}{q_{2m}q_{2m-1}} < 0$ so that $C_{2m-1} > C_{2m}$.

To compare C_{2k} and C_{2j-1}, we have $C_{2j-1} > C_{2j+2k-1} > C_{2j+2k} > C_{2k}$, so that every odd-numbered convergent is greater than every even-numbered convergent. ■

Definition 2.4.6 The convergents between the first and last convergents of a finite continued fraction are called intermediate fractions.

Definition 2.4.7 The mediant of two fractions $\frac{a}{b}$ and $\frac{c}{d}$ with positive denominators is the fraction

$$\frac{a+c}{b+d}.$$

Lemma 2.4.8 The mediant of two fractions always lies between them in value.

Proof: Suppose that we have two fractions $\dfrac{a}{b}$ and $\dfrac{c}{d}$. By Definition 2.4.7, the mediant of these two fractions is $\dfrac{a+c}{b+d}$. For definiteness, assume that $\dfrac{a}{b} \leq \dfrac{c}{d}$.

Consequently, $\dfrac{a+c}{b+d} - \dfrac{a}{b} = \dfrac{bc-ad}{b(b+d)} \geq 0$ and $\dfrac{a+c}{b+d} - \dfrac{c}{d} = \dfrac{ad-bc}{b(b+d)} \leq 0$,
which proves the lemma. ■

Proposition 2.4.9 Each intermediate fraction always lies between an arbitrary convergent and the mediant of that convergent and the preceding one.

Proof: Consider the following sequence of fractions

$$\frac{p_{k-2}}{q_{k-2}}, \frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}}, \frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}}, \ldots, \frac{p_{k-2}+a_kp_{k-1}}{q_{k-2}+a_kq_{k-1}} = \frac{p_k}{q_k}. \tag{2.6}$$

We observe that each of the fractions in the progression of (2.6) is the mediant of the preceding fraction and the fraction $\frac{p_{k-1}}{q_{k-1}}$. By going through the progression and successively forming the mediants, we proceed from the convergent $\frac{p_{k-2}}{q_{k-2}}$ in the direction of $\frac{p_{k-1}}{q_{k-1}}$. The concluding step in this sequence will occur when the mediant constructed coincides with $\frac{p_k}{q_k}$. From Corollary 2.4.5 (c), we know that this last fraction lies between $\frac{p_{k-1}}{q_{k-1}}$ and $\frac{p_{k-2}}{q_{k-2}}$. Let α be the value of a given continued fraction that lies between $\frac{p_{k-2}}{q_{k-2}}$ and $\frac{p_k}{q_k}$. So the fractions $\frac{p_{k-2}}{q_{k-2}}$ and $\frac{p_k}{q_k}$, which are either both of even order or odd order, lie on the same side of α. (By even or odd order, we mean that both convergents are either even convergents or else both convergents are odd convergents, since we know that each of the convergents alternate between even and odd-numbered subscripts). It follows from this that the entire progression lies on one side of α and that the fraction $\frac{p_{k-1}}{q_{k-1}}$ lies on the other side. In particular, the fractions $\frac{p_{k-1}+p_{k-2}}{q_{k-1}+q_{k-2}}$ and $\frac{p_{k-1}}{q_{k-1}}$ are always on opposite sides of α. In other words, the value of a continued fraction always lies between an arbitrary convergent and the mediant of that convergent and the preceding one. ■

Theorem 2.4.10 Suppose that $\frac{p_m}{q_m}$ and $\frac{p_{m+2}}{q_{m+2}}$ are convergents of a real number α. Then

$$\frac{1}{q_m(q_{m+1}+q_m)} < \left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}}. \tag{2.7}$$

Proof: We first prove the inequality on the right-hand side of (2.7).
By Corollary 2.4.5 (a), we know that

$$C_m - C_{m+1} = \frac{(-1)^{m+1}}{q_m q_{m+1}},$$

so that

$$|C_m - C_{m+1}| = \frac{1}{q_m q_{m+1}}.$$

Since α is between two successive convergents, its distance away from C_m must be less than the full distance between the two convergents. That is,

$$|\alpha - C_m| < |C_m - C_{m+1}| = \frac{1}{q_m q_{m+1}}.$$

Hence,

$$\left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}}.$$

The inequality on the left-hand side of (2.7) follows as a direct consequence of the positions of convergents around α.
We know that α lies between two convergents, say $\frac{p_m}{q_m}$ and $\frac{p_{m+1}}{q_{m+1}}$. The mediant of $\frac{p_m}{q_m}$ and $\frac{p_{m+1}}{q_{m+1}}$ is $\frac{p_m+p_{m+1}}{q_m+q_{m+1}}$. By Proposition 2.4.9, we conclude that α is between $\frac{p_m+p_{m+1}}{q_m+q_{m+1}}$ and $\frac{p_{m+1}}{q_{m+1}}$ and so $\frac{p_m+p_{m+1}}{q_m+q_{m+1}}$ is between $\frac{p_m}{q_m}$ and α. It turns out that the intermediate fraction $(p_m + p_{m+1})/(q_m + q_{m+1})$ lies between p_m/q_m and α and $(p_m + p_{m+1})/(q_m + q_{m+1})$ lies closer to p_m/q_m than it does to α [9]. That is, the distance between α and p_m/q_m is larger than the distance between $(p_m + p_{m+1})/(q_m + q_{m+1})$ and α. So,

$$\begin{aligned}
\left|\alpha - \frac{p_m}{q_m}\right| &> \left|\frac{p_m + p_{m+1}}{q_m + q_{m+1}} - \frac{p_m}{q_m}\right| \\
&= \left|\frac{q_m(p_m + p_{m+1}) - p_m(q_m + q_{m+1})}{q_m(q_{m+1} + q_m)}\right| \\
&= \left|\frac{q_m p_m + q_m p_{m+1} - q_m p_m - p_m q_{m+1}}{q_m(q_{m+1} + q_m)}\right| \\
&= \left|\frac{q_m p_{m+1} - p_m q_{m+1}}{q_m(q_{m+1} + q_m)}\right| \\
&= \left|\frac{-(-1)^m}{q_m(q_{m+1} + q_m)}\right| \\
&= \frac{1}{q_m(q_{m+1} + q_m)}.
\end{aligned}$$

(The second last line follows from Lemma 2.4.3). This concludes the proof. ■

Recall that the modulus n of the RSA cryptosystem is the product of two large primes p and q, where p and q are distinct and have approximately the same number of bits.
The public exponent e and the secret exponent d are related by $ed \equiv 1 \pmod{\phi(n)}$, where $\phi(n) = (p-1)(q-1) = n - p - q + 1$. This relation between e and d implies that there is an integer k such that

$$ed - k\phi(n) = 1. \tag{2.8}$$

Theorem 2.4.11 If $p < q < 2p$, $e < n$ and $d < \frac{1}{3}\sqrt[4]{n}$, then

$$\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}.$$

Proof: Firstly, since $n = pq$, $p < q = \frac{n}{p}$. Thus

$$p < \sqrt{n}. \tag{2.9}$$

Since $p < q < 2p$, then $q < 2p$ implies

$$p + q - 1 < p + 2p - 1 = 3p - 1 < 3\sqrt{n}.$$

The last inequality is true by (2.9).
So, we have

$$p + q - 1 < 3\sqrt{n}. \tag{2.10}$$

We know that $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$. So $n - \phi(n) = n - (n - p - q + 1) = p + q - 1 < 3\sqrt{n}$ by (2.10). Hence,

$$n - \phi(n) < 3\sqrt{n}. \tag{2.11}$$

We have

$$\begin{aligned}
\left|\frac{k}{d} - \frac{e}{n}\right| &= \left|\frac{kn - ed}{dn}\right| \\
&= \left|\frac{kn - ed - k\phi(n) + k\phi(n)}{dn}\right| \\
&= \left|\frac{(kn - k\phi(n)) - (ed - k\phi(n))}{dn}\right| \\
&= \left|\frac{k(n - \phi(n)) - 1}{dn}\right| < \frac{3k\sqrt{n}}{dn} = \frac{3k}{d\sqrt{n}}, \text{ (by (2.8) and (2.11)).}
\end{aligned}$$

Thus,

$$\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{3k}{d\sqrt{n}}. \tag{2.12}$$

Since $e = d^{-1} \pmod{\phi(n)}$, we have $e < \phi(n)$, which implies that $ke < k\phi(n) = ed - 1 < ed$. This implies

$$k < d < \frac{1}{3}\sqrt[4]{n}. \tag{2.13}$$

However,

$$2d < n^{\frac{1}{4}}.$$

Therefore,

$$\frac{1}{2d^2} > \frac{1}{dn^{\frac{1}{4}}}. \tag{2.14}$$

Making use of (2.12), (2.13) and (2.14) gives

$$\begin{aligned}\left|\frac{k}{d} - \frac{e}{n}\right| &< \frac{3k\sqrt{n}}{dn} \\ &< \frac{3(\frac{1}{3}\sqrt[4]{n})\sqrt{n}}{dn} = \frac{n^{\frac{3}{4}}}{dn} = \frac{1}{dn^{\frac{1}{4}}} < \frac{1}{2d^2}.\end{aligned}$$

Hence,

$$\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}. \quad \blacksquare$$

Theorem 2.4.12 (Legendre).
If k, d, e and n are all distinct, positive integers with d and n nonzero, $(k, d) = (e, n) = 1$ and $|\frac{k}{d} - \frac{e}{n}| < \frac{1}{2d^2}$, then $\frac{k}{d}$ is a convergent of the continued fraction of $\frac{e}{n}$.

Proof: If $n \leq d$ (that is, $\frac{n}{2d} \leq \frac{1}{2}$) , then $\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}$ implies that

$$|kn - ed| < \frac{1}{2d^2} \leq \frac{nd}{2d^2},$$

so that

$$|kn - ed| < \frac{n}{2d} \leq \frac{1}{2}.$$

So, if $n \leq d$, then $|kn - ed| < \frac{1}{2}$ which would mean that $kn - ed = 0$. That is, $kn = ed$, which would imply that (2.8) becomes $k(n - \phi(n)) = 1$. This is only possible if $k = 1$ and $n - \phi(n) = 1$. However, $n - \phi(n) = pq - [(p-1)(q-1)] = p + q - 1$ and to have $p + q - 1 = 1$, it would mean that $p + q = 2$, which is impossible since p and q are distinct primes, greater than or equal to 2. So we reach a contradiction when assuming $kn - ed = 0$.
Hence, it must be that $|kn - ed|$ is a positive integer. Thus, $n > d$.

Suppose that $\frac{k}{d}$ is not a convergent of the continued fraction for $\frac{e}{n}$. Since the denominators of the convergents increase to n (where $n > d$), there must be two successive convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ such that

$$q_n < d < q_{n+1}. \tag{2.15}$$

Utilising the assumption that $\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}$, and the triangle inequality below, we have

$$\begin{aligned}\frac{1}{2d^2} &> \left|\frac{k}{d} - \frac{e}{n}\right| \\ &= \left|\frac{k}{d} - \frac{p_n}{q_n} + \frac{p_n}{q_n} - \frac{e}{n}\right| \\ &\geq \left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{e}{n} - \frac{p_n}{q_n}\right| \\ &\geq \left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|.\end{aligned}$$

(The last line is true because the $(n+1)$st convergent is on the other side of $\frac{e}{n}$ from the nth convergent).

So,

$$\frac{1}{2d^2} > \left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|. \tag{2.16}$$

Note that if $kq_n - dp_n = 0$, then $kq_n = dp_n$ so that $\frac{k}{d} = \frac{p_n}{q_n}$ which contradicts the assumption that $\frac{k}{d}$ is not a convergent of $\frac{e}{n}$. Hence,

$$|kq_n - dp_n| \geq 1. \tag{2.17}$$

Dividing both sides of (2.17) by $|dq_n|$ gives

$$\left|\frac{kq_n - dp_n}{dq_n}\right| \geq \frac{1}{dq_n}. \tag{2.18}$$

Now,

$$\left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \geq \frac{1}{dq_n} - \frac{1}{q_n q_{n+1}}. \tag{2.19}$$

This is because

$$\left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{kq_n - dp_n}{dq_n}\right| - \left|\frac{q_n p_{n+1} - p_n q_{n+1}}{q_n q_{n+1}}\right|,$$

where the numerator of the first difference on the right side is a nonzero integer by (2.17) and by applying Lemma 2.4.3 to the numerator of the second difference on the right side, we know that $q_n p_{n+1} - p_n q_{n+1} = (-1)^{n-1}$ such that if n is even, then $q_n p_{n+1} - p_n q_{n+1} = 1$. If n is odd, then $q_n p_{n+1} - p_n q_{n+1} = -1$.
Combining (2.16) and (2.19) gives

$$\frac{1}{2d^2} > \frac{1}{dq_n} - \frac{1}{q_n q_{n+1}}.$$

So,

$$\begin{aligned}\frac{1}{2} &> \frac{d}{q_n}\left(1-\frac{d}{q_{n+1}}\right)\\ &> \left(1-\frac{d}{q_{n+1}}\right).\end{aligned}$$

So, $\frac{1}{2} > 1-\frac{d}{q_{n+1}}$, meaning that

$$\frac{1}{2} < \frac{d}{q_{n+1}}. \tag{2.20}$$

Since $q_n < d < q_{n+1}$ by (2.15), we know that the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ divide the line into three regions. As $\frac{k}{d}$ could be in any of these regions, we have the following cases:

(Note that we assume $\frac{k}{d}$ is not a convergent and so $\frac{k}{d} \neq \frac{p_n}{q_n}$ and $\frac{k}{d} \neq \frac{p_{n+1}}{q_{n+1}}$ as both $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ are convergents of $\frac{e}{n}$).

Case 1: If $\frac{k}{d}$ is between the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ then by (2.17), we have

$$\frac{1}{dq_n} \leq \left|\frac{k}{d}-\frac{p_n}{q_n}\right| = \left|\frac{kq_n-dp_n}{dq_n}\right|.$$

We know that the assumption of Case 1 is that $\frac{k}{d}$ is between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, where the $(n+1)$st convergent is farther from the nth convergent than $\frac{k}{d}$. This fact is used in the second line below

$$\begin{aligned}\frac{1}{dq_n} &\leq \left|\frac{k}{d}-\frac{p_n}{q_n}\right|\\ &\leq \left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|\\ &= \frac{1}{q_{n+1}q_n}.\end{aligned}$$

(The first line makes use of (2.18) and the last line makes use of Lemma 2.4.3: $q_np_{n+1} - p_nq_{n+1} = (-1)^{n-1}$. The absolute value results in a positive value of 1 in the numerator of the last line).

We see that

$$\frac{1}{dq_n} \leq \frac{1}{q_{n+1}q_n},$$

which implies that

$$dq_n \geq q_{n+1}q_n.$$

Dividing both sides by q_n gives

$$d \geq q_{n+1}.$$

This is a contradiction to (2.15) which states that $q_n < d < q_{n+1}$.

Case 2: If $\frac{k}{d}$ is not between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, then we have

Sub-case(a): $\frac{k}{d}$ is closer to $\frac{p_n}{q_n}$.

We know that

$$\frac{1}{dq_n} \leq \left|\frac{k}{d} - \frac{p_n}{q_n}\right| \leq \left|\frac{k}{d} - \frac{e}{n}\right|.$$

(The first inequality is due to (2.18). The second inequality is due to the assumption that $\frac{k}{d}$ is closer to $\frac{p_n}{q_n}$ than $\frac{e}{n}$).

Applying Theorem 2.4.11, we have

$$\frac{1}{dq_n} \leq \left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}.$$

We see that

$$\frac{1}{dq_n} < \frac{1}{2d^2}.$$

So

$$q_n > 2d > d$$

implying that

$$q_n > d.$$

This is a contradiction to (2.15).

Sub-case (b): $\frac{k}{d}$ is closer to $\frac{p_{n+1}}{q_{n+1}}$.

Applying (2.18) and the assumption of sub-case (b), we have

$$\frac{1}{dq_{n+1}} \leq \left|\frac{k}{d} - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\frac{k}{d} - \frac{e}{n}\right|.$$

Applying Theorem 2.4.11, we have that

$$\frac{1}{dq_{n+1}} \leq \left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}.$$

So we have that

$$\frac{1}{dq_{n+1}} < \frac{1}{2d^2}.$$

This implies that

$$\frac{d}{q_{n+1}} < \frac{1}{2}.$$

This contradicts (2.20).
Therefore, we conclude that $\frac{k}{d}$ must be a convergent of the continued fraction of $\frac{e}{n}$. ■

2.5 A cryptosystem based on continued fractions

In this section, we are going to describe a cryptosystem that is based on finite simple continued fractions. Invented by Arthur Porges in 1954 [13], this cryptosystem is described to be one of the first cryptosystems based on continued fractions.

ASCII printable characters	Number symbol
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

Table 2.5.1: ASCII codes

Table 2.5.1 gives the number associated with each letter of the alphabet, as per the ASCII codes. To encrypt plaintext, convert each letter of the plaintext into a list of integers as per the table of ASCII codes, then utilise these integers as continued fraction coefficients and the resulting rational number that stems out of this continued fraction expansion will be the ciphertext. To then decrypt this ciphertext, which is a rational number, we find the partial quotients of the continued fraction expansion associated with this rational number. We then use the ASCII codes to turn each of the numbers into letters that make up the original plaintext. We demonstrate this procedure with a small example

Example 2 Suppose that our plaintext is the word **COP**. Converting each letter to its ASCII code as represented in Table 2.5.1, we get the following: [67; 79 , 80]. Representing these number coefficients as a continued fraction gives

$67 + \dfrac{1}{79 + \dfrac{1}{80}} = \dfrac{423587}{6321}$ and this rational number is our ciphertext.

For another individual to decrypt this, he/she goes in the opposite direction: Take the rational number, find its partial quotients using the recursive rule described in Remark 2.3.3 and then use the table of ASCII codes to turn each of the integer partial quotients into letters making up the plaintext. From Remark 2.3.4, we know that the continued fraction representation of a rational number is not unique. For every rational number $\frac{a}{b}$, we have two representations: $\frac{a}{b} = [a_0, a_1, \ldots, a_{m-1}, a_m] = [a_0, a_1, \ldots, a_{m-1}, a_m - 1, 1]$.
So which continued fraction representation will give the correct plaintext? The answer to this lies in the fact that the characters $A, B, \ldots, Z$ in the ASCII table correspond to the numbers $65, 66, \ldots, 90$. This means that a partial quotient a_i is such that $64 < a_i < 91$. In particular, the last partial quotient should be between 64 and 91. Thus the continued fraction representation which has 1 as the last partial quotient cannot be the correct one. So in decryption, we should place a limitation on the partial quotients such that for every partial quotient a_i, it should be that $64 < a_i < 91$ in order for the receiver to obtain the correct plaintext. ■

Chapter 3

WIENER'S ATTACK

In the paper titled *Cryptanalysis of Short RSA Secret Exponents* by Michael J. Wiener [22], an attack on the RSA cryptosystem using short secret exponents is described. This attack makes use of an algorithm based on continued fractions. In this chapter, we survey some aspects of Wiener's work.

3.1 Application of continued fractions

To form the continued fraction expansion of a positive rational f, we subtract away the integer part of f and repeatedly invert the remainder, continuing with these steps until we get a remainder of zero.
Let f denote the positive rational number. Suppose that a_i denotes the integer quotient $(i = 0, 1, \ldots, m)$ and r_i denotes the remainder at step i. Suppose there are m inversion steps:

$$a_0 = \lfloor f \rfloor, r_0 = f - a_0, a_i = \left\lfloor \frac{1}{r_{i-1}} \right\rfloor, r_i = \frac{1}{r_{i-1}} - a_i, \quad \text{for} \quad i = 1, 2, \ldots, m. \tag{3.1}$$

Once we get to $r_m = 0$, we have $f = [a_0, a_1, \ldots, a_m]$.

At this point, a very important observation is made, which we present in the form of a lemma below.

Lemma 3.1.1 For a finite continued fraction, the last partial quotient a_m is greater than or equal to 2.

Proof: Suppose that $a_m < 2$. By definition, $a_0, \ldots, a_m$ are integer quotients that are greater than or equal to zero and so $a_m = 0$ or $a_m = 1$.

Consider $a_m = 0$.

Case 1: $m = 0$. That is, last term $a_m = a_0 = 0$.

In this case, $f = (a_0) = (0)$, meaning that $f = 0$, which is impossible since $f > 0$.

Case 2: $m > 0$.

We know that $a_1, \ldots, a_m \geq 1$ because the partial quotients $a_1, \ldots, a_m$ are all raised over 1 and having $\frac{1}{0}$ is undefined. So the case of $m > 0$ for which $a_m = 0$ is also impossible.

If $a_m = 1$, then by (3.1)
$a_m = \left\lfloor \frac{1}{r_{m-1}} \right\rfloor = 1$, which can only happen if $r_{m-1} = 1$.
However, having $r_{m-1} = 1$ is impossible. ■

Proposition 3.1.2 For any $x > 0$,

$$[a_0, a_1, a_2, \ldots, a_m] < [a_0, a_1, a_2, \ldots, a_{m-1}, a_m + x], \tag{3.2}$$

if m is even.

$$[a_0, a_1, a_2, \ldots, a_m] > [a_0, a_1, a_2, \ldots, a_{m-1}, a_m + x], \tag{3.3}$$

if m is odd.

Proof: See Wiener [22].

Using Theorem 2.4.2, $f = \frac{n_m}{d_m}$ can be reconstructed from its continued fraction expansion. We let n_i and d_i be a sequence of numerators and denominators, which are defined as follows:

$$\frac{n_i}{d_i} = [a_0, a_1, \ldots, a_i],\ (n_i, d_i) = 1,\ \text{for } i = 0, 1, \ldots, m \text{ and} \tag{3.4}$$

$a_0, \ldots, a_i$ are the partial quotients. Note that it is always the case that $(n_i, d_i) = 1$ because upon expressing a positive rational number f as $f = \dfrac{n_m}{d_m}$, we take the fraction in its simplest form.

3.2 Wiener's algorithm

Let f' be an underestimate of f. Then for some $\delta \geq 0$, we have

$$f' = f(1 - \delta). \tag{3.5}$$

Arranging (3.5) to make δ the subject of the formula gives

$$1 - \frac{f'}{f} = \delta. \tag{3.6}$$

Let a_i, r_i and a'_i, r'_i be the ith quotients and remainders of f and f', respectively. If δ is small enough, then the numerator and denominator of f can be found using the following algorithm [22]:

(1) Generate the next quotient (a'_i) of the continued fraction expansion of f'.

(2) Use Theorem 2.4.2 to construct the fraction equal to

$$[a'_0, a'_1, \ldots, a'_{i-1}, a'_i + 1],\ \text{if } i \text{ is even}$$

and

$$[a_0', a_1', \ldots, a_i'], \text{ if } i \text{ is odd.}$$

(3) Check whether the constructed fraction is equal to f. If not, repeat steps (1) and (2).

The continued fraction algorithm will succeed if

$$[a_0, a_1, \ldots, a_{m-1}, a_m - 1] < f' \leq [a_0, a_1, \ldots, a_m], \text{ if } m \text{ is even,} \tag{3.7}$$

$$[a_0, a_1, \cdots, a_{m-1}, a_m + 1] < f' \leq [a_0, a_1, \ldots, a_m], \text{ if } m \text{ is odd.} \tag{3.8}$$

Alternatively, the continued fraction algorithm will succeed if

$$\delta < \frac{1}{n_m d_m} \text{ , for } m \text{ even,}$$

$$\delta < \frac{1}{\frac{3}{2} n_m d_m} \text{ , for } m \text{ odd.}$$

We explore why the delta conditions imply that (3.7) and (3.8) hold. We do this by analysing the cases where m is even separately from the cases where m is odd.

Case 1: $m = 0$.
Suppose,

$$\delta < \frac{1}{n_0 d_0}. \tag{3.9}$$

By Theorem 2.4.2, we know that $n_0 = a_0$ and $d_0 = 1$. So (3.9) can be re-written as

$$\begin{aligned}
\delta &< \frac{1}{a_0 \cdot 1} \\
&= \frac{a_0 - a_0 + 1}{a_0} \\
&= \frac{a_0 - (a_0 - 1)}{a_0} \\
&= \frac{[a_0] - [a_0 - 1]}{[a_0]} \\
&= \frac{[a_0]}{[a_0]} - \frac{[a_0 - 1]}{[a_0]} < 1 - \frac{[a_0 - 1]}{[a_0]}.
\end{aligned}$$

So, we have

$$\delta < 1 - \frac{[a_0 - 1]}{[a_0]}, \text{ i.e.} \tag{3.10}$$

$$1 - \frac{[a_0 - 1]}{[a_0]} > 1 - \frac{f'}{f} \geq 0, \text{ which implies}$$

$$\frac{[a_0 - 1]}{[a_0]} < \frac{f'}{f} \leq 1.$$

In this case, since $f = [a_0]$, we have

$$[a_0 - 1] < f' \leq [a_0]. \tag{3.11}$$

Case 2: $m = 1$.
Suppose

$$\delta < \frac{1}{\frac{3}{2}n_1 d_1}. \tag{3.12}$$

By Theorem 2.4.2, $n_1 = a_0a_1 + 1$ and $d_1 = a_1$. So (3.12) can be re-written as

$$\begin{aligned}\delta &< \frac{1}{\frac{3}{2}(a_0a_1 + 1)a_1} \\ &= \left(\frac{1}{a_0a_1 + 1}\right)\left(\frac{1}{\frac{3}{2}a_1}\right).\end{aligned}$$

That is,

$$\delta < \left(\frac{1}{a_0a_1 + 1}\right)\left(\frac{1}{\frac{3}{2}a_1}\right). \tag{3.13}$$

By Lemma 3.1.1, we know that $a_m \geq 2$. In this case, for $m = 1$, $a_1 \geq 2$ so that

$$a_1 \geq \frac{2}{3}(a_1 + 1).$$

This can also be written as

$$\frac{1}{a_1 + 1} \;\geq\; \frac{1}{\frac{3}{2}a_1},$$

which is true even when we multiply both sides by any constant, so

$$\left(\frac{1}{a_0a_1 + 1}\right)\left(\frac{1}{a_1 + 1}\right) \;\geq\; \left(\frac{1}{a_0a_1 + 1}\right)\left(\frac{1}{\frac{3}{2}a_1}\right) > \delta. \tag{3.14}$$

Thus, by (3.14), we have

$$\begin{aligned}\delta &< \frac{1}{(a_0a_1 + 1)(a_1 + 1)} \\ &= \frac{a_1a_0a_1 - a_1a_0a_1 + a_0a_1 - a_0a_1 + a_1 - a_1 + 1}{(a_0a_1 + 1)(a_1 + 1)} \\ &= \frac{a_1a_0a_1 + a_0a_1 + a_1 + 1 - a_1a_0a_1 - a_0a_1 - a_1}{(a_0a_1 + 1)(a_1 + 1)} \\ &= \frac{(a_0a_1 + 1)(a_1 + 1)}{(a_0a_1 + 1)(a_1 + 1)} - \frac{a_1a_0a_1 + a_0a_1 + a_1}{(a_0a_1 + 1)(a_1 + 1)} \\ &= 1 - \frac{a_1(a_0a_1 + a_0 + 1)}{(a_0a_1 + 1)(a_1 + 1)} \\ &= 1 - \left[\frac{a_0a_1 + a_0 + 1}{a_1 + 1} \times \frac{a_1}{a_0a_1 + 1}\right]\end{aligned}$$

$$
\begin{aligned}
&= 1 - \left[\frac{a_0(a_1+1)+1}{a_1+1} \div \frac{a_0a_1+1}{a_1} \right] \\
&= 1 - \left[\left(\frac{a_0}{1} + \frac{1}{a_1+1} \right) \div \left(\frac{a_0}{1} + \frac{1}{a_1} \right) \right] \\
&= 1 - \frac{a_0 + \frac{1}{a_1+1}}{a_0 + \frac{1}{a_1}} \\
&= 1 - \frac{[a_0, a_1+1]}{[a_0, a_1]}.
\end{aligned}
$$

So, we have

$$\delta < 1 - \frac{[a_0, a_1+1]}{[a_0, a_1]}, \tag{3.15}$$

which implies

$$\frac{[a_0, a_1+1]}{[a_0, a_1]} < \frac{f'}{f} \leq 1.$$

Since $f = [a_0, a_1]$, we have

$$[a_0, a_1+1] < f' \leq [a_0, a_1]. \tag{3.16}$$

Case 3: m even and $m \geq 2$.
Suppose

$$\delta < \frac{1}{n_m d_m}. \tag{3.17}$$

Note that $d_m - d_{m-1} < d_m$,

so that

$$\frac{1}{d_m - d_{m-1}} > \frac{1}{d_m},$$

which implies that

$$\frac{1}{n_m(d_m - d_{m-1})} > \frac{1}{n_m(d_m)} > \delta. \tag{3.18}$$

Thus, by (3.18), we have

$$\delta < \frac{1}{n_m(d_m - d_{m-1})}. \tag{3.19}$$

Since m is even, then (3.19) can also be written as

$$\delta < \frac{(-1)^m}{n_m(d_m - d_{m-1})}. \tag{3.20}$$

Applying Lemma 2.4.3 to the numerator of (3.20) and Theorem 2.4.2 to the denominator of (3.20) gives

$$\delta < \frac{n_{m-1}d_{m-2} - n_{m-2}d_{m-1}}{(a_m n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2} - d_{m-1})}. \tag{3.21}$$

We now expand on (3.21) further. (Note that we make use of (3.4) in the last line of the expansion).

$$\begin{aligned}
\delta &< \frac{n_{m-1}d_{m-2} - n_{m-2}d_{m-1}}{(a_m n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2} - d_{m-1})} \\
&= \frac{(a_m d_{m-1} - d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2}) - [(a_m n_{m-1} - n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2})]}{(a_m d_{m-1} - d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2})} \\
&= \frac{((a_m-1) d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2}) - [((a_m-1) n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2})]}{((a_m-1) d_{m-1} + d_{m-2})\,(a_m n_{m-1} + n_{m-2})} \\
&= \frac{((a_m-1) d_{m-1} + d_{m-2})\,(a_m n_{m-1} + n_{m-2})}{((a_m-1) d_{m-1} + d_{m-2})\,(a_m n_{m-1} + n_{m-2})} - \left[\frac{((a_m-1) n_{m-1} + n_{m-2})\,(a_m d_{m-1} + d_{m-2})}{((a_m-1) d_{m-1} + d_{m-2})\,(a_m n_{m-1} + n_{m-2})}\right] \\
&= 1 - \left[\frac{((a_m-1) n_{m-1} + n_{m-2})\,(a_m d_{m-1} + d_{m-2})}{((a_m-1) d_{m-1} + d_{m-2})\,(a_m n_{m-1} + n_{m-2})}\right] \\
&= 1 - \left[\frac{(a_m-1) n_{m-1} + n_{m-2}}{(a_m-1) d_{m-1} + d_{m-2}} \times \frac{a_m d_{m-1} + d_{m-2}}{a_m n_{m-1} + n_{m-2}}\right] \\
&= 1 - \left[\frac{(a_m-1) n_{m-1} + n_{m-2}}{(a_m-1) d_{m-1} + d_{m-2}} \div \frac{a_m n_{m-1} + n_{m-2}}{a_m d_{m-1} + d_{m-2}}\right] \\
&= 1 - \frac{\frac{(a_m-1) n_{m-1} + n_{m-2}}{(a_m-1) d_{m-1} + d_{m-2}}}{\frac{a_m n_{m-1} + n_{m-2}}{a_m d_{m-1} + d_{m-2}}} \\
&= 1 - \frac{[a_0, a_1, \ldots, a_m - 1]}{[a_0, a_1, \ldots, a_m]}.
\end{aligned}$$

So, we have

$$\delta < 1 - \frac{[a_0, a_1, \ldots, a_m - 1]}{[a_0, a_1, \ldots, a_m]}, \tag{3.22}$$

i.e.

$$1 - \frac{[a_0, a_1, \ldots, a_{m-1}, a_m - 1]}{[a_0, a_1, \ldots, a_m]} > 1 - \frac{f'}{f} \geq 0.$$

Since $f = [a_0, a_1, \ldots, a_m]$, we have

$$[a_0, a_1, \ldots, a_{m-1}, a_m - 1] < f' \leq [a_0, a_1, \ldots, a_m]. \tag{3.23}$$

Case 4: m odd and $m \geq 3$.
Suppose

$$\delta < \frac{1}{\frac{3}{2} n_m d_m}. \tag{3.24}$$

By Theorem 2.4.2, we know that $d_m = a_m d_{m-1} + d_{m-2}$. Thus,

$$d_m \;\geq\; a_m d_{m-1},$$

and since $a_m \geq 2$, we have

$$d_m \;\geq\; 2 d_{m-1},$$

so that

$$\frac{1}{2} d_m + d_m \;\geq\; d_{m-1} + d_m,$$

i.e.

$$\frac{1}{\frac{3}{2}d_m} \leq \frac{1}{d_m + d_{m-1}},$$

i.e.

$$\frac{1}{d_m + d_{m-1}} \geq \frac{1}{\frac{3}{2}d_m},$$

so that

$$\frac{1}{n_m(d_m + d_{m-1})} \geq \frac{1}{\frac{3}{2}n_m d_m} > \delta. \tag{3.25}$$

Thus, by (3.25), we have

$$\delta < \frac{1}{n_m(d_m + d_{m-1})}. \tag{3.26}$$

Since m is odd, (3.26) can also be written as

$$\delta < \frac{-(-1)^m}{n_m(d_m + d_{m-1})}. \tag{3.27}$$

Applying Lemma 2.4.3 to the numerator of (3.27) and Theorem 2.4.2 to the denominator of (3.27) gives

$$\begin{aligned}
\delta &< \frac{-\left[n_{m-1}d_{m-2} - n_{m-2}d_{m-1}\right]}{\left(a_m n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2} + d_{m-1}\right)} \\
&= \frac{-n_{m-1}d_{m-2} + n_{m-2}d_{m-1}}{\left(a_m n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2} + d_{m-1}\right)} \\
&= \frac{n_{m-2}d_{m-1} - n_{m-1}d_{m-2}}{\left(a_m n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2} + d_{m-1}\right)}.
\end{aligned}$$

We have

$$\delta < \frac{n_{m-2}d_{m-1} - n_{m-1}d_{m-2}}{\left(a_m n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2} + d_{m-1}\right)}. \tag{3.28}$$

We now expand on (3.28) further (Note that we make use of (3.4) in the last line of the expansion).

$$\begin{aligned}
\delta &< \frac{n_{m-2}d_{m-1} - n_{m-1}d_{m-2}}{\left(a_m n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2} + d_{m-1}\right)} \\
&= \frac{(a_m d_{m-1} + d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2}) - [(a_m n_{m-1} + n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2})]}{\left((a_m d_{m-1} + d_{m-1} + d_{m-2})\left(a_m n_{m-1} + n_{m-2}\right)\right.} \\
&= \frac{((a_m+1) d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2}) - [((a_m+1) n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2})]}{\left((a_m+1) d_{m-1} + d_{m-2})\left(a_m n_{m-1} + n_{m-2}\right)\right.} \\
&= \frac{\left((a_m+1) d_{m-1} + d_{m-2}\right)\left(a_m n_{m-1} + n_{m-2}\right)}{\left((a_m+1) d_{m-1} + d_{m-2}\right)\left(a_m n_{m-1} + n_{m-2}\right)} - \left[\frac{\left((a_m+1) n_{m-1} + n_{m-2}\right)\left(a_m d_{m-1} + d_{m-2}\right)}{\left((a_m+1) d_{m-1} + d_{m-2}\right)\left(a_m n_{m-1} + n_{m-2}\right)}\right] \\
&= 1 - \left[\frac{((a_m+1) n_{m-1} + n_{m-2})(a_m d_{m-1} + d_{m-2})}{((a_m+1) d_{m-1} + d_{m-2})(a_m n_{m-1} + n_{m-2})}\right]
\end{aligned}$$

$$
\begin{aligned}
&= 1 - \left[\frac{(a_m+1)n_{m-1}+n_{m-2}}{(a_m+1)d_{m-1}+d_{m-2}} \times \frac{a_m d_{m-1}+d_{m-2}}{a_m n_{m-1}+n_{m-2}}\right] \\
&= 1 - \left[\frac{(a_m+1)n_{m-1}+n_{m-2}}{(a_m+1)d_{m-1}+d_{m-2}} \div \frac{a_m n_{m-1}+n_{m-2}}{a_m d_{m-1}+d_{m-2}}\right] \\
&= 1 - \frac{\frac{(a_{m+1})n_{m-1}+n_{m-2}}{(a_m+1)d_{m-1}+d_{m-2}}}{\frac{a_m n_{m-1}+n_{m-2}}{a_m d_{m-1}+d_{m-2}}} \\
&= 1 - \frac{[a_0, a_1, \ldots, a_m+1]}{[a_0, \ldots, a_m]}.
\end{aligned}
$$

Thus,

$$\delta < 1 - \frac{[a_0, a_1, \ldots, a_m+1]}{[a_0, a_1, \ldots, a_m]}, \tag{3.29}$$

which implies

$$1 - \frac{[a_0, a_1, \ldots, a_m+1]}{[a_0, a_1, \ldots, a_m]} > 1 - \frac{f'}{f} \quad \geq 0.$$

Since $f = [a_0, a_1, \ldots, a_m]$, we have

$$[a_0, \ldots, a_m+1] < f' \leq [a_0, a_1, \ldots, a_m]. \tag{3.30}$$

In general,

$$\delta < \frac{1}{\frac{3}{2}n_m d_m}, \tag{3.31}$$

is sufficient to guarantee the success of the continued fraction algorithm, where m could either be even or odd [22].

We now look at an example of applying the continued fraction algorithm

Example 3 Suppose we have m even and $m \geq 2$. By (3.31), we know that $\delta < \frac{1}{\frac{3}{2}n_m d_m}$ is sufficient to guarantee the success of the continued fraction algorithm.

Suppose that we have $f = \frac{n_m}{d_m} = \frac{56}{33} = (1; 1, 2, 3, 3)$. Here, $m = 4$.

Choose f' such that $\delta < \frac{1}{\frac{3}{2}n_m d_m}$. That is, choose f' such that $1 - \frac{f'}{f} < \frac{1}{\frac{3}{2} \times 56 \times 33}$.

Suppose we choose $f' = \frac{5542}{3267}$, which is one such value of f' that abides by the above inequality.

The partial quotients of f' are [1; 1, 2, 3, 2, 2, 4, 13].

Running Wiener's continued fraction algorithm gives the following

$$[a'_0, a'_0 + 1] \;=\; [1, 2] = \;\frac{3}{2} \neq f,$$

$$[a'_0, a'_1] \;= [1, 1] \;= 1 + \frac{1}{1} \;=\; 2 \neq f,$$

$$[a'_0, a'_1, a'_2 + 1] \;= [1, 1, 3] \;=\; \frac{7}{4} \neq f,$$

$$[a'_0, a'_1, a'_2, a'_3] \;=\; [1, 1, 2, 3] \;=\; \frac{17}{10} \neq f,$$

$$[a'_0, a'_1, a'_2, a'_3, a'_4 + 1] \;= [1, 1, 2, 3, 3] = \;\frac{56}{33} \;=\; f. \;\blacksquare$$

3.3 Wiener's algorithm applied to RSA

Recall from the RSA cryptosystem that by choosing the public exponent e such that $(e, (p-1)(q-1)) = 1$, we have an integer d such that

$$ed \equiv 1 \pmod{(p-1)(q-1)}). \tag{3.32}$$

Also, by [14]

$$ed \equiv 1 \pmod{lcm(p-1, q-1)}). \tag{3.33}$$

Since $lcm(p-1, q-1) = \frac{(p-1)(q-1)}{(p-1,q-1)}$, we divide out any possible common factors between $p-1$ and $q-1$. We already know that $(e, \phi(n)) = 1$. The greatest common divisor will still be 1 if we remove any common factors between $p-1$ and $q-1$. Thus $(e, \phi(n)) = 1 = (e, \frac{\phi(n)}{(p-1,q-1)}) = (e, lcm(p-1, q-1))$ and so (3.33) holds.

Even though (3.32) and (3.33) churn out different d values, both lead to the same m value being recovered.

Example 4 Given that $m = 2$, $e = 7$, $p = 11$, $q = 13$ and so $n = pq = 143$ and $(e, (p-1)(q-1)) = (7, 120) = 1$.
This would mean that $C \equiv m^e \pmod{n} \equiv 2^7 \pmod{143} \equiv 128$.

Using $ed \equiv 1 \pmod{(p-1)(q-1)}$ yields
$d = 7^{-1} \pmod{120} = 103$ so that
$m = c^d \pmod{n} = 128^{103} = 2$.

Using $ed \equiv 1 \pmod{lcm(p-1, q-1)}$ yields
$d = 7^{-1} \pmod{60} = 43$ so that
$m = c^d \pmod{n} = 128^{43} = 2$. $\blacksquare$

In Section 2.2, we unpacked the decryption process for RSA given that (3.32) holds. We briefly unpack the decryption process given that (3.33) holds:

Let $G =(p-1, q-1)$. Note that lcm(p - 1, q - 1) $= \frac{(p-1)(q-1)}{G}$.

So $ed \equiv 1 \pmod{lcm(p-1, q-1)}$ implies that $ed \equiv 1 \pmod{\frac{(p-1)(q-1)}{G}}$ and by definition of congruence, there exists an integer k such that
$ed = 1 + k(p-1)(q-1)/G$.

Case 1: $(m, pq) = 1$.

$$\begin{aligned} C^d &\equiv (m^e)^d \pmod{pq} \\ &\equiv m^{1+k(p-1)(q-1)/G} \pmod{pq} \\ &\equiv m^1 \cdot (m^{(p-1)(q-1)/G})^k \pmod{pq} \\ &\equiv m \cdot 1^k \pmod{pq} \\ &\equiv m \pmod{pq}. \end{aligned}$$

The second last line is true by Euler's formula, where $G = 1$, since $(m, pq) = 1$.

Case 2: $(m, pq) > 1$
If m is divisible by exactly one of p and q, say $p|m$ and $q \nmid m$, then $p|m$ implies that $m \equiv c^d \equiv 0(\mod p)$ but since $q \nmid m$, it means that $(q, m) = 1$ and so

$$\begin{aligned} C^d &\equiv (m^e)^d \pmod{q} \\ &\equiv m^{1+k(p-1)(q-1)/G} \pmod{q} \\ &\equiv m^1 \cdot (m^{(p-1)(q-1)/G})^k \pmod{q} \\ &\equiv m \cdot 1^k \pmod{q} \quad \text{(By Euler's formula)} \\ &\equiv m \pmod{q}. \end{aligned}$$

Furthermore, when $m = 0$, we have $(m, pq) = (0, pq) = pq > 1$, which then gives the same result as above. ■

Congruence (3.33) implies that there must exist an integer K such that

$$ed = K \cdot lcm(p-1, q-1) + 1. \tag{3.34}$$

This is due to the definition of congruence. In general, $x \equiv y \pmod{m}$ is the same as saying that $m|x-y$ and there exists an integer k such that $x - y = km$. That is, $x = km + y$. In the case of (3.34), $x = ed$, $k = K$, $m = lcm\ (p-1, q-1)$ and $y = 1$.

Letting $G = (p-1, q-1)$ and using the fact that $lcm(p-1, q-1) = \frac{(p-1)(q-1)}{G}$, we obtain

$$ed = \frac{K}{G}(p-1)(q-1) + 1. \tag{3.35}$$

Since it is possible for K and G to have common factors, we can define $k = K\ /\ (K, G)$ and $g = G\ /\ (K, G)$, so that $k\ /\ g = K\ /\ G$ and $(k, g) = 1$. (3.35) now becomes

$$ed = \frac{k}{g}(p-1)(q-1) + 1. \tag{3.36}$$

Dividing through by dpq in (3.36) gives

$$\frac{e}{pq} = \frac{k}{dg}(1-\delta), \ \ where \ \delta = \frac{p+q-1-\frac{g}{k}}{pq}. \tag{3.37}$$

Since e is public information and $n = pq$ is also public information, $\frac{e}{pq}$ is known information and it is a close underestimate of $\frac{k}{dg}$, which is unknown since d is the secret exponent. In using the continued fraction algorithm, we can recover what $\frac{k}{dg}$ is. However, before making use of the continued fraction algorithm, we look at some further analysis.

From (3.34), we see that $(K, d) = 1$. Since $k = K/\ (K, G)$, it means that k is a divisor of K. Hence, $(k, d) = 1$.
Also, as justified previously, $(k, g) = 1$ (Recall if $(a, b) = d$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$).

Since $(k, d) = 1$ and $(k, g) = 1$, we know that $(k, dg) = 1$ and Wiener's algorithm can be used to find k and dg as long as δ is small enough. To be precise,

$$kdg < \frac{pq}{\frac{3}{2}(p+q)}, \tag{3.38}$$

is sufficient to allow k and dg to be found [22]. We proceed to show how (3.38) is derived.

In Chapter 2, we defined $f = \frac{n_m}{d_m}$. In this case, $f = \frac{k}{dg}$ where $n_m = k$ and $d_m = dg$. By (3.31),

$$\delta < \frac{1}{\frac{3}{2}n_m d_m}.$$

In this case,

$$\delta < \frac{1}{\frac{3}{2}kdg}.$$

As indicated in (3.37), $\delta = \frac{p+q-1-\frac{g}{k}}{pq}$, so

$$\frac{p+q-1-\frac{g}{k}}{pq} < \frac{1}{\frac{3}{2}kdg},$$

i.e.

$$\frac{3}{2}kdg(p+q-1-\frac{g}{k}) < pq$$

so that

$$kdg < \frac{pq}{\frac{3}{2}(p+q)}.$$

Note that $-1-\frac{g}{k}$ in the expression of δ was dropped because it is small compared to $(p+q)$. This does not affect the validity of (3.38) because $-1-\frac{g}{k}$ serves to reduce the size of δ [22].

Wiener's attack will find secret exponents up to a size of approximately 2^{255}. If $d > 2^{255}$, then (3.38) would not hold anymore and thus Wiener's attack would no longer be applicable.

Chapter 4

A VARIANT ON WIENER'S ATTACK

In this chapter, we explore the paper titled *Continued fractions and RSA with small secret exponent* by A. Dujella [5]. This paper follows Wiener's ideas very closely with the aim of developing a more efficient variant of Wiener's attack.

4.1 A further look at Wiener's attack

Theorem 2.4.11 proved that $\left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2}$ given that $p < q < 2p$, $e < n$ and $d < \frac{1}{3}\sqrt[4]{n}$. By Theorem 2.4.12, $\frac{k}{d}$ is a convergent of the continued fraction of $\frac{e}{n}$ given that the conditions from Theorem 2.4.11 hold. The secret exponent d is the denominator of some convergent of the continued fraction of $\frac{e}{n}$, for $d < n^{0.25}$. Therefore, d can be computed efficiently from the public key (e, n).

There are many convergents of $\frac{e}{n}$. The correct convergent that will give $\frac{e}{n}$ using Wiener's algorithm will have $d < \frac{1}{3}\sqrt[4]{n}$. However, there is more than one convergent that may meet this criterion. There is a way to find the correct convergent without having to test all convergents. This is what we will now touch on.
Assuming that $p < q < 2p$. Then as highlighted in [5],

$$2\sqrt{n} < p + q < \frac{3\sqrt{2}}{2}\sqrt{n} < 2.1214\sqrt{n}. \tag{4.1}$$

This implies

$$\frac{k}{d} - \frac{e}{n} = \frac{k(p+q) - k - 1}{dn} > \frac{2k(\sqrt{n} - 1)}{dn}. \tag{4.2}$$

We now expand on why (4.2) holds true.

$$\begin{aligned}
\frac{k}{d} - \frac{e}{n} &= \frac{kn - ed}{dn} \\
&= \frac{kn - ed - k\phi(n) + k\phi(n)}{dn} \\
&= \frac{(kn - k\phi(n)) - (ed - k\phi(n))}{dn} \\
&= \frac{kn - k\phi(n) - 1}{dn}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{k(n-\phi(n))-1}{dn} \\
&= \frac{k(pq-(p-1)(q-1))-1}{dn} \\
&= \frac{k(pq-(pq-p-q+1)-1}{dn} \\
&= \frac{k(pq-pq+p+q-1)-1}{dn} \\
&= \frac{k(p+q-1)-1}{dn} \\
&= \frac{kp+kq-k-1}{dn} \\
&= \frac{k(p+q)-k-1}{dn}.
\end{aligned}
$$

By (4.1), $p+q > 2\sqrt{n}$, and so

$$
\frac{k(p+q)-k-1}{dn} > \frac{2k(\sqrt{n}-1)}{dn} = \frac{k(2\sqrt{n})-2k}{dn}.
$$

Thus, (4.2) holds.

Since $\frac{k}{d} > \frac{e}{n} \cdot \frac{n}{n-2\sqrt{n}+1}$ [5], we observe

$$
\begin{aligned}
\frac{k}{d} - \frac{e}{n} &> \frac{en-e(n-2\sqrt{n}+1)}{n(n-2\sqrt{n}+1)} \\
&= \frac{en-en+2e\sqrt{n}-e}{n(\sqrt{n}-1)^2} \\
&= \frac{2e\sqrt{n}-e}{n(\sqrt{n}-1)^2} \\
&> \frac{2e\sqrt{n}-2e}{n(\sqrt{n}-1)^2} \\
&= \frac{2e(\sqrt{n}-1)}{n(\sqrt{n}-1)^2} \\
&= \frac{2e}{n(\sqrt{n}-1)} \\
&> \frac{2e}{n\sqrt{n}}.
\end{aligned}
$$

Hence, we see that

$$
\frac{k}{d} - \frac{e}{n} > \frac{2e}{n\sqrt{n}}. \tag{4.3}
$$

Using (4.2) and (4.1), we get

$$\frac{k}{d} - \frac{e}{n} = \frac{k(p+q) - k - 1}{dn} < \frac{k(2.1214\sqrt{n})}{dn} = \frac{2.1214k}{d\sqrt{n}}.$$

Thus,

$$\frac{k}{d} - \frac{e}{n} < \frac{2.1214k}{d\sqrt{n}}. \tag{4.4}$$

Combining (4.3) and (4.4) gives

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2.1214k}{d\sqrt{n}}.$$

Assuming that $n > 10^8$, then as highlighted in [5], we have $\frac{k}{d} < 1.00023\frac{e}{n}$, and

$$\frac{k}{d} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}}. \tag{4.5}$$

Combining (4.5) and (4.3) gives

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}}. \tag{4.6}$$

$\frac{k}{d}$ is a unique (odd) convergent satisfying (4.6). This follows from the fact that if $\frac{p_m}{q_m}$ and $\frac{p_{m+2}}{q_{m+2}}$ are two successive (odd) convergents of a real number α, then $\frac{p_{m+2}}{q_{m+2}}$ is at least a twice better approximation of α than $\frac{p_m}{q_m}$, which is a direct consequence of Theorem 2.4.10.

If $\frac{k}{d} = \frac{p_m}{q_m}$ and $\frac{e}{n} = \frac{p_{m+1}}{q_{m+1}}$, then using Lemma 2.4.3 below, we have

$$\begin{aligned}
\frac{k}{d} - \frac{e}{n} &= \frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}} \\
&= \frac{p_m q_{m+1} - q_m p_{m+1}}{q_m q_{m+1}} \\
&= \frac{-q_m p_{m+1} + p_m q_{m+1}}{q_m q_{m+1}} \\
&= \frac{-(q_m p_{m+1} - p_m q_{m+1})}{q_m q_{m+1}} \\
&= \frac{-(-1)^m}{q_m q_{m+1}} \\
&= \frac{-(-1)}{q_m q_{m+1}} \\
&= \frac{1}{q_m q_{m+1}}.
\end{aligned}$$

(By assuming $\frac{k}{d} = \frac{p_m}{q_m}$ to be an odd convergent, it means that m is odd such that $(-1)^m = -1$ which gives a positive numerator of $-(-1)$ in the last few lines of the above steps).

Thus, we see that with $\frac{k}{d} = \frac{p_m}{q_m}$, we have $\frac{k}{d} - \frac{e}{n} = \frac{1}{q_m q_{m+1}}$ and (4.6) becomes

$$\frac{2e}{n\sqrt{n}} < \frac{1}{q_m q_{m+1}} < \frac{2.122e}{n\sqrt{n}}.$$

Inverting the above inequality gives

$$\frac{n\sqrt{n}}{2e} > q_m q_{m+1} > \frac{n\sqrt{n}}{2.122e}.$$

Now,

$$\frac{n\sqrt{n}}{2.122e} > \frac{n\sqrt{n}}{4.224e}.$$

So,

$$\frac{n\sqrt{n}}{2e} > q_m q_{m+1} > \frac{n\sqrt{n}}{2.122e} > \frac{n\sqrt{n}}{4.224e},$$

which gives

$$\frac{n\sqrt{n}}{4.224e} < q_m q_{m+1} < \frac{n\sqrt{n}}{2e},$$

where m is the unique odd, positive integer satisfying this inequality.

In summary, the above observations lead to an efficient algorithm for finding the correct convergent in Wiener's attack. Namely, $\frac{k}{d} = \frac{p_m}{q_m}$, where m is the smallest odd, positive integer such that $q_m q_{m+1} > \frac{n\sqrt{n}}{4.224e}$.

As highlighted in [5], Wiener's attack can be slightly improved by using a better approximation to $\frac{k}{d}$, such as $\frac{e}{f}$, where $f = n - \lfloor 2\sqrt{n} \rfloor + 1$ and

$$0 < \frac{k}{d} - \frac{e}{f} < \frac{0.1221}{\sqrt{n}}.$$

If $d < 4.04 n^{\frac{1}{4}}$, then $\frac{0.1221}{\sqrt{n}} < \frac{2}{d^2}$ and d can be found in polynomial time [5].

Up till now, we have considered how to find the correct convergent of $\frac{e}{n}$ for which Wiener's algorithm would work. We also looked at how Wiener's algorithm can be improved slightly [5]. In the next section, we study a variant of Wiener's attack highlighted in A. Dujella's paper.

4.2 Verheul and Van Tilborg variant of Wiener's attack

In 1997, Verheul and van Tilborg proposed the following extension of Wiener's attack. Let m be the largest (odd) integer satisfying

$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}. \tag{4.7}$$

The aim is to search for $\frac{k}{d}$ between fractions of the form $rp_{m+1} + sp_m$ and $rq_{m+1} + sq_m$. Consider the linear system

$$rp_{m+1} + sp_m = k, \tag{4.8}$$

$$rq_{m+1} + sq_m = d. \tag{4.9}$$

Within this linear system, the assumption is that r and s are non-negative integers [5]. This means that the system has positive integer solutions.
By Lemma 2.4.3, $p_{m+1}q_m - q_{m+1}p_m = (-1)^m$. So the determinant is

$$|p_{m+1}q_m - q_{m+1}p_m| = 1.$$

Taking (4.8) and multiplying throughout by q_m gives

$$rp_{m+1}q_m + sp_mq_m = kq_m. \tag{4.10}$$

Taking (4.9) and multiplying throughout by p_m gives

$$rq_{m+1}p_m + sq_mp_m = dp_m. \tag{4.11}$$

Subtracting (4.11) from equation (4.10) gives

$$rq_{m+1}p_m - rp_{m+1}q_m + sq_mp_m - sq_mp_m = dp_m - kq_m.$$

So,

$$r(q_{m+1}p_m - p_{m+1}q_m) = dp_m - kq_m.$$

That is,

$$r(1) = dp_m - kq_m.$$

Giving

$$r = dp_m - kq_m. \tag{4.12}$$

Aside: By Lemma 2.4.3, $(q_{m+1}p_m - p_{m+1}q_m) = -(p_{m+1}q_m - q_{m+1}p_m) = -(-1)^m = 1$ where $(-1)^m = -1$ since m is odd.

Similarly, taking (4.8) and multiplying throughout by q_{m+1} gives

$$rp_{m+1}q_{m+1} + sp_mq_{m+1} = kq_{m+1}. \tag{4.13}$$

Taking (4.9) and multiplying throughout by p_{m+1} gives

$$rq_{m+1}p_{m+1} + sq_mp_{m+1} = dp_{m+1}. \tag{4.14}$$

Subtracting (4.13) from (4.14) gives

$$rp_{m+1}q_{m+1} - rq_{m+1}p_{m+1} + sp_mq_{m+1} - sq_mp_{m+1} = kq_{m+1} - dp_{m+1}.$$

So,

$$s(p_mq_{m+1} - q_mp_{m+1}) = kq_{m+1} - dp_{m+1}.$$

That is,

$$s(1) = kq_{m+1} - dp_{m+1}.$$

Giving

$$s = kq_{m+1} - dp_{m+1}. \tag{4.15}$$

If r and s in (4.12) and (4.15) are small, then they can be found by an exhaustive search (trial and error). In an exhaustive search, we formulate an algorithm to run through all possible values of r and all possible values of s. Finding upper bounds for r and s helps us to be sure that r is less than a certain quantity and s is less than a certain quantity. In this way, finding upper bounds for r and s assists in such an exhaustive search. We now proceed to find these upper bounds.

Recall Theorem 2.4.10

$$\frac{1}{q_m(q_{m+1} + q_m)} < \left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}}.$$

We can take α to be $\frac{k}{d}$ and terms within the absolute value can be swapped to give

$$\frac{1}{q_m(q_{m+1} + q_m)} < \left|\frac{p_m}{q_m} - \frac{k}{d}\right| < \frac{1}{q_m q_{m+1}}. \tag{4.16}$$

We can estimate the number of steps in this exhaustive search by finding upper bounds for r and s. Let $d = Dn^{\frac{1}{4}}$. Firstly, we look for another expression of r by taking (4.12) and transforming it

$$\begin{aligned} r &= dp_m - kq_m \\ &= \frac{dq_m dp_m}{dq_m} - \frac{dq_m kq_m}{dq_m} \\ &= dq_m\left(\frac{dp_m}{dq_m} - \frac{kq_m}{dq_m}\right) \\ &= dq_m\left(\frac{p_m}{q_m} - \frac{k}{d}\right). \end{aligned}$$

We now use this new expression of r to find an upper bound of r, making use of (4.16).

$$\begin{aligned} r &= dq_m\left(\frac{p_m}{q_m} - \frac{k}{d}\right) \\ &< dq_m\left(\frac{1}{q_m q_{m+1}}\right) \\ &= \frac{d}{q_{m+1}}. \end{aligned}$$

Hence,

$$r < \frac{d}{q_{m+1}}. \tag{4.17}$$

(4.17) gives an upper bound for r.

We now look for another expression of s by taking (4.15) and transforming it.

$$\begin{aligned} s &= kq_{m+1} - dp_{m+1} \\ &= \frac{dq_{m+1}kq_{m+1}}{dq_{m+1}} - \frac{dq_{m+1}dp_{m+1}}{dq_{m+1}} \\ &= dq_{m+1}\left(\frac{kq_{m+1}}{dq_{m+1}} - \frac{dp_{m+1}}{dq_{m+1}}\right) \\ &= dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right). \end{aligned}$$

So,

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right). \tag{4.18}$$

The estimate (upper bound) for s depends on the sign of the number

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} - \frac{2.122e}{n\sqrt{n}}.$$

We see why below by considering the case where the sign is positive vs the sign being negative. In each of the cases, we unpack what the upper bound for s is and what the upper bound is for the number of steps in the exhaustive search.

Case 1: The sign is positive, i.e.

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} - \frac{2.122e}{n\sqrt{n}} > 0.$$

This can also be written as

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} > \frac{2.122e}{n\sqrt{n}}.$$

Also, by (4.5)

$$\frac{k}{d} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}}.$$

This means that

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} > \frac{2.122e}{n\sqrt{n}} > \frac{k}{d} - \frac{e}{n}.$$

So,

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} > \frac{k}{d} - \frac{e}{n}.$$

That is,

$$-\frac{p_{m+1}}{q_{m+1}} > \frac{k}{d} - \frac{e}{n} - \frac{e}{n}.$$

So, we have

$$-\frac{p_{m+1}}{q_{m+1}} > \frac{k}{d} - 2\left(\frac{e}{n}\right).$$

This can also be written as

$$\frac{k}{d} - 2\left(\frac{e}{n}\right) < \frac{-dp_{m+1}}{dq_{m+1}}.$$

Multiplying by dq_{m+1} on both sides gives

$$dq_{m+1}\left(\frac{k}{d} - 2\frac{e}{n}\right) < -dp_{m+1}.$$

So,

$$dq_{m+1}\left(\frac{k}{d} - 2\frac{e}{n}\right) + dp_{m+1} < 0.$$

Expanding out gives

$$dq_{m+1}\frac{k}{d} - 2dq_{m+1}\frac{e}{n} + dp_{m+1} < 0,$$

i.e.

$$dq_{m+1}\frac{k}{d} + dp_{m+1} < 2dq_{m+1}\frac{e}{n}.$$

The left side can also be written as

$$dq_{m+1}\frac{k}{d} - dp_{m+1} + 2dp_{m+1} < 2dq_{m+1}\frac{e}{n}.$$

So,

$$dq_{m+1}\frac{k}{d} - dp_{m+1} < 2dq_{m+1}\frac{e}{n} - 2dp_{m+1}.$$

This can also be written as

$$dq_{m+1}\frac{k}{d} - dq_{m+1}\frac{p_{m+1}}{q_{m+1}} < 2dq_{m+1}\frac{e}{n} - 2dq_{m+1}\frac{p_{m+1}}{q_{m+1}}.$$

Taking out common factors on both sides gives

$$dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < 2dq_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right). \tag{4.19}$$

Combining (4.18) and (4.19) gives

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < 2dq_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right). \tag{4.20}$$

Next, we need to show that

$$2dq_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right) < \frac{2d}{q_{m+2}}.$$

Taking $\frac{e}{n}$ to be α gives the following (by (4.16))

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} < \frac{1}{q_{m+1}q_{m+2}}.$$

So,

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} < \frac{1}{q_{m+1}} \frac{1}{q_{m+2}}.$$

Multiplying both sides by q_{m+1} gives

$$q_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right) < \frac{1}{q_{m+2}}.$$

Multiplying both sides by $2d$ gives

$$2dq_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right) < \frac{2d}{q_{m+2}}. \tag{4.21}$$

Combining (4.20) and (4.21) gives

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < 2dq_{m+1}\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right) < \frac{2d}{q_{m+2}}. \tag{4.22}$$

From (4.22), we see that

$$s < \frac{2d}{q_{m+2}}. \tag{4.23}$$

Inequality (4.23) gives an upper bound for s in Case 1, assuming that $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} - \frac{2.122e}{n\sqrt{n}} > 0$.

We now expand on the upper bound for the number of steps in the exhaustive search for Case 1.
By (4.16), (where $\frac{k}{d}$ is replaced with α), we know that

$$\frac{1}{q_m(q_{m+1} + q_m)} < \left|\frac{p_m}{q_m} - \alpha\right|. \tag{4.24}$$

Replacing m by $m+2$ and taking $\alpha = \frac{e}{n}$, (4.24) becomes

$$\frac{1}{q_{m+2}(q_{m+3} + q_{m+2})} < \frac{p_{m+2}}{q_{m+2}} - \frac{e}{n}. \tag{4.25}$$

Note that we do not have an absolute value when subtracting e/n from p_{m+2}/q_{m+2} because the difference is positive due to the fact that p_{m+2}/q_{m+2} is above e/n (we know that e/n is between two successive convergents: p_{m+1}/q_{m+1} and p_{m+2}/q_{m+2}, where p_{m+1}/q_{m+1} is below e/n while p_{m+2}/q_{m+2} is above $\frac{e}{n}$).
Next, we aim to show that

$$\frac{1}{q_{m+2}^2(a_{m+3} + 2)} < \frac{1}{q_{m+2}(q_{m+3} + q_{m+2})}.$$

Recall that the a_i's are the partial quotients of a finite continued fraction and by Theorem 2.2.2, the q_i's are defined recursively as follows

$$q_0 = 1,$$

$$q_1 = a_1,$$

$$q_i = a_i q_{i-1} + q_{i-2}, \quad \text{for } i \geq 2.$$

In particular, for $i = m + 3$

$$q_{m+3} = a_{m+3} q_{m+2} + q_{m+1}.$$

So,

$$q_{m+3} - q_{m+1} = a_{m+3} q_{m+2}.$$

Dividing both sides by q_{m+2} to make a_{m+3} subject of formula gives

$$a_{m+3} = \frac{q_{m+3} - q_{m+1}}{q_{m+2}}. \tag{4.26}$$

The recursive definition of the q_i's above tells us that the q_i's form an increasing sequence (each successive q_i value will be bigger than the preceding q_i values). In particular

$$q_{m+2} > q_{m+1}.$$

So,

$$q_{m+3} - q_{m+1} > q_{m+3} - q_{m+2}$$

(since we subtract something smaller from q_{m+3} on the left side). This can also be re-written as

$$\left(\frac{q_{m+3} - q_{m+1}}{q_{m+2}} \right) q_{m+2} > q_{m+3} - q_{m+2}.$$

Substituting (4.26) on the left side gives

$$a_{m+3} q_{m+2} > q_{m+3} - q_{m+2}.$$

Dividing both sides by q_{m+2} gives

$$a_{m+3} > \frac{q_{m+3} - q_{m+2}}{q_{m+2}}.$$

This can also be written as

$$a_{m+3} > \frac{q_{m+3}}{q_{m+2}} - 1.$$

So,

$$a_{m+3} + 1 > \frac{q_{m+3}}{q_{m+2}}.$$

This can also be written as

$$a_{m+3} + 2 - 1 > \frac{q_{m+3}}{q_{m+2}}.$$

That is,

$$a_{m+3} + 2 > 1 + \frac{q_{m+3}}{q_{m+2}}.$$

Thus,

$$a_{m+3} + 2 > \frac{q_{m+2}}{q_{m+2}} + \frac{q_{m+3}}{q_{m+2}}.$$

Multiplying both sides by q_{m+2} gives

$$q_{m+2}(a_{m+3}+2) > q_{m+2}+q_{m+3}.$$

This can also be expressed as

$$\frac{q_{m+2}^2(a_{m+3}+2)}{q_{m+2}} > \frac{q_{m+2}^2}{q_{m+2}} + \frac{q_{m+2}q_{m+3}}{q_{m+2}}.$$

Multiplying by q_{m+2} on both sides gives

$$q_{m+2}^2(a_{m+3}+2) > q_{m+2}^2 + q_{m+2}q_{m+3}.$$

Taking out the common factor on the right side gives

$$q_{m+2}^2(a_{m+3}+2) > q_{m+2}(q_{m+2}+q_{m+3}).$$

Taking the reciprocals on both sides gives

$$\frac{1}{q_{m+2}^2(a_{m+3}+2)} < \frac{1}{q_{m+2}(q_{m+2}+q_{m+3})}. \tag{4.27}$$

Combining (4.25) and (4.27) gives

$$\frac{1}{q_{m+2}^2(a_{m+3}+2)} < \frac{1}{q_{m+2}(q_{m+2}+q_{m+3})} < \frac{p_{m+2}}{q_{m+2}} - \frac{e}{n}.$$

Thus, we have

$$\frac{1}{q_{m+2}^2(a_{m+3}+2)} < \frac{p_{m+2}}{q_{m+2}} - \frac{e}{n}. \tag{4.28}$$

By (4.7), m is the largest (odd) integer satisfying

$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}.$$

We expect that (4.7) will not hold for any odd integer greater than m due to the above assumption that m is the largest (odd) integer satisfying the above inequality.
In particular, if we replace m with $m+2$, (where $m+2$ is odd with $m+2 > m$), the above inequality will not hold, otherwise we would have a contradiction to the assumption that m is the largest (odd) integer satisfying the above inequality.
So it must be that

$$\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} \leq \frac{2.122e}{n\sqrt{n}}.$$

However,

$$\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} \neq \frac{2.122e}{n\sqrt{n}}.$$

So it must be that

$$\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}}.$$

By assumption, $e < n$ and so $e/n < 1$. Therefore,

$$\frac{2.122e}{n\sqrt{n}} < \frac{2.122}{\sqrt{n}}.$$

In which case, we know that

$$\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}} < \frac{2.122}{\sqrt{n}}. \tag{4.29}$$

Combining (4.28) and (4.29) gives

$$\frac{1}{q_{m+2}^2(a_{m+3}+2)} < \frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}} < \frac{2.122}{\sqrt{n}}. \tag{4.30}$$

Inequalities (4.30) imply that

$$\frac{1}{q_{m+2}^2(a_{m+3}+2)} < \frac{2.122}{\sqrt{n}}.$$

Taking reciprocals on both sides gives

$$\frac{q_{m+2}^2(a_{m+3}+2)}{1} > \frac{\sqrt{n}}{2.122}.$$

Dividing both sides by $a_{m+3}+2$ gives

$$q_{m+2}^2 > \frac{\sqrt{n}}{2.122(a_{m+3}+2)}.$$

Taking square roots on both sides gives

$$q_{m+2} > \frac{\sqrt[4]{n}}{\sqrt{2.122(a_{m+3}+2)}}. \tag{4.31}$$

So,

$$\frac{1}{q_{m+2}} < \frac{\sqrt{2.122(a_{m+3}+2)}}{\sqrt[4]{n}}. \tag{4.32}$$

Also, clearly

$$a_{m+2}q_{m+1} + q_{m+1} > q_{m+2} = a_{m+2}q_{m+1} + q_m.$$

That is,

$$q_{m+1}(a_{m+2}+1) > q_{m+2}.$$

So,

$$q_{m+1} > \frac{q_{m+2}}{(a_{m+2}+1)}. \tag{4.33}$$

Hence,

$$\frac{1}{q_{m+1}} < \frac{(a_{m+2}+1)}{q_{m+2}}. \tag{4.34}$$

Putting all these estimates together (using the fact that $d = D\sqrt[4]{n}$ and using (4.17), (4.34) and (4.32)), gives

$$\begin{aligned} r &< \frac{d}{q_{m+1}} \\ &= d\left(\frac{1}{q_{m+1}}\right) \\ &< d \cdot \frac{(a_{m+2}+1)}{q_{m+2}} \\ &= d \cdot (a_{m+2}+1) \cdot \frac{1}{q_{m+2}} \\ &< d \cdot (a_{m+2}+1) \cdot \frac{\sqrt{2.122(a_{m+3}+2)}}{\sqrt[4]{n}} \\ &= D\sqrt[4]{n} \cdot (a_{m+2}+1) \cdot \frac{\sqrt{2.122(a_{m+3}+2)}}{\sqrt[4]{n}} \\ &= D \cdot (a_{m+2}+1) \cdot \sqrt{2.122(a_{m+3}+2)}. \end{aligned}$$

Hence, we have

$$r < \sqrt{2.122(a_{m+3}+2)}(a_{m+2}+1)D. \tag{4.35}$$

With regards to s, recall by (4.18) that

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right).$$

By (4.16), we know that

$$\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < \frac{1}{q_{m+1}q_{m+2}}.$$

Combining (4.18) and (4.16) gives

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < dq_{m+1}\left(\frac{1}{q_{m+1}q_{m+2}}\right) = \frac{d}{q_{m+2}}.$$

So,

$$s < \frac{d}{q_{m+2}}. \tag{4.36}$$

Again, using the fact that $d = D\sqrt[4]{n}$ and using (4.36) and (4.32) gives

$$\begin{aligned} s &< \frac{d}{q_{m+2}} \\ &= d \cdot \frac{1}{q_{m+2}} \\ &< d \cdot \frac{\sqrt{2.122(a_{m+3}+2)}}{\sqrt[4]{n}} \end{aligned}$$

$$= D\sqrt[4]{n} \cdot \frac{\sqrt{2.122(a_{m+3}+2)}}{\sqrt[4]{n}}$$
$$= D \cdot \sqrt{2.122(a_{m+3}+2)}.$$

Hence, we have

$$s < \sqrt{2.122(a_{m+3}+2)}D. \tag{4.37}$$

So, multiplying the upper bounds of r and s gives that the maximum number of steps to find r and s in Case 1 is bounded by $2.122(a_{m+3}+2)(a_{m+2}+1)D^2$.

Case 2: The sign is negative. That is,

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} - \frac{2.122e}{n\sqrt{n}} \leq 0.$$

This can also be written as

$$\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} \leq \frac{2.122e}{n\sqrt{n}}.$$

By (4.7), m be the largest (odd) integer satisfying

$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}}.$$

Also, by (4.5)

$$\frac{2.122e}{n\sqrt{n}} > \frac{k}{d} - \frac{e}{n}.$$

So,

$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{2.122e}{n\sqrt{n}} > \frac{k}{d} - \frac{e}{n}.$$

That is,

$$\frac{p_m}{q_m} - \frac{e}{n} > \frac{k}{d} - \frac{e}{n}.$$

Adding $\frac{e}{n}$ on both sides gives

$$\frac{p_m}{q_m} > \frac{k}{d}.$$

This can also be written as

$$\frac{p_m}{q_m} > \frac{k}{d} - \frac{p_{m+1}}{q_{m+1}} + \frac{p_{m+1}}{q_{m+1}}.$$

Re-arranging the terms gives

$$\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}} > \frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}.$$

Multiplying both sides by dq_{m+1} gives

$$dq_{m+1}\left(\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right) > dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) = s.$$

(We know that s is equal to the quantity on the extreme right by (4.18)).

So, we have

$$s = dq_{m+1}\left(\frac{k}{d} - \frac{p_{m+1}}{q_{m+1}}\right) < dq_{m+1}\left(\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right) = \frac{d}{q_m}. \tag{4.38}$$

Note for the terms on the extreme right of (4.38):

$$\begin{aligned} dq_{m+1}\left(\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right) &= dq_{m+1}\left(\frac{p_m q_{m+1} - q_m p_{m+1}}{q_m q_{m+1}}\right) \\ &= dq_{m+1}\left(\frac{1}{q_m q_{m+1}}\right) \\ &= \frac{d}{q_m}. \end{aligned}$$

So, the upper bound of s in Case 2 is

$$s < \frac{d}{q_m}. \tag{4.39}$$

We now expand on the upper bound for the number of steps in exhaustive search for Case 2.

Since in this case $\frac{p_{m+1}}{q_{m+1}}$ is close enough to $\frac{e}{n}$, we have an estimate for q_{m+1} which is analogous to the estimate of q_{m+2} in Case 1.

As with Case 1, we have

$$\frac{1}{q_{m+1}^2(a_{m+2}+2)} < \frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} < \frac{2.122e}{n\sqrt{n}} < \frac{2.122}{\sqrt{n}}.$$

So,

$$\frac{1}{q_{m+1}^2(a_{m+2}+2)} < \frac{2.122}{\sqrt{n}}.$$

Inverting gives

$$q_{m+1}^2(a_{m+2}+2) > \frac{\sqrt{n}}{2.122}.$$

Dividing both sides by $a_{m+2}+2$ gives

$$q_{m+1}^2 > \frac{\sqrt{n}}{2.122(a_{m+2}+2)}.$$

Taking square roots on both sides gives

$$q_{m+1} > \frac{\sqrt[4]{n}}{\sqrt{2.122(a_{m+2}+2)}}. \tag{4.40}$$

Inverting gives

$$\frac{1}{q_{m+1}} < \frac{\sqrt{2.122(a_{m+2}+2)}}{\sqrt[4]{n}}. \tag{4.41}$$

Also

$$a_{m+1}q_m + q_m > q_{m+1} = a_{m+1}q_m + q_{m-1}.$$

That is,

$$q_m(a_{m+1} + 1) > q_{m+1}.$$

So,

$$q_m > \frac{q_{m+1}}{(a_{m+1} + 1)}. \tag{4.42}$$

Inverting gives

$$\frac{1}{q_m} < \frac{(a_{m+1} + 1)}{q_{m+1}}. \tag{4.43}$$

Putting all these estimates together (using the fact that $d = D\sqrt[4]{n}$ and using (4.17) and (4.41)), gives

$$\begin{aligned} r &< \frac{d}{q_{m+1}} \\ &= d \cdot \frac{1}{q_{m+1}} \\ &< d \cdot \frac{\sqrt{2.122(a_{m+2} + 2)}}{\sqrt[4]{n}} \\ &= D\sqrt[4]{n} \cdot \frac{\sqrt{2.122(a_{m+2} + 2)}}{\sqrt[4]{n}} \\ &= D\sqrt{2.122(a_{m+2} + 2)}. \end{aligned}$$

Hence,

$$r < \sqrt{2.122(a_{m+2} + 2)}D. \tag{4.44}$$

With regards to s, we also use the fact that $d = D\sqrt[4]{n}$ and make use of (4.39), (4.43) and (4.41) below to give

$$\begin{aligned} s &< \frac{d}{q_m} \\ &= d \cdot \frac{1}{q_m} \\ &< d \cdot \frac{(a_{m+1} + 1)}{q_{m+1}} \\ &= d \cdot (a_{m+1} + 1) \cdot \frac{1}{q_{m+1}} \\ &< d \cdot (a_{m+1} + 1) \cdot \frac{\sqrt{2.122(a_{m+2} + 2)}}{\sqrt[4]{n}} \\ &= D\sqrt[4]{n} \cdot (a_{m+1} + 1) \cdot \frac{\sqrt{2.122(a_{m+2} + 2)}}{\sqrt[4]{n}} \\ &= D(a_{m+1} + 1)\sqrt{2.122(a_{m+2} + 2)}. \end{aligned}$$

Hence,

$$s < \sqrt{2.122(a_{m+2}+2)}(a_{m+1}+1)D. \tag{4.45}$$

As explained in Case 1, the number of steps for the exhaustive search of r and s can be found by multiplying the upper bound of r with the upper bound of s. In Case 2, we multiply (4.44) with (4.45) to give that the maximum number of steps to find r and s is bounded by $2.122(a_{m+2}+2)(a_{m+1}+1)D^2$. Note that the number of steps in this attack is dependent on the partial quotients of a finite continued fraction. Particularly a_{m+1}, a_{m+2} and a_{m+3}. The time estimate can be generalised to $O(D^2)$ with some coefficients that depend on the partial quotients a_{m+1}, a_{m+2} and a_{m+3}. Some attacks attempt to remove dependency on partial quotients.

Chapter 5

IMPROVEMENT TO WIENER'S ATTACK

In this chapter, we survey a paper by M. Bunder and J. Tonien [2] which presents a new improved attack on RSA based on Wiener's technique using continued fractions. Both the original and improved methods make use of the public key (e, n) where n is a 1024-bit modulus. However, instead of using the convergents of the continued fraction of $\frac{e}{n}$ as in Wiener's original attack, the new method uses the convergents of the continued fraction of $\frac{e}{n'}$ where n' is given by

$$\left\lfloor n - \left(1 + \frac{3}{2\sqrt{2}}\right) n^{\frac{1}{2}} + 1 \right\rfloor.$$

5.1 The method

We now go on to explore the new method in more detail, starting with a lemma that leads to the main theorem making up this method.

Lemma 5.1.1 For $n > 2000000 = 2 \times 10^6$, we have

$$\frac{(\frac{3}{\sqrt{2}} - 2)n^{\frac{1}{2}} + 4}{2(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2} < \frac{1}{16n^{\frac{3}{2}}}.$$

Proof: By assumption, $n > 2000000 = 2 \times 10^6$, so

$$1515811 < 2000000 < n.$$

That is,

$$\left(\frac{32 + 3\sqrt{2}}{17 - 12\sqrt{2}}\right)^2 < 2000000 < n.$$

Thus,

$$\left(\frac{32 + 3\sqrt{2}}{17 - 12\sqrt{2}}\right)^2 < n.$$

Taking square roots gives

$$\left(\frac{32 + 3\sqrt{2}}{17 - 12\sqrt{2}}\right) < n^{\frac{1}{2}}.$$

The above inequality will still hold true if we add a term to the right side

$$\frac{32+3\sqrt{2}}{17-12\sqrt{2}} < n^{\frac{1}{2}} + \frac{9}{2(17-12\sqrt{2})n^{\frac{1}{2}}}.$$

Multiplying both sides by $(17-12\sqrt{2})n^{\frac{1}{2}}$ gives

$$\iff (32+3\sqrt{2})n^{\frac{1}{2}} < (17-12\sqrt{2})n + \frac{9}{2}.$$

$$\iff 8n^{\frac{1}{2}}\left[\frac{3}{\sqrt{2}}n^{\frac{1}{2}} - 2n^{\frac{1}{2}} + 4\right] < n - 3\sqrt{2}n^{\frac{1}{2}} + \frac{9}{2}.$$

$$\iff 8n^{\frac{3}{2}}\left[\left(\frac{3}{\sqrt{2}} - 2\right)n^{\frac{1}{2}} + 4\right] < n^2 - 3\sqrt{2}n^{\frac{3}{2}} + \frac{9}{2}n.$$

$$\iff 8n^{\frac{3}{2}}\left[\left(\frac{3}{\sqrt{2}} - 2\right)n^{\frac{1}{2}} + 4\right] < \left(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}}\right)^2.$$

Multiplying both sides by 2 gives

$$\iff 16n^{\frac{3}{2}}\left[\left(\frac{3}{\sqrt{2}} - 2\right)n^{\frac{1}{2}} + 4\right] < 2\left(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}}\right)^2.$$

$$\iff \frac{(\frac{3}{\sqrt{2}} - 2)n^{\frac{1}{2}} + 4}{2(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2} < \frac{1}{16n^{\frac{3}{2}}}. \quad \blacksquare$$

Theorem 5.1.2 In the RSA algorithm, if the following conditions are satisfied

$$q < p < 2q,$$

$$0 < e < \phi(n),$$

$$ed - k\phi(n) = 1,$$

$$n > 2000000 = 2 \times 10^6,$$

$$d < 2\sqrt{2}\left(\frac{n}{e}\right)^{\frac{1}{2}} n^{\frac{1}{4}},$$

$$n' = \left\lfloor n - \left(1 + \frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}} + 1 \right\rfloor,$$

then $\frac{k}{d}$ is a convergent of $\frac{e}{n'}$. Thus the secret information p, q, d, k can be recovered from public information (e, n).

Proof: Let $\phi_1 = n + 1 - \frac{3}{\sqrt{2}}n^{\frac{1}{2}}$ and $\phi_2 = n + 1 - 2n^{\frac{1}{2}}$.

Since $q < p < 2q$ (by assumption), we see that

$$q < p.$$

Dividing both sides by q gives

$$1 < \frac{p}{q}.$$

Taking square roots on both sides gives

$$1 < \sqrt{\frac{p}{q}}. \tag{5.1}$$

From the assumption $q < p < 2q$, we see that

$$p < 2q.$$

Dividing both sides by q gives

$$\frac{p}{q} < 2.$$

Taking square roots on both sides gives

$$\sqrt{\frac{p}{q}} < \sqrt{2}. \tag{5.2}$$

Combining (5.1) and (5.2) gives

$$1 < \sqrt{\frac{p}{q}} < \sqrt{2}. \tag{5.3}$$

Suppose we have a function

$$f(x) = x + \frac{1}{x}.$$

We know that this is an increasing function on $[1, +\infty)$.
If we take x to be a variable such that $1 < x < \sqrt{2}$, this would imply that

$$f(1) < f(x) < f(\sqrt{2}),$$

where

$$f(1) = 1 + \frac{1}{1} = 2,$$

$$f(\sqrt{2}) = 1 + \frac{1}{\sqrt{2}} = \frac{3}{\sqrt{2}}.$$

This tells us that if we assign any value of x that is between 1 and $\sqrt{2}$, the following identity always holds

$$2 < x + \frac{1}{x} < \frac{3}{\sqrt{2}}.$$

In particular, if we take x to be $\sqrt{\frac{p}{q}}$ (we know by (5.3) that $\sqrt{\frac{p}{q}}$ lies between 1 and $\sqrt{2}$), then we will have

$$2 < \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \frac{3}{\sqrt{2}}.$$

This can also be written as

$$2 < \frac{p+q}{n^{\frac{1}{2}}} < \frac{3}{\sqrt{2}}.$$

Multiplying by $n^{\frac{1}{2}}$ throughout gives

$$2n^{\frac{1}{2}} < p + q < \frac{3}{\sqrt{2}} n^{\frac{1}{2}}. \tag{5.4}$$

Dividing by -1 throughout gives

$$-2n^{\frac{1}{2}} > -(p+q) > -\frac{3}{\sqrt{2}}n^{\frac{1}{2}}.$$

Adding $n+1$ throughout gives

$$n+1-2n^{\frac{1}{2}} > n+1-p-q > n+1-\frac{3}{\sqrt{2}}n^{\frac{1}{2}}.$$

So,

$$\phi_2 > \phi(n) > \phi_1. \tag{5.5}$$

Let

$$\phi_{mid} = n - \left(1+\frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}} + 1.$$

Then $n' = \lfloor \phi_{mid} \rfloor$ and ϕ_{mid} is the midpoint of the interval $[\phi_1, \phi_2]$.
Note that ϕ_{mid} is not an integer because we have square roots that are irrational numbers making it up.
We have $\phi(n) \in (\phi_1, \phi_2)$.
So,

$$\begin{aligned} |\phi(n) - n'| &= |\phi(n) - \phi_{mid} + \phi_{mid} - n'| \\ &< |\phi(n) - \phi_{mid}| + |\phi_{mid} - n'|. \end{aligned}$$

We make use of the triangle inequality in the last line. (We have a strict inequality because $|\phi(n) - n'|$ is an integer but $|\phi(n) - \phi_{mid}| + |\phi_{mid} - n'|$ is not an integer). Thus, we have

$$|\phi(n) - n'| < |\phi(n) - \phi_{mid}| + |\phi_{mid} - n'|. \tag{5.6}$$

Next, we aim to show that

$$|\phi(n) - \phi_{mid}| + |\phi_{mid} - n'| < \frac{1}{2}(\phi_2 - \phi_1) + 1.$$

In (5.4), we saw that $2n^{\frac{1}{2}} < p+q$. The left side of (5.4) can also written as

$$\frac{4+3\sqrt{2}}{4}n^{\frac{1}{2}} - \frac{3\sqrt{2}}{4}n^{\frac{1}{2}} + n^{\frac{1}{2}} < p+q.$$

Regrouping terms

$$\frac{4+3\sqrt{2}}{4}n^{\frac{1}{2}} - p - q < \frac{3\sqrt{2}}{4}n^{\frac{1}{2}} - n^{\frac{1}{2}}.$$

That is,

$$\frac{4+3\sqrt{2}}{4}n^{\frac{1}{2}} - p - q < \frac{-4+3\sqrt{2}}{4}n^{\frac{1}{2}}$$

$$
\begin{aligned}
&= \frac{1}{2}\left(\frac{-4+3\sqrt{2}}{2}n^{\frac{1}{2}}\right) \\
&= \frac{1}{2}\left[\left(\frac{3}{\sqrt{2}}-2\right)n^{\frac{1}{2}}\right] \\
&= \frac{1}{2}\left(n+1-2n^{\frac{1}{2}}-n-1+\frac{3}{\sqrt{2}}n^{\frac{1}{2}}\right) \\
&= \frac{1}{2}\left[\left(n+1-2n^{\frac{1}{2}}\right)-\left(n+1-\frac{3}{\sqrt{2}}n^{\frac{1}{2}}\right)\right] \\
&= \frac{1}{2}(\phi_2-\phi_1).
\end{aligned}
$$

So, we have

$$\frac{4+3\sqrt{2}}{4}n^{\frac{1}{2}}-p-q<\frac{1}{2}(\phi_2-\phi_1).$$

The left side of the above inequality can also be written as

$$pq-pq-1+1+\left(1+\frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}}-p-q<\frac{1}{2}(\phi_2-\phi_1).$$

Rearranging terms on the left gives

$$pq-p-q+1-pq+\left(1+\frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}}-1<\frac{1}{2}(\phi_2-\phi_1).$$

That is,

$$(p-1)(q-1)-n+\left(1+\frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}}-1<\frac{1}{2}(\phi_2-\phi_1).$$

This can also be written as

$$\phi(n)-\left(n-\left(1+\frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}}+1\right)<\frac{1}{2}(\phi_2-\phi_1).$$

Thus,

$$\phi(n)-\phi_{mid}<\frac{1}{2}(\phi_2-\phi_1).$$

If $\phi(n)\geq\phi_{mid}$ (that is $\phi(n)-\phi_{mid}\geq 0$), then it is clear that

$$|\phi(n)-\phi_{mid}|<\frac{1}{2}(\phi_2-\phi_1).$$

If $\phi(n)<\phi_{mid}$, we need to prove that the above inequality still holds true using a proof by contradiction.

Under the assumption $\phi(n)<\phi_{mid}$, suppose that

$$|\phi(n)-\phi_{mid}|\geq\frac{1}{2}(\phi_2-\phi_1).$$

In this case, we have

$$\begin{aligned}|\phi(n) - \phi_{mid}| &= -(\phi(n) - \phi_{mid}) \\ &= \phi_{mid} - \phi(n).\end{aligned}$$

So, we have

$$\phi_{mid} - \phi(n) = |\phi(n) - \phi_{mid}| \geq \frac{1}{2}(\phi_2 - \phi_1).$$

That is,

$$\phi_{mid} - \phi(n) \geq \frac{1}{2}(\phi_2 - \phi_1).$$

So,

$$\frac{\phi_1 + \phi_2}{2} - \phi(n) \geq \frac{\phi_2 - \phi_1}{2}.$$

Rearranging terms gives

$$\frac{\phi_1 + \phi_2}{2} - \frac{\phi_2 - \phi_1}{2} \geq \phi(n).$$

Meaning

$$\frac{\phi_2 - \phi_2 + \phi_1 + \phi_1}{2} \geq \phi_(n).$$

So,

$$\phi_1 \geq \phi_n,$$

which is a contradiction to (5.5).

So, for both cases $\phi(n) > \phi_{mid}$ and $\phi(n) < \phi_{mid}$, we have

$$|\phi(n) - \phi_{mid}| < \frac{1}{2}(\phi_2 - \phi_1). \tag{5.7}$$

Since $n' = \lfloor \phi_{mid} \rfloor$ then by properties of floor functions, we know that

$$0 < |\phi_{mid} - n'| < 1. \tag{5.8}$$

Adding $|\phi_{mid} - n'|$ to both sides of (5.7) gives

$$|\phi(n) - \phi_{mid}| + |\phi_{mid} - n'| < \frac{1}{2}(\phi_2 - \phi_1) + |\phi_{mid} - n'|.$$

By (5.8), we know that $|\phi_{mid} - n'| < 1$ and so,

$$|\phi(n) - \phi_{mid}| + |\phi_{mid} - n'| < \frac{1}{2}(\phi_2 - \phi_1) + 1 = \frac{1}{2}(\phi_2 - \phi_1 + 2). \tag{5.9}$$

Combining (5.6) and (5.9) gives

$$|\phi(n) - n'| < |\phi(n) - \phi_{mid}| + |\phi_{mid} - n'| < \frac{1}{2}(\phi_2 - \phi_1) + 1 = \frac{1}{2}(\phi_2 - \phi_1 + 2).$$

Thus, we have

$$|\phi(n) - n'| < \frac{1}{2}(\phi_2 - \phi_1 + 2). \tag{5.10}$$

Next, we establish some very important inequalities that we make use of later on.

$$\phi_1 = n + 1 - \frac{3}{\sqrt{2}}n^{\frac{1}{2}} < n + 1 - \frac{4+3\sqrt{2}}{4}n^{\frac{1}{2}} = n'.$$

(The inequality in the middle is due to the fact that we subtract something bigger on the left as opposed to the right).
So, we have

$$\phi_1 < n'. \tag{5.11}$$

By (5.5), we know that

$$\phi_1 < \phi(n).$$

So, by (5.11) and (5.5), we know that

$$\phi_1 \cdot \phi_1 < \phi(n) \cdot n'.$$

Taking reciprocals gives

$$\frac{1}{\phi_1^2} > \frac{1}{n'\phi(n)}. \tag{5.12}$$

Taking (5.5) and adding 1 to the right side of the inequality then multiplying the first term by $k > 1$ still makes the inequality hold true:

$$\phi_1 < k\phi(n) + 1. \tag{5.13}$$

So, by (5.5) and (5.13), we have

$$\phi_1 \cdot \phi_1 < \phi(n) \cdot (k\phi(n) + 1).$$

Taking reciprocals gives

$$\frac{1}{\phi_1^2} > \frac{1}{\phi(n)(k\phi(n) + 1)}. \tag{5.14}$$

Another important fact to recall is that since e and d are inverses of each other, we have an integer k such that

$$ed - k\phi(n) = 1.$$

This can be re-written as

$$ed = 1 + k\phi(n). \tag{5.15}$$

Another important inequality

$$\phi_1^2 > (\phi_1^2 - 1).$$

Taking reciprocals gives

$$\frac{1}{\phi_1^2} < \frac{1}{(\phi_1^2 - 1)}. \tag{5.16}$$

We use (5.10), (5.12), (5.14), (5.15) and (5.16) in the computations on the next page. We also make use of the triangle inequality in the eighth line, as well as the definitions of ϕ_1

and ϕ_2 in the last line.

$$\begin{aligned}
\left|\frac{e}{n'}-\frac{k}{d}\right| &= \left|\frac{e}{n'}-\frac{e}{\phi(n)}+\frac{e}{\phi(n)}-\frac{k}{d}\right| \\
&= \left|\left(\frac{e}{n'}-\frac{e}{\phi(n)}\right)+\left(\frac{e}{\phi(n)}-\frac{k}{d}\right)\right| \\
&= \left|\frac{e\phi(n)-en'}{n'\phi(n)}+\frac{ed-k\phi(n)}{d\phi(n)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{1}{d\phi(n)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{(k\phi(n)+1)}{d\phi(n)(k\phi(n)+1)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{ed}{d\phi(n)(k\phi(n)+1)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{e}{\phi(n)(k\phi(n)+1)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{e}{\phi(n)(k\phi(n)+1)}\right| \\
&= \left|\frac{e(\phi(n)-n')}{n'\phi(n)}+\frac{e}{\phi(n)(k\phi(n)+1)}\right| \\
&< \frac{e|\phi(n)-n'|}{n'\phi(n)}+\frac{e}{\phi(n)(k\phi(n)+1)} \\
&< \frac{e\left[\frac{1}{2}(\phi_2-\phi_1+2)\right]}{\phi_1^2}+\frac{e}{\phi_1^2} \\
&= \frac{e(\phi_2-\phi_1+1)/2+e}{\phi_1^2} \\
&= \frac{e(\phi_2-\phi_1+1)+2e}{2\phi_1^2} \\
&= \frac{e\phi_2-e\phi_1+3e}{2\phi_1^2} \\
&< \frac{e\phi_2-e\phi_1+4e}{2\phi_1^2} \\
&< \frac{e(\phi_2-\phi_1+4)}{2(\phi_1-1)^2} \\
&= e\frac{(\frac{3}{\sqrt{2}}-2)n^{\frac{1}{2}}+4}{2(n-\frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2}.
\end{aligned}$$

Thus,

$$\left|\frac{e}{n'}-\frac{k}{d}\right| < e\frac{(\frac{3}{\sqrt{2}}-2)n^{\frac{1}{2}}+4}{2(n-\frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2}. \tag{5.17}$$

Recall by Lemma 5.1.1 that for $n > 2 \times 10^6$, we have

$$\frac{(\frac{3}{\sqrt{2}} - 2)n^{\frac{1}{2}} + 4}{2(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2} < \frac{1}{16n^{\frac{3}{2}}}.$$

Therefore, (5.17) can be written as

$$\left|\frac{e}{n'} - \frac{k}{d}\right| < \frac{e}{16n^{\frac{3}{2}}}.$$

Now, recall our underlying assumption

$$d^2 e < 8n^{\frac{3}{2}}.$$

Dividing both sides by $8n^{\frac{3}{2}} \cdot d^2$ gives

$$\frac{e}{8n^{\frac{3}{2}}} < \frac{1}{d^2}.$$

Multiplying both sides by $\frac{1}{2}$ gives

$$\frac{e}{16n^{\frac{3}{2}}} < \frac{1}{2d^2}.$$

So, we have

$$\left|\frac{e}{n'} - \frac{k}{d}\right| < \frac{e}{16n^{\frac{3}{2}}} < \frac{1}{2d^2}.$$

So,

$$\left|\frac{e}{n'} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Hence, by Theorem 2.4.12, $\frac{k}{d}$ is a convergent of $\frac{e}{n'}$. ■

This result is similar to that of the following theorem adapted from *Blomer and May, 2004* [1]. It is an attack on RSA based on factoring n, which is as follows

Theorem 5.1.3 Let (e, n) be an RSA public key, where $n = pq$. Suppose that e satisfies an equation $ex + y \equiv 0 \mod \phi(n)$ with

$$0 < x \leq \frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}, \tag{5.18}$$

and

$$|y| \leq \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ex. \tag{5.19}$$

Then n can be factored in time polynomial in $\log n$.

With $x = d$, (5.18) becomes

$$d < \frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}.$$

Squaring both sides gives

$$\begin{aligned} d^2 &< \left(\frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}\right)\cdot\left(\frac{1}{3}\sqrt{\frac{\phi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q}\right) \\ &= \frac{1}{9}\cdot\frac{\phi(n)}{e}\cdot\frac{n^{\frac{3}{2}}}{(p-q)^2}. \end{aligned}$$

So, we have

$$d^2 < \frac{1}{9}\cdot\frac{\phi(n)}{e}\cdot\frac{n^{\frac{3}{2}}}{(p-q)^2}.$$

Multiplying both sides by e gives

$$ed^2 < \frac{\phi(n)n^{\frac{3}{2}}}{9(p-q)^2}. \tag{5.20}$$

With $x = d$ and $y = -1$, (5.19) becomes

$$|-1| < \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ed.$$

So, we have

$$1 < \frac{p-q}{\phi(n)n^{\frac{1}{4}}}ed.$$

Multiplying both sides by $\phi(n)n^{\frac{1}{4}}$ gives

$$\phi(n)n^{\frac{1}{4}} < (p-q)ed. \tag{5.21}$$

Inequalities (5.20) and (5.21) are the conditions needed for the method by *Blomer and May* [1] to work, while the method by *Bunder, M. and Tonien, J.* [2] needs only one bound / condition to work, which is

$$ed^2 < 8n^{\frac{3}{2}}. \tag{5.22}$$

Let R be the ratio between the bound in (5.22) and the bound in (5.20).

$$\begin{aligned} R &= \frac{8n^{\frac{3}{2}}}{\frac{\phi(n)n^{\frac{3}{2}}}{9(p-q)^2}} \\ &= \frac{8n^{\frac{3}{2}}}{1}\times\frac{9(p-q)^2}{\phi(n)n^{\frac{3}{2}}} \\ &= \frac{72(p-q)^2}{\phi(n)} \\ &= \frac{n}{\phi(n)}\cdot\frac{72(p-q)^2}{n}. \end{aligned}$$

We now derive another way to express R.

$$\begin{aligned}
R =& \frac{n}{\phi(n)} \frac{72(p-q)^2}{pq} \\
&= \frac{n}{\phi(n)} \frac{72(p^2-2pq+q^2)}{pq} \\
&= \frac{n}{\phi(n)} \frac{72(\frac{p^2-2pq+q^2}{q})}{p} \\
&= \frac{n}{\phi(n)} \frac{72\left(\frac{p^2q}{q^2} - \frac{2pq}{q} + q\right)}{p} \\
&= \frac{n}{\phi(n)} \frac{72q\left(\frac{p^2}{q^2} - \frac{2p}{q} + 1\right)}{p} \\
&= \frac{n}{\phi(n)} \frac{72q\left(\frac{p}{q} - 1\right)^2}{p} \\
&= \frac{n}{\phi(n)} \frac{72\left(\frac{p}{q} - 1\right)^2}{1} \times \frac{q}{p} \\
&= \frac{n}{\phi(n)} \frac{72\left(\frac{p}{q} - 1\right)^2}{1} \div \frac{p}{q} \\
&= \frac{n}{\phi(n)} \frac{72\left(\frac{p}{q} - 1\right)^2}{\frac{p}{q}}.
\end{aligned}$$

Thus,

$$R = \frac{n}{\phi(n)} \frac{72(p-q)^2}{pq} = \frac{n}{\phi(n)} \frac{72\left(\frac{p}{q} - 1\right)^2}{\frac{p}{q}}.$$

We know that $q < p < 2q$. Dividing throughout by q gives $1 < \frac{p}{q} < 2$.

Consider the function

$$f(x) = \frac{72(x-1)^2}{x}, \text{ for } x \in (1,2).$$

We observe that $f(x) = 1$ for $x = \frac{9}{8}$, $f(x) < 1$ for $x \in (1, \frac{9}{8})$ and $f(x) > 1$ for $x \in (\frac{9}{8}, 2)$.

So for $x = \frac{p}{q}$ such that

$$f\left(\frac{p}{q}\right) = \frac{72\left(\frac{p}{q} - 1\right)^2}{\frac{p}{q}},$$

if $\frac{p}{q} \in \left(\frac{9}{8}, 2\right)$, then

$$R = \frac{n}{\phi(n)} f\left(\frac{p}{q}\right) > 1.$$

(This is because we know that if $\frac{p}{q} \in \left(\frac{9}{8}, 2\right)$ then $f\left(\frac{p}{q}\right) > 1$ by our observation above. Also, $\frac{n}{\phi(n)} > 1$ since $n > \phi(n)$).

So for $\frac{p}{q} \in (\frac{9}{8}, 2)$, we have

$$R > 1.$$

That is,

$$R = \frac{8n^{\frac{3}{2}}}{\frac{\phi(n)n^{\frac{3}{2}}}{9(p-q)^2}} > 1,$$

implying that

$$8n^{\frac{3}{2}} > \frac{\phi(n)n^{\frac{3}{2}}}{9(p-q)^2}.$$

This tells us that the bound in (5.22) [2] is better than the bound in (5.20) [1], because the upper bound of (5.22) is much bigger than the upper bound of (5.20), allowing us to compensate for more possibilities of larger values for ed^2 in the upper bound proposed by [2], as opposed to the upper bound proposed by [1].

From Theorem 5.1.2, we have the following result:

Corollary 5.1.4 In the RSA algorithm, if the following conditions are satisfied:

$$q < p < 2q,$$

$$0 < e < \phi(n),$$

$$ed - k\phi(n) = 1,$$

$$n > 2 \times 10^6,$$

$$d < 2\sqrt{2}n^{\frac{1}{4}},$$

and

$$n' = \left\lfloor n - \left(1 + \frac{3}{2\sqrt{2}}\right) n^{\frac{1}{2}} + 1 \right\rfloor,$$

then $\frac{k}{d}$ is a convergent of $\frac{e}{n'}$. Thus, the secret information p, q, d, k can be recovered from public information (e, n) [2].

Note that Corollary 5.1.4 has $d < 2\sqrt{2}n^{\frac{1}{4}}$ while Wiener's result had $d < \frac{1}{3}n^{\frac{1}{4}}$.

Example 5 Suppose we have

$$p = 59,$$

$$q = 67,$$

$$pq = n = 3953,$$

$$\left\lfloor n - \left(1 + \frac{3}{2\sqrt{2}}\right) n^{\frac{1}{2}} + 1 \right\rfloor = n' = 3824,$$
$$(p-1)(q-1) = \phi(n) = 3828,$$
$$e = 589,$$
$$e^{-1} \mod (\phi(n)) = d = 13,$$
$$ed - k\phi(n) = 1 \text{ so } k = 2.$$

We see that

$$\frac{e}{n'} = \frac{589}{3824} = [0; 6, 2, 32, 4, 2],$$
$$\frac{k}{d} = \frac{2}{13} = [0; 6, 2],$$
$$\frac{e}{n} = \frac{589}{3953} = [0; 6, 1, 2, 2, 6, 1, 1, 2, 2].$$

Observe that the first three partial quotients of $\frac{k}{d}$ are the same as the first three partial quotients of $\frac{e}{n'}$. This tells us that using $\frac{e}{n'}$ allows us to get to $\frac{k}{d}$ without using Wiener's algorithm. On the other hand, by using $\frac{e}{n}$, we would need to use Wiener's algorithm to get $\frac{k}{d}$.

We also note that the upper bound for d in [2] is greater than the upper bound for d in [22]. So the new method [2] gives an improvement in terms of the bound of d.

Chapter 6

CONCLUSION

The focus of the dissertation has been on a method of cryptanalysis of the RSA cryptosystem. The RSA cryptosystem is one of the most commonly used cryptosystems today. Therefore, the identification of possible attacks is important to ensure increased security. The method of cryptanalysis identified by M.J. Wiener uses continued fractions as a tool of attack in the case of a short secret exponent being used in the RSA cryptosystem. The development of a continued fraction algorithm [22] has formed the basis of the attack. This attack has created a stir and led to the development of further literature by A. Dujella, M. Bunder and J. Tonien [2], [5] to study several variations and improvements to the attack. The dissertation has unpacked such variations and improvements to Wiener's attack where a larger bound for the secret exponent can be accommodated and a method had also been developed where the secret exponent can even be extracted without the use of Wiener's algorithm altogether [2]. At this point, a better way to avoid Wiener's attack would be to avoid the use of short secret exponents.

Appendix A

A code for Wiener's algorithm in SageMath

```
def f(a, b, c, d):
    j = a * 1/b
    l = c * 1/d
    e = 1 - (l/j)
    if a/b < c/d or e > 2/(3 * a * b):
        return "error"
    else:
        g = list(continued_fraction(a/b))
        n = len(g)
        h = continued_fraction(c/d)
        m = len(h)
        w = []
        i = 0
        w.append(h[0])
        while g != w and i < m:
            if i % 2 == 0:
                w.append(h[i] + 1)
                print(w)
                if g != w:
                    w = list(h[0: i + 1])
            elif i % 2 == 1:
                w.append(h[i])
                print(w)
            i = i + 1

    return w
```

Bibliography

[1] J. Blomer, and A. May, *A generalized Wiener attack on RSA*. In International Workshop on Public Key Cryptography, pp 1-13, Springer, 2004.

[2] M. Bunder, and J. Tonien, *A New Attack on the RSA Cryptosystem Based on Continued Fractions*, Malays. J. Math. Sci. 11 (2017), Special Issue: The 5th International Cryptology and Information Security Conference 2016, 45(57).

[3] H. Delfs and H. Knebl, *Introduction to Cryptography*, 2nd ed., Springer, 2006.

[4] J. F. Dooley, *History of Cryptography and Cryptanalysis*, Springer, 2018.

[5] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math Publ. **29** (2004), pp 101-112.

[6] A. Dujella, *Number Theory*, Školska knjiga, 2021.

[7] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2014.

[8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Taylor and Francis Group, 2008.

[9] A. Khinchin, *Continued fractions*, Dover, New York, 1997.

[10] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer, 1994.

[11] N. Koblitz, *Algebraic Aspects of Cryptography*, 2nd ed., Springer, 1999.

[12] G. Krishnan, *Continued fractions*, Cornell University, 2016.

[13] A. Porges, *A Continued Fraction Cipher*, The American Mathematical Monthly, **59**(4)(1952), p 236.

[14] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM.***21**(2)(1978), pp 158 - 164.

[15] K. H. Rosen, *Elementary Number Theory and Its Applications*, 6th ed., Addison-Wesley, 1986 (reprinted).

[16] E. Schaefer, *An introduction to cryptography and cryptanalysis*, Santa Clara University, pp 45 - 49.

[17] W.T. Scott, H. S. Wall, *Continued Fractions*, National Mathematics Magazine, Vol. 13, No. 7, Taylor and Francis Ltd, pp 6 - 7, 1939.

[18] T. R. Shemanske, *Modern Cryptography and Elliptic curves*, American Mathematical Society, 2017.

[19] W. Stein, *Elementary Number Theory: Primes, Congruences, and secrets*, Springer, 2009.

[20] D. R. Stinson, *Cryptography Theory and Practice*, 2nd ed., Chapman and Hall, 2002.

[21] E. R. Verheul, H. C. A. Van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8**, pp 425 - 435, 1997.

[22] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory, **36**(3)(1990), pp 553-558.