IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 17, Issue 5 Ser. II (Sep. – Oct. 2021), PP 09-15
www.iosrjournals.org

Diophatine Attack on RSA Using More Than One Decryption Exponent

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

[1]*Department of Mathematics, Faculty of Science, UsmanuDanfodio University, Sokoto, Nigeria.*
[2]*Department of Mathematics, ShehuShagari College of Education, Sokoto, Nigeria.*
[3]*Department of Mathematics, Faculty of Science, Sokoto State University, Sokoto, Nigeria.*
[4]*Department of Science, Mathematics Unit,State Collage of Basic and Remedial Studies, Sokoto, Nigeria.*

Abstract
In this paper, we present anew attack on RSA in the presence of three encryption and decryption exponents e_i *and* d_i *for* $i = 1, 2, 3$ *respectively with thesame modulus N.The attack is an extension of Guo's attack on RSA using continued fraction method to find new weaknesses in RSA. In the new attackwe used prime power difference* $|p^2 - q^2| < N^{1/2}$ *to show that if* $\frac{k_i}{d_i}$ *is one of the convergences of the continued fraction expansion of* $\frac{e_i}{N}$ *and the private exponent* d_i *used in the RSApublic-key cryptosystem is less than* $\frac{1}{4}N^{2/3}$ *for* $i = 1, 2, 3$ *then the system is more secureand stronger than the previous ones.*

Keywords: *Prime power, Factorization, Cryptography, Encryption, Decryption and Continued fraction.*

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

I. Introduction

The theory of Diophantine approximations, named after Diophantus of Alexandria, deals withthe approximation of real numbers by rational numbers which can be achieved by continuedfractions. Continued fractions have many properties and applications in Number Theory andcryptographic problems. They are used to find good Diophantine approximations to rationaland irrational numbers, to solve Diophantine equations and to build attacks on some instancesof RSA, (Nitaj, 2013).It is well known that most successful attacks on RSA are not based on factoring the modulus N, ratherthey exploit the mathematical weaknesses of the RSA algorithm or the improper use of the RSA system, such as lower exponents, common modulus, and knowledge of parts of the private exponent (Nitaj and Rachidi, 2015).

Takagi (2003) proposes a cryptosystem modulus $N = p^r q$ based on theRSA cryptosystem. He chooses an appropriate modulus $N = p^r q$ which resiststwo of the fastest factoring algorithms, namely the number field sieve and the elliptic curve method, (Shehu and Ariffin, 2017).

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 approachesare applications of Coppersmith's method for solving modular univariate polynomialequations. From these new attacks they directly derive partial keyexposure attack, which is attack when the secret exponent is not necessarily small but when a fraction of the secret key bits is known to the attacker, (Ariffin et al., 2018).

Hinek (2007) showed that it is possible to factor the k modulus N_i if $d < N^{\delta}$ with $\delta = \frac{k}{2(k+1)} - \varepsilon$ where ε is a small constant depending on the size of $max N_i$.

In 2010, Sarkar and Maitra improved Howgrave-Graham and Seifert bound up to $d_1,\ d_2 < N^{0.416}$, (Nitaj, 2016).

Nitaj (2016) proposed that the bound $d_i < N^{1/2}$ obtained by Sarkar and Maitra can be improved using continued fraction method and the approximation $\tilde{P}$ of p such that $|p - \tilde{P}| < 2N^{1/4}$ as in Coppersmith theorem.

Shehu and Ariffin, (2017) presented three new attacks on Prime Power modulus $N = p^r q$ 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 $\frac{e}{N - 2N^{\frac{r}{r+1}} + N^{\frac{r-1}{r+1}}}$ and that one can factor the modulus $N = p^r q$ in polynomial time.

It is in view of this the study is going to present a new a attack to extend the Guo's work using prime power moduli $N = p^2 q$ with three encryption and decryption exponents.

Our Contribution: In this paper, we propose a new attack on RSA prime power moduli$N = p^2q$ using continued fraction method. In the attack we used$S$ asan approximation of$p^2 + q^2$such that$|p^2 + q^2 - S| < \frac{|p^2-q^2|}{3(p^2+q^2)}N^{1/3}$ and if$t < \frac{|p^2-q^2|}{3(p^2+q^2)}N^{1/3} < N^{1/3}$ with$\frac{k_i}{d_i}$ among the convergent of$\frac{e_i}{N}$lead to discover$d_i < \frac{1}{4}N^{2/3}$.
The rest of this paper is structured as follows: In section 2, we give a brief review of basic facts about the continued fractions, Euclidean algorithm for computation of Greatest Common Divisor(gcd) and Euler Totient function as well as Guo's method of attack on RSA. In section 3, we put forward the new attack. We conclude this paper in section 4.

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 attack.

2.1 Continued Fraction Expansion

A continued fraction is an expression of the form:

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

wherea_0 is an integer anda_m are positive integers for$m \geq 1$. Thea_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$\frac{p}{q}$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$x$ (Nitaj, 2013).

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)*

Ifm and$n$ are integers we say that a positive integer d is thegcd 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

$\phi$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.$GCD\ (a_i, n) = 1, where\ a_i = 1, 2, \dots, n-1$).

- (Hoffstein, et. al., 2008)

2.5 Guo's attack on RSA

Theorem:
Let$N = pq$ be an RSA modulus. Consider three instances of RSA with a common modulus$N$ and public exponentse_1, e_2, e_3 satisfying
$e_1d_1 \equiv 1(mod\phi(N)),\quad e_2d_2 \equiv 1(mod\phi(N)),\quad e_3d_3 \equiv 1(mod\phi(N)),$
If all thek_i andd_i are pairwise relatively prime and$d_i < N^{\frac{1}{3}-\epsilon}$ for$i = 1, 2, 3$,with$\epsilon > 0$, then factor$N$ can be factored in polynomial time (Graham, 1997).

Proof:
Transforming the three congruence$e_id_i \equiv 1\ (mod\ \varphi(N)), i = 1, 2, 3$ into equations we get:

$$e_1d_1 = 1 + k_1\varphi(N) \quad (2.1)$$
$$e_2d_2 = 1 + k_2\varphi(N) \quad (2.2)$$
$$e_3d_3 = 1 + k_3\varphi(N) \quad (2.3)$$

Where$k_1,\ k_2,\ k_3$ are positive integers.
From equation (2.1), we have:

$$k_1\varphi(N) = e_1d_1 - 1$$
$$\Longrightarrow \varphi(N) = \frac{e_1d_1 - 1}{k_1} \quad (2.4)$$

From equation (2.2):

$$k_2\varphi(N) = e_2d_2 - 1$$

$$\Rightarrow \varphi(N) = \frac{e_2 d_2 - 1}{k_2} \quad (2.5)$$

And from equation (2.3):

$k_3\varphi(N) = e_3 d_3 - 1$

$$\Rightarrow \varphi(N) = \frac{e_3 d_3 - 1}{k_3} \quad (2.6)$$

Equating (2.4) and (2.5), we have:

$$\frac{e_1 d_1 - 1}{k_1} = \frac{e_2 d_2 - 1}{k_2}$$

$\Rightarrow e_1 d_1 k_2 - k_2 = e_2 d_2 k_1 - k_1$

$\Rightarrow e_1 d_1 k_2 - e_2 d_2 k_1 = k_2 - k_1 (2.7)$

Also, equating (2.4) and (2.6), we have:

$$\frac{e_1 d_1 - 1}{k_1} = \frac{e_3 d_3 - 1}{k_3}$$

$\Rightarrow e_1 d_1 k_3 - k_3 = e_3 d_3 k_1 - k_1$

$\Rightarrow e_1 d_1 k_3 - e_3 d_3 k_1 = k_3 - k_1 (2.8)$

And equating (2.5) and (2.6), we have:

$$\frac{e_2 d_2 - 1}{k_2} = \frac{e_3 d_3 - 1}{k_3}$$

$\Rightarrow e_2 d_2 k_3 - k_2 = e_3 d_3 k_2 - k_3$

$\Rightarrow e_2 d_2 k_3 - e_3 d_3 k_2 = k_2 - k_3 (2.9)$

Also, equating (2.6) and (2.4), we have:

$$\frac{e_3 d_3 - 1}{k_3} = \frac{e_1 d_1 - 1}{k_1} \Rightarrow e_3 d_3 k_1 - k_1 = e_1 d_1 k_3 - k_3$$

$\Rightarrow e_3 d_3 k_1 - e_1 d_1 k_3 = k_1 - k_3 (2.10)$

Dividing equation (2.7) by $e_2 d_1 k_2$ yields:

$$\frac{e_1 d_1 k_2}{e_2 d_1 k_2} - \frac{e_2 d_2 k_1}{e_2 d_1 k_2} = \frac{k_2 - k_1}{e_2 d_1 k_2}$$

$$\Rightarrow \left|\frac{e_1}{e_2} - \frac{d_2 k_1}{d_1 k_2}\right| = \frac{|k_2 - k_1|}{e_2 d_1 k_2} (2.11)$$

Under the condition $\gcd(d_2 k_1, d_1 k_2) = 1$ and using Legendre's equation

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$$

We have: $\left|\frac{e_1}{e_2} - \frac{d_2 k_1}{d_1 k_2}\right| < \frac{1}{2(d_1 k_2)^2}$

$\Rightarrow \frac{d_2 k_1}{d_1 k_2}$ is a convergent of the continued expansion of the fraction $\frac{e_1}{e_2}$

Equation (2.11) becomes:

$$\frac{|k_2 - k_1|}{e_2 d_1 k_2} < \frac{1}{2(d_1 k_2)^2}$$

$$\Rightarrow \frac{2|k_2 - k_1|(d_1 k_2)^2}{e_2 d_1 k_2} < 1$$

To have: $\frac{2|k_2 - k_1| d_1 k_2}{e_2} < 1$

$$\Rightarrow \mathrm{d}_1 < \frac{e_2}{2k_2|k_2 - k_1|} (2.12)$$

Similarly, dividing equation (2.8) by $e_3 d_1 k_3$:

$$\Rightarrow \left|\frac{e_1 d_1 k_3}{e_3 d_1 k_3} - \frac{e_3 d_3 k_1}{e_3 d_1 k_3}\right| = \frac{|k_3 - k_1|}{e_3 d_1 k_3}$$

$$\Rightarrow \left|\frac{e_1}{e_3} - \frac{d_3 k_1}{d_1 k_3}\right| = \frac{|k_3 - k_1|}{e_3 d_1 k_3} (2.13)$$

To have $\frac{d_3 k_1}{d_1 k_3}$ as one of the convergent of the continued fraction expansion of $\frac{e_1}{e_3}$

Under the condition $\gcd(d_3 k_1, d_1 k_3) = 1$ and using Legendre's equation

We have: $\left|\frac{e_1}{e_3} - \frac{d_3 k_1}{d_1 k_3}\right| < \frac{1}{2(d_1 k_3)^2}$

Equation (2.13) becomes:

$$\frac{|k_3 - k_1|}{e_3 d_1 k_3} < \frac{1}{2(d_1 k_3)^2}$$
$$\Rightarrow \frac{2|k_3 - k_1|(d_1 k_3)^2}{e_3 d_1 k_3} < 1$$
To have: $\frac{2|k_3 - k_1| d_1 k_3}{e_3} < 1$
$$\Rightarrow \mathrm{d}_1 < \frac{e_3}{2k_3|k_3 - k_1|} (2.14)$$
And also, dividing equation (2.9) by $e_3 d_2 k_3$ gives:
$$\Rightarrow \left|\frac{e_2 d_2 k_3}{e_3 d_2 k_3} - \frac{e_3 d_3 k_2}{e_3 d_2 k_3}\right| = \frac{|k_3 - k_2|}{e_3 d_2 k_3}$$
$$\Rightarrow \left|\frac{e_2}{e_3} - \frac{d_3 k_2}{d_2 k_3}\right| = \frac{|k_3 - k_2|}{e_3 d_2 k_3} (2.15)$$
To have $\frac{d_3 k_2}{d_2 k_3}$ as one of the convergent of the continued fraction expansion of $\frac{e_2}{e_3}$
Under the condition $\gcd\ (d_3 k_2, d_2 k_3) = 1$ and using Legendre's equation
Equation (2.15) becomes:
$$\frac{|k_3 - k_2|}{e_3 d_2 k_3} < \frac{1}{2(d_2 k_3)^2}$$
$$\Rightarrow \frac{2|k_3 - k_2|(d_1 k_3)^2}{e_3 d_2 k_3} < 1$$
To have: $\frac{2|k_3 - k_2| d_2 k_3}{e_3} < 1$
$$\Rightarrow \mathrm{d}_2 < \frac{e_3}{2k_3|k_3 - k_1|} (2.16)$$
If all the $k_i's$ and $d_i's$ are pair wise relatively prime, then $d_1 = \gcd(d_1 k_2,\ d_1 k_3)$ and $k_1 = \gcd(d_2 k_1,\ d_3 k_1)$, which leads to $\varphi(N) = \frac{e_1 d_1 - 1}{k_1}$ and finally to the factorization of N. And also if $k_i < d_i < N^{\delta}$ for a positive constant δ, and $e_1 < N$, then the condition $\frac{|k_2 - k_1|}{e_2 d_1 k_2} < \frac{1}{2(d_1 k_2)^2}$ can be written as $\mathrm{N}^{3\delta} < \frac{1}{2} N = N^{1-3\varepsilon}$ or equivalently $\delta = \frac{1}{3} - \varepsilon$, where $\varepsilon > 0$ is a small constant depending on N.

2.6. Some Useful Lemmas

Lemma 2.1

Let $N = p^2 q$ 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 $N = p^2 q, q = \frac{N}{p^2} \Rightarrow \frac{N}{p^2} < p < 2\left(\frac{N}{p^2}\right)$
$$\Rightarrow N < p^3 < 2N$$
$$\Rightarrow N^{1/3} < p < 2^{1/3} N^{1/3} (2.17)$$
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:
$$\Rightarrow \frac{1}{2^{2/3} N^{2/3}} < \frac{1}{p^2} < \frac{1}{N^{2/3}}$$
Multiply by N:
$$\Rightarrow \frac{N}{2^{2/3} N^{2/3}} < \frac{N}{p^2} < \frac{N}{N^{2/3}}$$
$$\Rightarrow \frac{N}{2^{2/3} N^{2/3}} < q < \frac{N}{N^{2/3}}$$
$$\Rightarrow 2^{-2/3} N^{1/3} < q < N^{1/3} (2.18)$$
Combining equation (2.17) and (2.18):
$$2^{-2/3} N^{\frac{1}{3}} < q < N^{1/3} < p < 2^{1/3} N^{1/3}$$
This terminates the proof.

Lemma 2.2

Let $N = p^2q$ be an RSA prime power modulus with q< p < 2q. Let$|p^2 - q^2| < N^{1/2}$. Suppose that$S$ isan approximation of$p^2 + q^2$such that$|p^2 + q^2 - S| < \frac{|p^2-q^2|}{3(p^2+q^2)} N^{1/3}$then$q = \left\lfloor \frac{S^2}{4N} \right\rfloor$.

Proof:

Let$S = p^2 + q^2$, where $0 < \frac{|p^2-q^2|}{3(p^2+q^2)} N^{1/3} < N^{1/3}$

We have:$(p^2 - q^2)^2 = (p^2 - q^2)(p^2 - q^2)$
$= p^4 - 2p^2q^2 + q^4$
$= (p^4 + q^4) - 2Nq$
$= (p^4 + q^4 + 2p^2q^2 - 2p^2q^2) - 2Nq$
$= [(p^2 + q^2)^2 - 2p^2q^2] - 2Nq$
$= [(p^2 + q^2)^2 - 2Nq] - 2Nq$
$= (p^2 + q^2)^2 - 4Nq$ (2.19)

Such that
$S^2 - 4Nq = (p^2 + q^2)^2 - 4Nq$
$= (p^2 + q^2)(p^2 + q^2) - 4Nq$
$= p^4 + 2p^2q^2 + q^4 - 4p^2q^2$
$= p^4 + q^4 - 2p^2q^2$
$\Longrightarrow S^2 - 4Nq = (p^2 - q^2)^2$(2.20)

Suppose$|p^2 - q^2| < \mathrm{N}^{1/2}$ and$0 < \frac{|p^2-q^2|}{3(p^2+q^2)} N^{1/3} < N^{1/3}$

Then equation (2.20) becomes:

$|S^2 - 4Nq| < (N^{1/2})^2 < N$

Dividing both sides of the above by$4N$we have:$\left|\frac{S^2}{4N} - q\right| < \frac{N}{4N} < \frac{1}{4} \Longrightarrow q < \frac{S^2}{4N} - \frac{1}{4}$

Hence, $q = \left\lfloor \frac{S^2}{4N} \right\rfloor$ as required.

Lemma 2.3

Let $N = p^2q$ be an RSA prime power modulus with q < p < 2q. Suppose$S$ is a positive integer such that$|p^2 + q2 - S < p2 - q2p2 + q2N13,\ S2 - 4Nq$isan approximation of$p2 - q2$then $p2 - q2 - D < N13$, whereD2=$S2 - 4Nq$

Proof:

$D \approx p^2 - q^2 \Longrightarrow D^2 \approx (p^2 - q^2)^2$
$= p^4 - 2p^2q^2 + q^4$
$= (p^4 + q^4) - 2Nq$
$= [(p^2 + q^2)^2 - 2p^2q^2] - 2Nq$
$= (p^2 + q^2)^2 - 4Nq$
$= S^2 - 4Nq$

hence, $D = \sqrt{S^2 - 4Nq}$(2.21)

Such that:$|(p^2 - q^2)^2 - D^2| = |(p^2 - q^2)^2 - (S^2 - 4Nq)|$
$= |(p^2 - q^2)^2 - S^2 + 4Nq|$
$= |p^4 - 2p^2q^2 + q^4 - S^2 + 4p^2q^2|$
$= |p^4 + q^4 + 2p^2q^2 - S^2|$
$= |(p^2 + q^2)^2 - S^2|$

Thus,$|(p^2 - q^2)^2 - D^2| = |(p^2 + q^2)^2 - S^2|$(2.22)

$|(p^2 - q^2)^2 - D^2|$can also be written as:

$|(p^2 - q^2)^2 - D^2| = |[(p^2 - q^2) - D][(p^2 - q^2) + D]|$
$= |p^2 - q^2 - D|[p^2 - q^2 + D]$

Dividing both sides by$[p^2 - q^2 + D]$

$\Longrightarrow |p^2 - q^2 - D| = \frac{|(p^2 - q^2)^2 - D^2|}{[p^2 - q^2 + D]}$

Substituting (2.22) into the above:

$\Longrightarrow |p^2 - q^2 - D| = \frac{|(p^2 + q^2)^2 - S^2|}{[p^2 - q^2 + D]}$
$\leq \frac{|(p^2 + q^2)^2 - S^2|}{|p^2 - q^2|}$(2.23)

Similarly,$|(p^2 + q^2)^2 - S^2|$ can be written as:

$|(p^2 + q^2)^2 - S^2| = |[(p^2 + q^2) - S][(p^2 + q^2) + S]|$

$$= |p^2 + q^2 - S|[p^2 + q^2 + S]$$

Such that equation (2.23) becomes:

$$|p^2 - q^2 - D| \leq \frac{|p^2 + q^2 - S|[p^2 + q^2 + S]}{|p^2 - q^2|} (2.24)$$

Using the fact that$|p^2 + q^2 - S| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$

$\Longrightarrow S < (p^2 + q^2) + \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$

Adding$(p^2 + q^2)$ to both sides of the above inequality gives:

$$S + (p^2 + q^2) < (p^2 + q^2) + (p^2 + q^2) + \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$$

$$< 2(p^2 + q^2) + \frac{|p^2 + q^2|}{3(p^2 + q^2)} N^{1/3}, \quad \because |p^2 - q^2| < |p^2 + q^2|$$

$$\Longrightarrow S + (p^2 + q^2) < 3(p^2 + q^2)$$

Substituting back into equation (2.24):

$$|p^2 - q^2 - D| \leq \frac{|p^2 + q^2 - S|[p^2 + q^2 + S]}{p^2 - q^2}$$

$$\leq \left(\frac{|p^2 + q^2 - S|}{p^2 - q^2}\right) 3(p^2 + q^2)$$

But$|p^2 + q^2 - S| < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$

$$\Longrightarrow |p^2 - q^2 - D| \leq \frac{3(p^2 + q^2)}{|p^2 - q^2|} \cdot \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3}$$

Hence,$|p^2 - q^2 - D| < N^{1/3}$, which terminate the proof

III. Our New Attack

Let$N = p^2 q$ be an RSA prime power modulus with$q < p < 2q$. Lete$_i$ be public key satisfying the equation$e_i d_i - k_i N = p^2 + q^2 + t$ with$gcd(d_i, k_i) = 1$. If$\frac{k_i}{d_i}$ is among the convergent of $\frac{e_i}{N}$ and$t < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3} < N^{1/3}$then$d_i < \frac{1}{4} N^{2/3}$.

Proof:

For$t < \frac{|p^2 - q^2|}{3(p^2 + q^2)} N^{1/3} \Longrightarrow t < N^{1/3}$ since $\frac{|p^2 - q^2|}{3(p^2 + q^2)} < 1$

And dividing$e_i d_i - k_i N = p^2 + q^2 + t$ by$N d_i$we have:

$$\left|\frac{e_i d_i}{N d_i} - \frac{k_i N}{N d_i}\right| = \frac{p^2 + q^2 + t}{N d_i}$$

$$\left|\frac{e_i}{N} - \frac{k_i}{d_i}\right| = \frac{|p^2 + q^2 + t|}{N d_i} \leq \frac{|p^2 + q^2| + |t|}{N d_i}$$

But$t < N^{1/3}$,

$$\Longrightarrow \left|\frac{e_i}{N} - \frac{k_i}{d_i}\right| \leq \frac{|p^2 + q^2| + N^{1/3}}{N d_i}$$

Applying Legendre's theorem, that is$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$

We have:$\left|\frac{e_i}{N} - \frac{k_i}{d_i}\right| < \frac{1}{2d_i^2}$

$\Rightarrow \frac{k_i}{d_i}$ is among the convergent of the continued expansion of the fraction $\frac{e_i}{N}$

$$\Longrightarrow \frac{|p^2 + q^2| + N^{1/3}}{N d_i} < \frac{1}{2d_i^2}$$

$$\Longrightarrow \frac{2d_i^2 \left||p^2 + q^2| + N^{1/3}\right|}{N d_i} < 1$$

$$\Longrightarrow \frac{2d_i \left||p^2 + q^2| + N^{1/3}\right|}{N} < 1$$

$$\Longrightarrow d_i < \frac{N}{2\left||p^2 + q^2| + N^{1/3}\right|}$$

For which$p^2 + q^2 > N^{1/3}$

$$\Rightarrow \frac{N}{2\left|\left|p^2+q^2\right|+N^{1/3}\right|} < \frac{N}{4N^{1/3}} = \frac{1}{4}N^{1-(1/3)} = \frac{1}{4}N^{2/3}$$

hence,$d_i < \frac{1}{4}N^{2/3}$.

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

Proposed Algorithm 1:

Input: an RSA prime power modulus$N = p^2q$with$q < p < 2q$, and public key $(e_i, N), \quad i = 1, 2, 3$

Output: The prime factors$p$ and$q$

1: Compute the continued fraction expansion of$\frac{e_1}{N}$

2: Compute the continued fraction expansion of$\frac{e_2}{N}$

3: Compute the continued fraction expansion of$\frac{e_3}{N}$

4: **For** every convergent$\frac{d_i}{k_i}$of$\frac{e_i}{N}$, compute $S = e_i d_i - k_i N$

5: Compute$\left\lfloor \frac{S^2}{4N} \right\rfloor$

6:$q = gcd\left(\left\lfloor \frac{S^2}{4N} \right\rfloor, N\right)$

7. If$1 < q < N, \ then\ p^2 = \frac{N}{q}$

8. End

IV. Conclusion

In this paper, we have shown that our developed attack on RSA prime power moduli$N = p^2q$ and$N = p^rq$ using continued fraction method can be used efficiently. The use of S asan approximation of$p^2 + q^2$such that$|p^2 + q^2 - S| < \frac{|p^2-q^2|}{3(p^2+q^2)}N^{1/3}$ and if$t < \frac{|p^2-q^2|}{3(p^2+q^2)}N^{1/3} < N^{1/3}$ with$\frac{k_i}{d_i}$ among the convergents of $\frac{e_i}{N}$then$d_i < \frac{1}{4}N^{2/3}$.

References

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

[2]. 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.

[3]. Boneh D. and Durfe G. (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, 1–11.

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

[5]. Hinek, M.J., (2007). *Cryptanalysis of RSA and Its Variants;* Chapman and Hall/CRC: Boca Raton, FL, USA.

[6]. Hoffstein et al. (2008). *An Introduction to Mathematical Cryptography.* Springer Science Business Media, LLC

[7]. Howgrave-Graham, N. A. (1997). *Finding small roots of univariate modular equations revisited*. In Cryptography and Coding, LNCS 1355, pp. 131|142, Springer-Verlag.

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

[9]. Nitaj, A, (2016). *New Attacks on RSA with two or three decryption exponents.*http://www.math.unicaen.fr/-nitaj. Downloaded August 10, 2019.

[10]. 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.

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

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

Ibrahim A. A, et. al. "Diophatine Attacks on RSA Using More Than One Decryption Exponent."*IOSR Journal of Mathematics (IOSR-JM)*, 17(5), (2021): pp. 09-15.