Course of Cybersecurity for Data Science - Professor C. Ferretti - Academic year 2024/2025

Wiener attack in the RSA cryptosystem

Chiara Mariani 918354

Università degli Studi di Milano-Bicocca, CdLM Data Science

Contents

1 Introduction

The word cryptography comes from the Greek words *kryptos*, meaning hidden, and *graphien*, meaning to write. The main actors in this context are the original message we want to protect (plaintext), the encryption function which produces a new string or number called ciphertext and the decryption function which transforms back the message in order to make it understandable to the recipient.

Cryptography can be categorized into two main types: symmetric cryptography, where the same key is used both for encryption and decryption, and asymmetric cryptography, which uses a pair of keys (one private and one public). In 1977 Ronald Rivest, Adi Shamir and Leonard Adleman invented an asymmetric encryption algorithm called RSA.

The RSA algorithm is based on the difficulty of factoring a very large number into two prime numbers. Therefore, even if someone has access to the encrypted information and the public key, it is very difficult for him to discover the private key that is needed to decode the message.

2 Mathematical foundations

Before analyzing one possible attack to the RSA cryptosystem, the Wiener attack, we have to clarify some important mathematical concepts.

Definition 1. A finite continued fraction is an expression of the form

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

Let $a_0, a_1, a_2, \ldots, a_n$ be real numbers with $a_1, a_2, \ldots, a_n > 0$. 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 $a_0, a_1, a_2, \ldots, a_n$ are all integers.

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

Definition 2. The convergents of the finite simple continued fraction $[a_0; a_1, a_2, \ldots, a_n]$ are defined to be the numbers

$$C_k = [a_0; a_1, a_2, \ldots, a_n] \quad \text{for } k = 0, 1, 2, \ldots, n$$

C_k is called the kth convergent. For $k < n$, these convergents may also be called partial convergents. If

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

then

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

Theorem 1. Let $a_0, a_1, a_2, \ldots, a_n$ be the partial quotients of the finite simple continued fraction $[a_0; a_1, a_2, \ldots, a_n]$. Let the sequence $p_0, p_1, \ldots, p_n$ and $q_0, q_1, \ldots, q_n$ be defined recursively by

$$p_0 = a_0 \qquad \text{and} \qquad q_0 = 1$$

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

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

Then the kth convergent is given by

$$C_k = \frac{p_k}{q_k}$$

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

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

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

$$C_2 = [a_0; a_1, a_2] = \frac{a_0}{1} + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1a_2+1}{a_2}} = \frac{a_0}{1} + \frac{a_2}{a_1a_2+1} = \frac{a_0(a_1a_2+1)+a_2}{a_1a_2+1}$$

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

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 $a_k + \frac{1}{a_k+1}$ in the definition of C_k , to obtain

$$C_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] = \left[a_0; a_1, \ldots, a_k, a_k + \frac{1}{a_k+1}\right] = \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}$$

$$= \frac{(\frac{a_k(a_{k+1})+1}{a_{k+1}})p_{k-1} + p_{k-2}}{\frac{a_k(a_{k+1})+1}{a_{k+1}})q_{k-1} + q_{k-2}} = \frac{a_{k+1}(a_kp_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_kq_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

□

This Theorem can be used to find the fraction associated with a given finite simple continued fraction expression.

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

$$p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1} \tag{1.1}$$

$$p_kq_{k-2} - p_{k-1}q_k = (-1)^k a_k \tag{1.2}$$

Proof:

For (1.1), we firstly recall from Theorem 1 that

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

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

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

Now we assume that (1.1) 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

$$p_{k+1}q_k - p_kq_{k+1} = (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1})$$
$$= a_{k+1}p_kq_k + p_{k-1}q_k - a_{k+1}p_kq_k - p_kq_{k-1}$$
$$= p_{k-1}q_k - p_kq_{k-1} = -(p_kq_{k-1} - p_{k-1}q_k) = -(-1)^{k-1} = (-1)^1(-1)^{k-1} = (-1)^k$$

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

For (1.2), we 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, we have that

$$p_kq_{k-2} - p_{k-2}q_k = (a_kp_{k-1} + p_{k-2})q_{k-2} - (a_kq_{k-1} + q_{k-2})p_{k-2}$$
$$= a_kp_{k-1}q_{k-2} + p_{k-2})q_{k-2} - a_kp_{k-2}q_{k-1} - p_{k-2}q_{k-2}$$
$$= a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = (-1)^{k-2}a_k = (-1)^k a_k$$

□

Theorem 2. 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 are also integers for $1 \leq k \leq n-1$.
For $1 \leq k \leq n-1$, as seen in Lemma 1, since p_k and q_k are a result of combinations of multiplication and subtraction of a_k. it must be that p_k and q_k are integers as well.
Note that by (1.1) of Lemma 1, we have

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

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.
□

Theorem 3. (Legendre) If k, d, e and n are all distinct positive integers with d and n non-zero, $\gcd(k,d) = \gcd(e,n) = 1$ and

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

then $\frac{k}{d}$ is a convergent of the continued fraction $\frac{e}{n}$

Proof:
Let consider $n \leq d$, that means $\frac{n}{2d} \leq \frac{1}{2}$. Then $\frac{k}{d} - \frac{e}{n} < \frac{1}{2d^2}$ implies that

$$|kn - ed| \leq \frac{nd}{2d^2} \qquad \text{so that} \qquad |kn - ed| < \frac{n}{2d} \leq \frac{1}{2}$$

Thus, if $n \leq d$, then $|kn - ed| \leq \frac{1}{2}$ which would mean that $kn - ed = 0$. That is $kn = ed$ which would imply that $ed - k\phi(n) = 1$, where $\phi(n) = (p-1)(q-1)$, 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, $n > d$.

Now suppose that $\frac{k}{d}$ is not a convergent of the continued fraction $\frac{e}{n}$. 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

$$q_n < d < q_{n+1} \tag{3.1}$$

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

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

So,

$$\frac{1}{2d^2} > \left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \tag{3.2}$$

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,

$$|kq_n - dp_n| \geq 1 \tag{3.3}$$

Dividing both sides of (3.3) by $|dq_n|$, we obtain

$$\frac{kq_n - dp_n}{dq_n} \geq \frac{1}{dq_n} \tag{3.4}$$

Now, we can say that

$$\left|\frac{k}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{kq_n - dp_n}{dq_n}\right| - \left|\frac{q_n p_{n+1} - p_n q_{n+1}}{q_n q_{n+1}}\right| \geq \frac{1}{dq_n} - \frac{1}{q_n q_{n+1}} \tag{3.5}$$

where the numerator $kq_n - dp_n$ is a nonzero integer by (3.2) and by applying Lemma 1 to the numerator $q_n p_{n+1} - p_n q_{n+1}$ we obtain that it is equal to $(-1)^{n-1}$.

Combining (3.2) and (3.5), we have

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

So,

$$\frac{1}{2} > \frac{d}{q_n}\left(1 - \frac{1}{dq_{n+1}}\right) > 1 - \frac{d}{q_{n+1}}$$

meaning that

$$\frac{1}{2} < \frac{d}{q_{n+1}} \tag{3.6}$$

Since $q_n < d < q_{n+1}$ by (3.1), we know that the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ divide the line into three regions.

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 $\frac{k}{d}$ could be in any of these regions, we have the following cases:

Case 1: $\frac{k}{d}$ is between the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$

If $\frac{k}{d}$ is between the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, then by (3.3) we have that

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

We know that the assumption of Case 1 is that $\frac{k}{d}$ is between the convergents $\frac{p_n}{q_n}$ 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 to justify this inequality:

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

So, we see that $\frac{1}{dq_n} \leq \frac{1}{q_n q_{n+1}}$, which implies

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

Dividing both sides by q_n, we obtain

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

This is a contradiction to (3.1) which states that $q_n < d < q_{n+1}$.

Case 2: $\frac{k}{d}$ is not between the convergents $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$

Sub-case (2.a): $\frac{k}{d}$ is closer to $\frac{p_n}{q_n}$

From (3.4) and from the assumption that $\frac{k}{d}$ is closer to $\frac{p_n}{q_n}$ than $\frac{e}{n}$, we know that

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

Applying the hypothesis of this theorem, we have

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

We see that

$$q_n > 2d > d \qquad \text{implying} \qquad q_n > d$$

This is a contradiction to (3.1).

Sub-case (2.b): $\frac{k}{d}$ is closer to $\frac{p_{n+1}}{q_{n+1}}$

Applying the (3.4) and the assumptions of sub-case (2.b), we have

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

Applying the hypothesis of this theorem, we have

$$\frac{1}{dq_{n+1}} \leq \left|\frac{k}{d} - \frac{e}{n}\right| < \frac{1}{2d^2} \qquad \text{which implies} \qquad \frac{d}{q_{n+1}} < \frac{1}{2}$$

This contradicts (3.6).

Therefore, at the end we can conclude that $\frac{k}{d}$ must be a convergent of the continued fraction of $\frac{e}{n}$.
□

Theorem 4. Let $r \in \mathbb{R}$. For any $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$ such that

$$\left|r - \frac{a}{b}\right| < \frac{1}{2b^2} \qquad (b \geq 1)$$

then $\frac{a}{b}$ is convergent of r.

Proof:
Let the convergent of r be $\frac{h_j}{k_j}$ and suppose that $\frac{a}{b}$ is not a convergent.
The inequalities $k_n \leq b < k_{n+1}$ determine an integer n.
For this n, the inequality $|rb - a| < |rk_n - h_n|$ is impossible, therefore we have that

$$|rk_n - h_n| \leq |rb - a| < \frac{1}{2b},$$

$$\left|r - \frac{h_n}{k_n}\right| < \frac{1}{2bk_n}$$

Using the fact that $\frac{a}{b} \neq \frac{h_n}{k_n}$ and that $bh_n - ak_n$ is an integer, we find that

$$\frac{1}{bk_n} \leq \frac{|bh_n - ak_n|}{bk_n} = \left|\frac{h_n}{k_n} - \frac{a}{b}\right| \leq \left|r - \frac{h_n}{k_n}\right| + \left|r - \frac{a}{b}\right| < \frac{1}{2bk_n} + \frac{1}{2b^2}$$

This implies $b < k_n$ which is a contradiction.
□

3 RSA cryptosystem

The RSA cryptosystem is a public key cryptosystem. The procedure of RSA involves a public-key generation, along with a designated encryption and decryption algorithm.

To better understand how the RSA algorithm works, we can consider the following scenario. Suppose that Alice would like to make use of the RSA cryptosystem to receive private information from Bob without being intercepted by someone else. Therefore, Bob must first encode his message in such a way that Alice can easily decode the message and the others cannot. Let us assume that Alice and Bob decide to encode/decode the message using the RSA cryptosystem.

Public Key Generation

Firstly, Alice chooses two large distinct prime numbers p and q. She computes their product $N = pq$, where N is called modulus, and then she computes the Euler totient function namely

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

which represents the number of integers between 1 and $N-1$ that are coprime with N. She then picks a number e at random, called encryption exponent, where

$$1 < e < \phi(N)$$

and such that $\gcd(e, \phi(N)) = 1$. 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

$$(e, N)$$

is considered as the public key; this is available to anyone who would like to send Alice a private message.

Private Key Generation

Alice chooses another number d, called decryption exponent, such that $ed \equiv 1 \ (\mathrm{mod}\phi(N))$. The pair

$$(d, N)$$

is considered as private key. Bob does the same computations and has his own pair of public and private keys.
Since Alice is expecting a message M from Bob, she sends her public key across the channel to him without taking care if someone intercepts it.

Encryption and Decryption Process

To encrypt a message in RSA, Bob needs to first convert the message M into a number, where $0 \leq M < N$ (if the message is too big it could be split into several parts in order to convert it to a number).
Bob then proceeds to retrieve Alice's public key (e, N) and compute

$$C = M^e \ (\mathrm{mod}N)$$

The result is a ciphertext C that could be send to Alice.

In order to decrypt Bob's message, Alice uses her private key (d, N) computing

$$M = C^d \ (\mathrm{mod}N)$$

to retrieve the message.

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. Security could be compromised when an attacker is able to retrieve p and q, and so to retrieve a message by exploiting short public exponents and short RSA secret exponents.

3.1 Example

We illustrate the RSA cryptosystem with a small numerical example. Of, course this example is not secure since the numbers are so small that it would be easy for somebody to factor the modulus N.

Alice chooses two secret primes $p = 1223$ and $q = 1987$.
She computes the public modulus as:

$$N = p \cdot q = 2430101$$

She computes the Euler totient function as:

$$\phi(N) = (p-1)(q-1) = 1222 \cdot 1986 = 2426892$$

Then she chooses a public encryption exponent $e = 948047$ with the property that:

$$\gcd(e, \phi(N)) = \gcd(948047, 2426892) = 1$$

Bob converts his plaintext into an integer $M = 1070777$ satisfying $1 \leq m < N$.
He uses Alice's public key $(N, e) = (2430101, 948047)$ to compute the ciphertext as:

$$C = M^e \; (\text{mod} N) = 1070777^{948047} \pmod{2430101} = 1473513$$

Alice knows that $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$, so she can solve

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}, \qquad 948047 \cdot d \equiv 1 \pmod{2426892}$$

for d and finds that $d = 1051235$.
Alice takes the ciphertext $c = 1473513$ and computes

$$M = C^d \pmod{N} = 1473513^{1051235} \pmod{2430101} = 1070777$$

The value M that she computes is Bob's message.

4 Wiener's attack

We now discuss an attack on the RSA cryptosystem that utilizes continued fractions. Wiener's attack represents one of the most significant cryptanalysis techniques that exploits the properties of continuous fractions to compromise the security of the RSA system when short secret exponents are used. This attack is based on the observation that, under certain conditions, the continuous fraction of $\frac{e}{N}$ can reveal information crucial to determining the private key d.

In order to remove some ambiguity from the analysis, we let $N = pq$ where p and q are odd primes and determine the smallest $a \in \mathbb{N}$ such that $p < q < ap$. Since $ed \equiv 1 \,(\mathrm{mod}\phi(N))$, we can rewrite this expression as

$$\phi(N) = \frac{ed-1}{k} \qquad (k \in \mathbb{N}) \tag{A}$$

The main idea of Wiener's attack is to show that certain restrictions on d allow the fraction $\frac{k}{d}$ to be a convergent of $\frac{e}{n}$. The following lemmas are useful to show the convergence.

Lemma 2. Let $N = pq$ where p and q are distinct primes such that $p < q < ap$ for some $a \in \mathbb{N}$. Then

$$N - (a+1)\sqrt{N} < \phi(N) < N$$

Proof:
We first prove that $\phi(N) < N$. Clearly, $(p-1)(q-1) < pq$.
We next prove that $N - (a+1)\sqrt{N} < \phi(N)$, we begin with

$$\sqrt{N} > p > \frac{p}{a+1}$$

This statement implies

$$(a+1)\sqrt{N} > (a+1)(p) - 1 > (p+q) - 1$$

Finally, we have

$$N(a+1)\sqrt{N} < N - (p+q) + 1 = \phi(N)$$

□

Lemma 3. Let (N, e) be the public key with $N = pq$ such that $p < q < ap$ for some $a \in \mathbb{N}$. Furthermore, let k and d be defined in the equation (A). Then

$$\left|\frac{e}{N} - \frac{k}{N}\right| < \frac{(a+1)k}{d\sqrt{N}}$$

Proof:
By Lemma 2 and (A), we have that

$$k(N - (a+1)\sqrt{N}) < ed - 1$$

Dividing the inequality by dN and rearranging, we have

$$\frac{k}{d} - \frac{e}{N} < \frac{(a+1)k}{d\sqrt{N}} - \frac{1}{dN} \tag{3.a}$$

Furthermore, from (A) we have that $ed - 1 + 2 = k\phi(N) + 2$, so we see that

$$ed + 1 = k\phi(N) + 2 < kN + (a+1)k\sqrt{N}$$

Rearranging and dividing the inequality by dN, we have

$$-\left(\frac{(a+1)k}{d\sqrt{N}}-\frac{1}{dN}\right)<\frac{k}{d}-\frac{e}{N} \tag{3.b}$$

Combining (3.a) and (3.b) gives

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{(a+1)k}{d\sqrt{N}}-\frac{1}{dN}<\frac{(a+1)k}{d\sqrt{N}}$$

□

Lemma 4. Let k and d as in (A). Then $k<d$.

Proof:
Rearranging (A) and using the fact that $e<\phi(N)$, we have

$$\frac{d}{k}=\frac{k\phi(N)+1}{ek}>1$$

Hence $k<d$.
□

We are now ready to prove Wiener's main result that $\frac{k}{d}$ is a convergent of $\frac{e}{N}$ for certain values of d. In order to do this, we appeal to the Legendre Theorem by examining when

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

Theorem 5. We have that $\frac{k}{d}$ is a convergent of $\frac{e}{N}$ provided that

$$d\leq\frac{\sqrt[4]{N}}{2(a+1)}$$

Proof:
By Theorem 3 and Lemma 3, $\frac{k}{d}$ is a convergent of $\frac{e}{N}$ if

$$\frac{(a+1)k}{d\sqrt{N}}<\frac{1}{2d^2} \tag{5.1}$$

We proceed with the fact that (5.1) is true if and only if $2(a+1)kd<\sqrt{N}$.
Lemma 4 implies that

$$2(a+1)kd<2(a+1)d^2 \tag{5.2}$$

We maximize d by letting $2(a+1)d^2\leq\sqrt{N}$, which yields

$$d\leq\frac{\sqrt[4]{N}}{2(a+1)} \tag{5.3}$$

□

Observe from the previous theorem that the bound on d depends on a. As the value of a increases, the value of d that guarantees $\frac{k}{d}$ to be a convergent of $\frac{e}{N}$ decreases.

We have shown that $\frac{k}{d}$ is a convergent of $\frac{e}{N}$ and so we can use the properties of continued fractions to find d in an efficient way. This is the Wiener attack.

Some restrictions on d, specifically $d\leq\frac{\sqrt[4]{N}}{2(a+1)}$, allow the fraction $\frac{k}{d}$ to be a convergent of $\frac{e}{N}$. In practice, we know e and N from the public key, we compute the convergents of $\frac{e}{N}$ using the algorithm of continued fractions and for every convergents $\frac{p_i}{q_i}$ we verify if q_i can be d checking if $ed=1\ (\mathrm{mod}\phi(N))$.

4.1 Wiener Test

With Theorem 5 proved, we are now ready to put our results into practice to perform the Wiener attack.

The Wiener Test will guide us through the steps required to exploit the continuous fraction convergents of $\frac{e}{N}$ in order to determine the private key d. This test represents a practical application of the mathematical theories discussed.

Suppose we are able to express N as

$$N = x^2 - y^2 = (x-y)(x+y) \quad (x, y \in \mathbb{N}) \tag{B.1}$$

Since $N = pq$, we have either $p = x - y$ and $q = x + y$, or $1 = x - y$ and $N = x + y$. Solving for x and y in the first and second case respectively, gives

$$x = \frac{q+p}{2} \quad \text{and} \quad y = \frac{q-p}{2}$$

$$x = \frac{N+1}{2} \quad \text{and} \quad y = \frac{N-1}{2} \tag{B.2}$$

This method of factoring N is called Fermat's Factorization Algorithm.

We now see how to use these observations in Wiener's attack to determine the private key (p, q, d). Assuming $N = x^2 - y^2$ and that Theorem 5 is satisfied, we test each convergent sequentially. Let $\frac{k'}{d'}$ be the convergent of $\frac{e}{N}$ that we are testing. For each convergent $\frac{k'}{d'}$, let $\phi'(N)$, x' and y' be defined as follows:

$$\phi'(N) = \frac{ed' - 1}{k'} \tag{B.3}$$

$$x' = \frac{N - \phi'(N) + 1}{2} \tag{B.4}$$

$$y' = \sqrt{(x')^2 - N} \tag{B.5}$$

The following theorem is known as the Wiener Test, which tells us how to use x' and y' to find (p, q, d).

Theorem 6. (Wiener Test) Let $\frac{k'}{d'}$ be a convergent of $\frac{e}{N}$. If $x', y' \in \mathbb{N}$ are defined as in (B.4) and (B.5), then the private key (p, q, d) is given by

$$(p, q, d) = (x' - y', x' + y', d')$$

Proof:
Since $x', y' \in \mathbb{N}$, by (B.5) we have

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

Suppose $x' = \frac{N+1}{2}$, then (B.3) and (B.4) give

$$N + 1 = N - \frac{ed' - 1}{k'} + 1$$

which is only satisfied if $e = 1$. However, since $e > 1$, by (B.2) we have

$$x' = \frac{q+p}{2} \quad , \quad y' = \frac{q-p}{2}$$

Using (B.4), we have

$$\phi'(N) = N - (p + q) + 1 = \phi(N)$$

Since $\phi'(N) = \phi(N)$, it follows that

$$d' \equiv d \ (\mathrm{mod} \phi(N))$$

However, a lemma guarantees $d' \not> d$ because we are testing the convergents sequentially and since $1 < d < \phi(N)$, it follows that $d' = d$.
□

4.2 Example

Consider $N = 826513$ and $e = 589063$. To compute the partial quotients of the continued fraction $\frac{e}{N}$, we compute:

$$\frac{589063}{826513} = 0 \quad \text{rest} = 589063 \qquad \rightarrow \qquad a_0 = 0$$

$$\frac{826513}{589063} = 1 \quad \text{rest} = 237450 \qquad \rightarrow \qquad a_1 = 1$$

$$\frac{589063}{237450} = 2 \quad \text{rest} = 114163 \qquad \rightarrow \qquad a_2 = 2$$

$$\ldots \quad \text{and so on}$$

So, we continue untile the rest is equal to zero and we obtain

$$\frac{e}{N} = [0; 1, 2, 2, 12, 1, 1, 19, 1, 2, 5, 2, 6]$$

The first three convergents are

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

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

$$C_2 = [a_0; a_1, a_2] = \frac{p_2}{q_2} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{2}{3}$$

and all of these fail the Wiener Test.

We apply the Wiener Test to the next convergent

$$C_3 = [a_0; a_1, a_2, a_3] = \frac{p_3}{q_3} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{5}{7}$$

We begin with

$$\phi'(N) = \frac{7e - 1}{5} = \frac{7 \cdot 589063 - 1}{5} = 824688$$

which gives

$$x' = \frac{N - \phi'(N) + 1}{2} = 913 \qquad y' = \sqrt{(x')^2 - N} = 84$$

Since $x', y' \in \mathbb{N}$, by Theorem 6, $\frac{5}{7}$ is the correct convergent and so

$$(p, q, d) = (x' - y', x' + y', d') = (829, 997, 7)$$

5 Limits and improvements

Wiener's attack on the RSA cryptosystem exploits vulnerabilities that arise from the use of short secret exponents. The method leverages continued fractions to find the private key when the public exponent e is small compared to the modulus N. The effectiveness of this attack is contingent on the relationship between e, N and the private exponent d.

Specifically, if d is less than $\frac{1}{2}N^{0.25}$, the attack becomes feasible. In fact Theorem 3 proved that $\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{1}{2d^2}$ given that $p < q < 2p$, $e < N$ and $d < \frac{1}{3}N^{\frac{1}{4}}$; so we have that, under this condition, the secret exponent d is the denominator of some convergent of the continued fraction of $\frac{e}{N}$. Therefore, d can be computed efficiently from the public key (e, N).

While short exponents improve encryption speed, they also weaken security, making the system susceptible to factorization attacks. This vulnerability highlights the importance of choosing a sufficiently large e to mitigate risks. As such, cryptographic standards typically recommend using larger values of e to enhance security. The smallest possible value for e is 3, but to defeat certain attacks the value $e = 2^{16} + 1 = 65537$ is recommended. When the value $e = 2^{16} + 1$ is used, signature verification requires 17 multiplications, as opposed to roughly 1000 when a random $e < \phi(N)$ is used. Since typically N is 1024 bits, it follows that d must be at least 256 bits long in order to avoid the attack.

The limitations of Wiener's attack illustrate the delicate balance between performance and security in cryptographic implementations. Therefore, careful consideration is required when selecting key parameters in RSA to avoid potential exploits.

Wiener's attack has been significantly enhanced through mathematical and computational innovations. For example, new researches show that the bound could be improved from

$$d < \frac{1}{3}N^{\frac{1}{4}} \qquad \text{to} \qquad d \leq \frac{1}{\sqrt[4]{18}}N^{\frac{1}{4}}$$

In order to reach this result, instead of using the convergents of the continued fraction of $\frac{e}{N}$ as in Wiener's original attack, it should be used the convergents of the continued fraction of $\frac{e}{N_0}$, where N_0 is given by

$$N_0 = \left\lfloor N - \left(1 + \frac{3}{2\sqrt{2}}\right) N^{\frac{1}{2}} + 1 \right\rfloor$$

Subsequent improvements by Boneh and Durfee introduced the first significant advancement over Wiener's result: using the Coppersmith technique, a method was developed to break RSA when $d < N^{0.292}$. Using a somewhat more optimized lattice, another approach by Herrmann and May also derived the same bound $d < N^{0.292}$. This bound $d < N^{0.292}$ remains the best known to date.