IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 17, Issue 5 Ser. II (Sep. – Oct. 2021), PP 01-08
www.iosrjournals.org

Cryptanalysis on RSA Using Decryption Exponent

Ibrahim A. A.[1], Muhammad A. H[2], Shehu S.[3], Abubakar T. U.[4], Zaid I.[3], Bello U.[2]

[1]Department of Mathematics, Faculty of Science, Usmanu Danfodio University, Sokoto, Nigeria.
[2]Department of Science, Mathematics Unit, State Collage of Basic and Remedial Studies, Sokoto, Nigeria.
[3]Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.
[4]Department of Mathematics, Shehu Shagari College of Education,Sokoto, Nigeria.

Abstract
In this paper, we present two new decryption exponent cryptanalysis on RSA, which successfully lead to the factorization of RSA modulus $N = pq$ and prime power modulus $N = p^2q$ in polynomial time. We applied Wiener's technique of attack in RSA and developed the new attacks. In the first attack, we consider RSA with modulus $N = pq,\ for\ q < p < 2q$, with public encryption exponent e and private decryption exponent d. If $p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}$ and $d < \frac{(6-4\sqrt{2})(\sqrt{4+3\sqrt{2}})}{2}N^{1/4}$then N can be factored in polynomial time.Furthermorein the second attack, we consider $N - \left(2^{1/3}N^{1/3} - 2^{-2/3}N^{1/3} + 1\right)2^{1/3}N^{1/3}$as anapproximation of $\varphi(N)$ andd $< \frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3}-2^{1/3}\right)N^{1/3}+2^{1/3}\right]}}$ which also lead to factorization of N in polynomial time.

Keywords: *Prime power, Factorization, Cryptanalysis, Encryption, Decryption, Euler Toitient function, attacks and Continued fraction.*

Date of Submission: 02-09-2021 Date of Acceptance: 16-09-2021

I. Introduction

Underlying thebirth of modern cryptography is a great deal of fascinating mathematics,some of which has been developed for cryptographic applications, but most of which is taken from the classical mathematical canon.The most popular public key cryptosystem in use today is the RSA cryptosystem,introduced by Rivest, Shamir and Adleman (Dujella, 2004).Its security isbasedon the fact that it is hard to control or deal with as it involves large integer factorization problem and since then it has been extensively used for many applications in the government as well as commercial domain, which include e-banking, secure telephone, smart cards, and communications in different types of networks (Dubey et.al, 2014).

The first attack on small decryption exponent was reported by Wiener in 1990. He showed that RSA is insecure if the small decryption exponent $d < \frac{1}{3}N^{1/4}$using the continued fractions method to recover d from the convergents of the continued fractions expansion of $\frac{e}{N}$. Since then, many attacks on short decryption exponents emerged, which improved the bound.

Boneh and Durfe (1999) proposed an attack on the small decryption exponent in which they heuristically showed that RSA is insecure if $d < N^{0.292}$, as reported by Shehu and Ariffin (2017).

de Weger (2002) proposed a cryptosystem used the prime difference method to carry out an attack on RSA modulus $N = pq$, where he proved that if $d < \frac{N^{3/4}}{|p-q|}$, and then the RSA cryptosystem is considered to be insecure where primes $p\ and\ q$ have the same bit-length.

May (2003) considered RSA-type schemes with modulus $N = p^r q$for $r \geq 2$, and presented two new attacks for small secret exponent d. Both approaches are applications of Coppersmith's method for solving modular univariate polynomialequations. From these new attacks they directly derive partial keyexposure attacks, that is attacks when the secret exponent is not necessarilysmall but when a fraction of the secret key bits is known to the attacker, as reported by Shehu and Ariffin, (2017).

Maitra and Sarkar (2008) improved the work of de Weger using the prime difference method of $|2q - p| < N^\gamma$and showed that RSA is not secure if $d < N^\gamma$.

Chen's et al. (2009) have generalized the work of Maitra and Sarkar, where they proposed an attack using the generalization method, in which they proved that RSA modulus $N = pq$ can be broken if $|ap -$

$bq| = N^{\gamma}$and $d < N^{3/4-\gamma}$,where the ratio of two primes $\frac{p}{q}$is very near to the ratio $\frac{b}{a}$, where $p < q < 2p, a, and\ b$are small positive integers less than $log\, N$, then the RSA modulus can be factored from the convergent of the continued fraction expansion of$\frac{\mathrm{e}}{\mathrm{N}-\frac{3}{\sqrt{2}}\sqrt{\mathrm{N}}+1}$. Substituting$a = b = 1$ gave the approximation of $\varphi(N)$as reported by Ariffin et al., (2018).

Shehu and Ariffin (2017) presented three new attacks on Prime Power $N = p^r q$ using good approximation of $\varphi(N)$and continued fractions they showed that $\frac{k}{d}$can be recovered among the convergence ofthe continued fraction expansion of $\frac{e}{N-2N^{\overline{\frac{r}{r+1}}}+N^{\overline{\frac{r-1}{r+1}}}}$ and that one can factorthe modulus $N = p^r q$ in polynomial time.

Our Contribution: As motivated from recent results of Shehu and Ariffin (2017), Maitra and Sarkar (2008), May (2003), de Weger (2002), Boneh and Durfe (1999) and Wiener (1990).This paper, proposes two new attacks on RSA modulus $N = pq$ and RSA prime power moduli$N = p^2 q$ using continued fraction method. In the first attack we consider an instance of $p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}$ which is the average of Wiener's bound on RSA modulus $N = pq$ which lead to discover a decryption exponent $\mathrm{d} < \frac{(6-4\sqrt{2})(\sqrt{4+3\sqrt{2}})}{2}\mathrm{N}^{1/4}$and also lead to factorization of N in polynomial time.Similarly, in the second attack we consider $N - \Big(2^{1/3}N^{1/3} -$ *2−23N13+1213N13* as an approximation of *φN* for the RSA prime power modulus *N=p2q* which lead to discover a decryption exponent $d < \frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3}-2^{1/3}\right)N^{1/3}+2^{1/3}\right]}}$which also lead to factorization of N in polynomial time. All the two new attacks reported are stronger than that of Wiener.

The rest of this paper is structured as follows: In section 2, we give a briefreview of basic facts about the continued fractions, Euclidean algorithm for computation of Greatest Common Divisor (gcd) and Euler Totient function as well as Wiener's method of attack on RSA. In section 3 and 4, we put forward the first and second attacks. We conclude this paper in section 5.

II. Preliminaries

We start with definitions and important results concerning the continuedfractions,Euclidean algorithm for computation of Greatest Common Divisor (gcd) and Euler Totient function as well as some useful lemmas needed for the attacks.

2.1 Continued Fraction Expansion

A continued fraction is an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_m + \ddots}}} = [a_0,\ a_1, \dots,\ a_m,\ \dots]$$

where a_0 is an integer and a_m are positive integers for $m \geq 1$. The a_m are called the partial quotients of the continued fraction, (Ariffin and Shehu, 2016).

That is, continued fraction expansion of a number is formed by subtracting away the integer part of it and inverting the remainder and then repeating this process till it terminates.

Theorem 2.1(Legendre): Let $x \in \mathbb{R}$ and $\frac{\mathrm{p}}{\mathrm{q}}$be a rational fraction such that $\gcd(p,q) = 1$ and $q < b$ if $x = \frac{a}{b}$with $\gcd(a,b) = 1$. If$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$then $\frac{p}{q}$is a convergent of the continued fraction expansion of$x$.

2.2 Euclidean Algorithm

Suppose $m\ and\ n \in \mathbb{Z}$, with m> 0 there are unique integers q and r such that $n = mq + r$ and $0 \leq r < m$, q is called the quotient and r is the remainder when n is divided by m.

2.3 Greatest Common Divisor *(GCD)*

If m and n are integers we say that a positive integer d is the gcd of $m\ and\ n$ if d divide both m and n, and d is the multiple of all the other divisors of $m\ and\ n$.

2.4 The Euler Totient Function

ϕ is the Euler's function for which $\phi(n)$ when $n \geq 2,\ n \in \mathbb{Z}$ is the number of integers in the set $\{1, 2, 3, \dots, n-1$ which are coprime to n (i.e. *GCD ai, n=1, where ai=1, 2, ..., n−1).*

2.5 Wiener’s attack on RSA

A well-known attack on RSA with low secret-exponent d was given byWiener (Wiener, 1990). Wiener showed that using continued fractions, one can efficiently recover the secretexponent d from the public key (N, e)as long as $d < \frac{1}{3}N^{1/4}$. For $N = pq$ with $q < p < 2q$,we present below Wiener’s attack.

Weiner uses this useful lemma:

Lemma 2.1: Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N} \text{ and } 2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$$

Wiener’s Theorem: Let $N = pq$ with $q < p < 2q$, let $d < \frac{1}{3}N^{1/4}$. Given public key (N, e) with $ed \equiv 1\ mod\varphi(N)$, attacker can efficiently recover d.

Proof:

Using RSA key equation:

$$ed - k\varphi(N) = 1$$

Dividing the above equation by $d\varphi(N)$, we have:

$$\left|\frac{ed}{d\varphi(N)} - \frac{k\varphi(N)}{d\varphi(N)}\right| = \frac{1}{d\varphi(N)}$$

$$\Rightarrow \left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}$$

We have $\varphi(N) = (p - 1)(q - 1)$

$$= pq - p - q + 1$$
$$= N - (p + q) + 1$$

$$\Rightarrow N - \varphi(N) = p + q - 1$$

For which $N - \varphi(N) > 0$ and $p + q - 1 < 2q + q - 1$ (since $p < 2q$)

$$\Rightarrow \quad 0 < N - \varphi(N) \text{ and } p + q - 1 < 3q - 1 < 3q$$

But $N = pq > q^2$, we have that $q < \sqrt{N}$, hence:

$$p + q - 1 < 3\sqrt{N}$$

But $\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN}{dN}\right|$

But $ed = 1 + k\varphi(N)$

$$\Rightarrow \left|\frac{ed - kN}{dN}\right| = \left|\frac{1 + k\varphi(N) - kN}{dN}\right|$$
$$= \left|\frac{1 + k[\varphi(N) - N]}{dN}\right|$$
$$= \left|\frac{1 + k(p + q - 1)}{dN}\right| < \frac{3k\sqrt{N}}{dN}$$

$$< \frac{3k}{d\sqrt{N}}$$

Since $k < d$, we have:

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{3}{\sqrt{N}}$$

Using Legendre’s theorem,$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$

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

$$\Rightarrow \frac{k}{d} \text{is a convergent of the continued expansion of the fraction } \frac{e}{N}$$

$$\Rightarrow \frac{3}{\sqrt{N}} < \frac{1}{3d^2}$$

$$\Rightarrow 9d^2 < \sqrt{N}$$

$$\Rightarrow d^2 < \frac{\sqrt{N}}{9} \quad \Rightarrow \quad d < \frac{1}{3}N^{1/4}$$

2.6 Some Useful Lemmas

Lemma 2.2: Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N} \text{ and } p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}$$

Proof:

Since $N = pq \Rightarrow q = \frac{N}{p}$, with$q < p < 2q$

$$\Rightarrow \frac{N}{p} < p < 2\left(\frac{N}{p}\right)$$
$$\Rightarrow N < p^2 < 2N$$
$$\Rightarrow \sqrt{N} < p < \sqrt{2}\sqrt{N}(2.1)$$

Taking reciprocal of both sides:

$$\Rightarrow \frac{1}{\sqrt{2}\sqrt{N}} < \frac{1}{p} < \frac{1}{\sqrt{N}}$$

Multiplying both sides by N

$$\Rightarrow \frac{N}{\sqrt{2}\sqrt{N}} < \frac{N}{p} < \frac{N}{\sqrt{N}}$$
$$\Rightarrow \frac{1}{\sqrt{2}}\sqrt{N} < q < \sqrt{N}$$
$$\Rightarrow \frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N}(2.2)$$

Combining equation (2.1) and (2.2):

$$\Rightarrow \quad \frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}$$

To prove that $p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}$

Taking the average of the Wiener's bounds $2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$, we have:

$$\frac{2\sqrt{N} + \frac{3\sqrt{2}}{2}\sqrt{N}}{2} = \frac{4\sqrt{N} + 3\sqrt{2}\sqrt{N}}{4}$$

Hence, $p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}(2.3)$

Lemma 2.3: Let $N = p^2q$ be an RSA prime power modulus with $q < p < 2q$. Then

$$2^{-2/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$$

Proof:

For $N = p^2q, q = \frac{N}{p^2} \Rightarrow \frac{N}{p^2} < p < 2\left(\frac{N}{p^2}\right)$

$$\Rightarrow N < p^3 < 2N$$
$$\Rightarrow N^{1/3} < p < 2^{1/3}N^{1/3}(2.4)$$

Taking reciprocal of the above equation:

$$\Rightarrow \frac{1}{2^{1/3}N^{1/3}} < \frac{1}{p} < \frac{1}{N^{1/3}}$$

Square both sides:

$$\Rightarrow \frac{1}{2^{2/3}N^{2/3}} < \frac{1}{p^2} < \frac{1}{N^{2/3}}$$

Multiplying by N:

$$\Rightarrow \frac{N}{2^{2/3}N^{2/3}} < \frac{N}{p^2} < \frac{N}{N^{2/3}}$$
$$\Rightarrow \frac{N}{2^{2/3}N^{2/3}} < q < \frac{N}{N^{2/3}}$$
$$\Rightarrow 2^{-2/3}N^{1/3} < q < N^{1/3}(2.5)$$

Combining equation (2.4)and (2.5):

$$2^{-2/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$$

This terminates the proof.

2.7 Approximate Value of $\varphi(N)$ in Terms of N for $N = p^2 q$

For the RSA modulus $N = p^2q,\ and\ q < p < 2q$.

With $2^{-2/3}N^{1/3} < q < N^{1/3} < p < 2^{1/3}N^{1/3}$ we have:

$$\varphi(N) = p(p-1)(q-1)$$
$$= p^2q - p^2 - pq + p$$

$$= N - p^2 - pq + p(2.6)$$

Suppose $p \approx 2q$, i.e. $q \approx 2^{-2/3}N^{1/3}$ *and* $p \approx 2^{1/3}N^{1/3}$, equation (2.6) becomes:

$$\varphi(N) = N - \left(2^{1/3}N^{1/3}\right)^2 - \left(2^{1/3}N^{1/3}\right)2^{-2/3}N^{1/3} + 2^{1/3}N^{1/3}$$
$$= N - \left(2^{2/3}N^{2/3}\right) - \left(2^{-1/3}N^{2/3}\right) + 2^{1/3}N^{1/3}$$
$$= N - \left(2^{1/3}N^{1/3} - 2^{-2/3}N^{1/3} + 1\right)2^{1/3}N^{1/3} \qquad (2.7)$$

Which is a good approximation of $\varphi(N)$ in terms of N, for $N = p^2q$.

III. Our New Attacks

3.1 First Attack on RSA Modulus $N = pq$

Let $N = pq$ be an RSA modulus with $q < p < 2q$, $e < \varphi(N)$ be a public exponent and d the corresponding private key satisfying $ed = 1 + k\varphi(N)$. For

$$p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}\text{then} \quad d < \frac{(6-4\sqrt{2})\left(\sqrt{4+3\sqrt{2}}\right)}{2}N^{\frac{1}{4}}.$$

Proof:

From the RSA key equation $ed - k\varphi(N) = 1$

$\Rightarrow ed - k(p-1)(q-1) = 1$

$\Rightarrow ed - k(pq - p - q + 1) = 1$

$\Rightarrow ed - k[N + 1 - (p+q)] = 1$

$\Rightarrow ed - kN - k[1 - (p+q)] = 1$

$\Rightarrow ed - kN = 1 - k(p+q-1)$

Divide both sides by Nd:

$$\left|\frac{ed}{Nd} - \frac{kN}{Nd}\right| = \frac{|1 - k(p+q-1)|}{\mathrm{Nd}} < \frac{k(p+q-1)}{\mathrm{Nd}}$$

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{|1 - k(p+q-1)|}{\mathrm{Nd}}$$

$$< \frac{k(p+q-1)}{\mathrm{Nd}} (3.1)$$

But $\frac{k}{d} < 1$

Therefore, equation (3.1) becomes,

$$\frac{k(p+q-1)}{\mathrm{Nd}} < \frac{p+q-1}{\mathrm{N}}$$

hence,$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{p+q-1}{\mathrm{N}} < \frac{p+q}{\mathrm{N}}$

But $p + q < \frac{4+3\ \sqrt{2}}{4}\ \sqrt{N}$(from equation (2.3))

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{p+q}{N} \Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{4+3\ \sqrt{2}}{4}\ \sqrt{N} \cdot \frac{1}{N}$$

$$< \frac{4+3\ \sqrt{2}}{4}N^{\frac{1}{2}-1}$$

$$< \frac{4+3\ \sqrt{2}}{4}N^{-\frac{1}{2}}$$

Using Legendre's equation $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$

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

$\Rightarrow \frac{k}{d}$ is among the convergent of the continued expansion of the fraction $\frac{e}{N}$

$$\therefore\ \frac{4+3\ \sqrt{2}}{4}N^{-\frac{1}{2}} < \frac{1}{2d^2}$$

$$\Rightarrow\ 2d^2\left(\frac{4+3\ \sqrt{2}}{4}N^{-\frac{1}{2}}\right) < 1$$

$$\Rightarrow\quad d^2 < \frac{2\ \sqrt{N}}{4+3\ \sqrt{2}}$$

$$\Rightarrow\quad d < \sqrt{\frac{2\ \sqrt{N}}{4+3\ \sqrt{2}}}$$

$$< \frac{\sqrt{2}N^{\frac{1}{4}}}{\sqrt{4+3\sqrt{2}}}$$

$$< \frac{\sqrt{2}N^{\frac{1}{4}}}{\sqrt{4+3\sqrt{2}}} \cdot \frac{\sqrt{4+3\sqrt{2}}}{\sqrt{4+3\sqrt{2}}}$$

$$< \frac{\sqrt{2}\sqrt{4+3\sqrt{2}}N^{\frac{1}{4}}}{4+3\sqrt{2}}$$

$$< \frac{\sqrt{2}\sqrt{4+3\sqrt{2}}N^{\frac{1}{4}}}{4+3\sqrt{2}} \cdot \frac{4-3\sqrt{2}}{4-3\sqrt{2}}$$

$$< \frac{\left(4-3\sqrt{2}\right)\left(\sqrt{4+3\sqrt{2}}\right)\sqrt{2}}{16-18}N^{\frac{1}{4}}$$

$$< \frac{\left(4-3\sqrt{2}\right)\left(\sqrt{4+3\sqrt{2}}\right)}{-2}N^{\frac{1}{4}}$$

$$< \frac{-\left(4\sqrt{2}-6\right)\left(\sqrt{4+3\sqrt{2}}\right)}{2}N^{\frac{1}{4}}$$

$$\text{hence, } d < \frac{\left(6-4\sqrt{2}\right)\left(\sqrt{4+3\sqrt{2}}\right)}{2}N^{\frac{1}{4}}$$

The following algorithm is designed to recover the prime factors p, q for the RSA modulus $N = pq$ in polynomial time.

Proposed Algorithm 1:

```
Input: an RSA prime modulus $N = pq$ with $q < p < 2q$, and public key $(e, N)$
Output: The private key $(N, d)$.
Choose two random and distinct n - bit strong primes $(p, q)$.
for each pair of the form $(p, q)$ do
$N = pq$
$\varphi(N) = (p-1)(q-1)$
for $p + q < \frac{(4+3\sqrt{2})}{4}\sqrt{N}$ do
compute the continued fraction expansion of $\frac{e}{N}$
for every convergent $\frac{k}{d}$ of $\frac{e}{N}$, compute $\varphi(N) = \frac{ed-1}{k}$
compute $d < \frac{(6-4\sqrt{2})(\sqrt{4+3\sqrt{2}})}{2}N^{\frac{1}{4}}$
end if
return the public key pair (N, e) and the private key pair (N, d).
```

4.3 Second Attack on Prime Power Modulus $N = p^2 q$

Let $N = p^2 q$ be an RSA prime power modulus with $q < p < 2q$, $1 < e < \varphi(N)$, $\varphi(N) = N - \left(2^{1/3}N^{1/3} -\right.$ $2-23N13+1213N13$and kd is among the convergence of the continued fraction expansion of eN, then $d < \frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3}-2^{-1/3}\right)N^{1/3}+2^{1/3}\right]}}$.

Proof:

The RSA key equation $ed - k\varphi(N) = 1$ can be transformed as:

$$ed - k\left[N - (2^{1/3}N^{1/3} - 2^{-2/3}N^{1/3} + 1)2^{1/3}N^{1/3}\right] = 1 \text{ (from equation (2.7))}$$

$$\Rightarrow ed - kN = 1 - k\left[(2^{1/3}N^{1/3} - 2^{-2/3}N^{1/3} + 1)2^{1/3}N^{1/3}\right]$$

$$\Rightarrow ed - kN = 1 - k\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}N^{1/3}$$

Divide both sides by $Nd\ gives$:

$$\left|\frac{ed}{Nd} - \frac{kN}{Nd}\right| = \frac{\left|1 - k\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}N^{1/3}\right|}{\mathrm{Nd}}$$

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{\left|1 - k\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}N^{1/3}\right|}{\mathrm{Nd}}$$

$$< \frac{k\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}N^{1/3}}{\mathrm{Nd}} \quad (3.2)$$

But $ed - k\varphi(N) = 1 \Rightarrow k = \frac{ed-1}{\varphi(N)} \Rightarrow k < \frac{ed}{\varphi(N)}$

$$\Rightarrow k < d \text{ [since } e < \varphi(N)] \Rightarrow \frac{k}{d} < 1$$

Hence, equation (3.2) becomes:

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}N^{1/3}}{\mathrm{N}}$$

$$< \frac{\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}}{N^{2/3}}$$

Using Legendre's equation $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$

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

$$\Rightarrow \frac{k}{d} \text{ is a convergent of the continued expansion of the fraction } \frac{e}{N}$$

$$\Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}}{N^{2/3}} < \frac{1}{2d^2}$$

$$\Rightarrow \frac{\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}}{N^{2/3}}(2d^2) < 1$$

$$\Rightarrow \ 2d^2 < \frac{N^{2/3}}{\left[\left(2^{1/3} - 2^{-2/3}\right)N^{1/3} + 1\right]2^{1/3}}$$

$$\Rightarrow d^2 < \frac{N^{2/3}}{2\left[\left(2^{2/3} - 2^{-1/3}\right)N^{1/3} + 2^{1/3}\right]}$$

$$\Rightarrow \ d < \frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3} - 2^{-1/3}\right)N^{1/3} + 2^{1/3}\right]}}$$

The following algorithm is designed to recover the prime factors p, q for primepower modulus $N = p^2q$ in polynomial time.

Proposed Algorithm 2:

```
Input: an RSA prime modulus $N = p^2q$ with $q < p < 2q$, and public key $(e, N)$
Output: The private key $(N, d)$.
1: Choose two random and distinct n - bit strong primes $(p, q)$.
2: for each pair of the form $(p, q)$do
3: $N : p^2q$
4: $\varphi(N) := N - p^2 - pq + p$
5: for$\varphi(N) = N - (2^{1/3}N^{1/3} - 2^{-2/3}N^{1/3} + 1)2^{1/3}N^{1/3}$ do
6: compute the continued fraction expansion of $\frac{e}{N}$
7: for every convergent $\frac{k}{d}$of $\frac{\mathrm{e}}{\mathrm{N}}$, compute $\varphi(N) = \frac{ed-1}{k}$
8: compute$d < \frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3}-2^{-1/3}\right)N^{1/3}+2^{1/3}\right]}}$
9. end if
10: return the public key pair (N, e) and the private key pair (N, d).
```

IV. Conclusion

This paper proposes two new attacks on the RSA modulus $N = pq$ and prime power moduli $N = p^2q$. For the first attack, we used continued fractions expansions and show that $\frac{k}{d}$ canbe recovered among the convergence of the continued fraction expansion of$\frac{e}{N}$and discovered a decryption exponent $d < \frac{(6-4\sqrt{2})\left(\sqrt{4+3\sqrt{2}}\right)}{2}N^{1/4}$. Hence, we can factor the RSA modulus $N = pq$inpolynomial time.

Furthermore, in the second attack, the use of $N-\left(2^{1/3}N^{1/3}-2^{-2/3}N^{1/3}+1\right)2^{1/3}N^{1/3}$as an approximation of $\varphi(N)$for the RSA prime power modulus $N=p^2q$and show that $\frac{k}{d}$ can be recovered among the convergences of the continued fraction expansion of $\frac{e}{N}$which also lead to discover a decryption exponent $d<\frac{N^{1/3}}{\sqrt{2\left[\left(2^{2/3}-2^{1/3}\right)N^{1/3}+2^{1/3}\right]}}$.

References

[1]. Ariffin et. al. (2018). *New Cryptanalytic Attack on RSA Modulus N = pq Using Small Prime Difference Method*. Malysia Journal of Mathematical Sciences

[2]. Ariffin M. R. K. and Shehu S. (2016). *Cryptanalysis on prime power RSA modulus of the form* $N = p^r q$. International of Applied Mathematical Research; pp. 167 -175.

[3]. Blömer, J. and May, A., (2004). *A generalized Wiener attack on RSA*. In International Workshop on Public Key Cryptography; Springer: Berlin/Heidelberg, Germany, pp. 1–13.

[4]. Chen, et al., (2009). A Generalization of de Weger's Method. In Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China, 18–20 August 2009; Volume 1, pp. 344–347.

[5]. D. Boneh, G. Durfee (1999), *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, *Advances in Cryptology* - Proceedings of Eurocrypt '99, Lecture Notes in Comp. Sci. 1952.

[6]. de Weger, B. (2002), *Cryptanalysis of RSA with small prime difference*, Applicable Algebra in Engineering, Communication and Computing, Vol. 13(1), pp. 17-28.

[7]. Maitra, S. and Sarkar, S. (2008). *Revisiting Wiener's attack–new weak keys in RSA*. In International Conference onInformation Security; Springer: Berlin/Heidelberg, Germany, pp. 228–243.

[8]. Nitaj, A. (2013), *Diophantine and lattice cryptanalysis of the RSA cryptosystem.* In Artificial Intelligence, Evolutionary Computing and Metaheuristics; Springer: Berlin/Heidelberg, Germany, 2013; pp. 139–168.

[9]. Nitaj, A. and Rachidi, T. (2015). *New attacks on RSA with modulus* $N = p^r q$. In Codes, Cryptology, and Information Security, pages 352 - 360. Springer.

[10]. Nitaj, et. al., (2014). *New attacks on the RSA cryptosystem.* In International Conference on Cryptology in Africa; Springer, Cham, Switzerland, pp. 178–198.

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

[12]. Shehu, S. and Ariffin M. R. K. (2017). *New attacks on prime power* $N = p^r q$ *using good approximation of* $\varphi(N)$. Malysia Journal of Mathematical Sciences 11(S); pp 121 -138.

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

Ibrahim A. A, et. al. "Cryptanalysis on RSA Using Decryption Exponent." *IOSR Journal of Mathematics (IOSR-JM)*, 17(5), (2021): pp. 01-08.