IJSGS VOL. 9(1), MARCH, 2023 https://doi.org/ 10.57233/ijsgs.v9i1.405 URL: https://fugus-ijsgs.com.ng

IJSGS

ISSN: 2488-9229
FEDERAL UNIVERSITY
GUSAU-NIGERIA

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY

Cryptanalysis Attacks on Multi Prime Power Modulus Through Analyzing Prime Difference

[1]Dogondaji, A M, [2] Sani, B. [3] Ibrahim, A.A and [4] Abubakar, S. I.

[1, 2&3]Department of Mathematics, Usmanu Danfodiyo University, P M B 2346, Sokoto-Nigeria

[4]Department of Mathematics, Sokoto State University, Sokoto-Nigeria

Corresponding Author's E- mail Address and Phone NO.: lambobs0615@gmail.com, 08065604196

Received on: January, 2023 **Revised and Accepted on:** February, 2023 **Published on:** March, 2023

ABSTRACT

The Security of Rivest, Shamir and Adleman Cryptosystem known as RSA and its variants rely on the difficulty of integer factorization problem. This paper presents a short decryption exponent attack on RSA variant $N = p^2q^2$ based on the key equation $ed - k\varphi(N) = 1$ where prime difference $\left|bq^2 - ap^2\right| < N^{\gamma}$ was carefully analyzed and came up with an approximation of $\varphi(N)$ as $N - \frac{a+b}{\sqrt{ab}}\sqrt{N}$ which enabled us to obtain an improved bound $d < \frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$ that led to the polynomial time factorization of the variant $N = p^2q^2$.

Keywords:
RSA modulus, Multi Prime power, Continued fraction, prime difference, short decryption attack.

1.0 INTRODUCTION

The development of RSA cryptosystem in (1978) by Rivest, Shamir and Adleman was seen as an evolution in the world of public key cryptosystem, (Nitaj, 2013). Moreover, the difficulty in solving integer factorization problem made RSA cryptosystem a standard at heart of modern technology with widespread applications in banking, industry, online shopping, telecommunication and information transferred etc, (Shehu et al. 2020).

RSA cryptosystem involves three processes of key generation, encryption and decryption. The choice of public key pair (e, N) and private key tuples (d, p, q) must always satisfy a given relation $ed \equiv 1 \bmod \varphi(N)$ with $e < \varphi(N)$ where $\varphi(N)$ represent totient function expressed as $\varphi(N) = p^{a-1}q^{b-1}(p-1)(q-1)$. RSA Cryptosystem with standard modulus $N = pq$ and its variants suffered a lot of attacks such as short decryption exponent attack, small public key exponent attack, common modulus attack and partial key exposure attacks etc. Wiener (1990) was first to launched attack on standard RSA modulus $N = pq$ with short decryption exponent bound using continued fraction expansion of $\frac{e}{N}$. He successfully recovered primes p and q using a bound $d < \frac{1}{3}N^{\frac{1}{4}}$, (Ariffin et al. 2019). On the other hand, RSA variant $N = p^r q$, $r \geq 2$ was proved to be factored when the short decryption exponent bound was $d < N^{\frac{1}{2(r+1\backslash)}}$ for $r \geq 2$ as first reported by Takagi (1998). He further established that decryption process is faster using prime power modulus than standard RSA modulus $N = pq$. Since then, many variant were

developed: Asbullah and Ariffin (2015) presented attack on variant $N = p^2q$ using continued fraction method; they showed that if $\frac{k}{d}$ is obtained from the continued fraction expansion of $\frac{e}{N-\left(2N^{\frac{2}{3}}-N^{\frac{1}{3}}\right)}$ then primes p and q can be obtained in polynomial time. In the same vein, AbdRahman and Ariffin (2016) proposed a similar attack on modulus $N = p^2q$ by fixing the sizes of p and q.

An extension of Asbullh and Ariffin (2015) was reported in the work of Shehu and Ariffin (2017) where $\frac{e}{N-2N^{\frac{r}{r+1}}+N^{\frac{r-1}{r+1}}}$ was used in mounting the attack on the modulus $N = p^rq$ $(r \geq 2)$ based on the condition that $p^{\frac{3r+1}{r+1}}\left|p^{\frac{r-1}{r+1}}-q^{\frac{r-1}{r+1}}\right|<\frac{1}{6}N^{\gamma}$ when the decryption exponent bound $d = N^{\delta}$ where $\delta < \frac{1-r}{2}$. Furthermore, Abubakar et al. (2020) presented another attack on $N = p^rq$ $(r \geq 2)$ where they obtained bound $d < \frac{1}{\sqrt{2}}\sqrt{N-2^{\frac{2r+1}{r+1}}N^{\frac{r}{r+1}}}$.

On multi prime power modulus $N = p^2q^2$, a polynomial time attack was reported by Shehu et al. (2020) using $p \approx 2^{\frac{1}{4}}N^{\frac{1}{4}}$ and $q \approx N^{\frac{1}{4}}$ which gave a good approximation of $\varphi(N)$ as $N+2^{\frac{1}{4}}N^{\frac{1}{2}}-\left(2^{\frac{1}{2}}N^{\frac{3}{4}}+2^{\frac{1}{4}}N^{\frac{3}{4}}\right)$. The correct convergent $\frac{k}{d}$ was obtained from the continued fraction expansion of $\frac{e}{N+2^{\frac{1}{4}}N^{\frac{1}{2}}-\left(2^{\frac{1}{2}}N^{\frac{3}{4}}+2^{\frac{1}{4}}N^{\frac{3}{4}}\right)}$ which led to factorization of the modulus $N = p^2q^2$. .Also, Abubakar et al. (2021) proposed small public exponent attack on multi prime power modulus $N = p^2q^2$ where $p \approx q \approx N^{\frac{1}{4}}$ which yielded a good approximation of $\varphi(N) \approx N-2N^{\frac{3}{4}}+N^{\frac{1}{4}}$. The correct convergent $\frac{k}{d}$ was found by taking continued fraction expansion of $\frac{e}{N-2N^{\frac{3}{4}}-N^{\frac{1}{4}}}$. This led to the successful recovery of prime factors p and q. In this paper, we present a short decryption exponent attack on the modulus $N = p^2q^2$ through analyzing small prime difference $\left|bp^2-aq^2\right|<N^{\gamma}$ where $0.25 \leq \gamma \leq 0.5$ using a bound of $d < \frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$. The paper shows that if $\left[a(b^2+1)q^2-b(a^2+1)p^2\right](bq^2-ap^2)>0$ and the ratio of $\frac{q^2}{p^2}$ is close to $\frac{b}{a}$ where a and b are suitably small positive integers, then the convergent $\frac{k}{d}$ can be obtained from the continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}$.

The paper consists of four sections. In section one (Introduction), we give an introduction and some cryptanalysis attacks on RSA and its prime power modulus. We also give an account on how attacks are being carried out. Section two (preliminaries), gives definition of some basic terms and Theorems that are related to our work. Results of the major finding are reported in section three. Finally, we conclude the paper in section four.

2.0 PRELIMINARIES

In this section, a highlight of some basic terms applicable to this paper like Continued fraction and some related theorems are presented.

Definition1Continued fraction: Given any positive real number x, define $x = x_0$ and for $i = 1,...n$ express $x_1 = \lfloor a_i \rfloor$, $x_{i+1} = \dfrac{1}{x_i - a_i}$ until $x \in Z$ Then the continued fraction of a real number x can be represented as $x = \{a_0, a_1, a_2, ...a_n\}$ where

$$\{a_0, a_1, a_2, ...a_n\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 ..... + \cfrac{1}{a_n}}}}$$

Any rational number $\dfrac{a}{b}$ can be expressed as a finite continued fraction $x = \{a_1, a_2, ..., a_n\}$. Similarly, the convergent of x is denoted by a function $\dfrac{a}{b} = \{a_1, ..., a_k\}$ for $k \geq 0$. It is pertinent to note here that, if $x = \dfrac{a}{b}$ is a rational number, then; continued fraction expansion is finite.

Theorem 1: If $\dfrac{n_1}{m_1}, \dfrac{n_2}{m_2}, \ldots, \dfrac{n_j}{m_j}$ are the convergent of continued fraction $\left[a_i, a_2, \ldots, a_j, \ldots\right]$, then the numerators and denominators of these convergents satisfy the following

$$n_1 = a_1,\ n_2 = a_2 a_1,\ n_j = a_j n_{j-1} + n_{j-2}$$

$$m_1 = 1,\ m_2 = a_2,\ m_j = a_j m_{j-1} + m_{j-2},$$

for $j \geq 3$. (Abubakar et al. 2019)

Theorem 2: Legendre (Shehu and Ariffin, 2017): Let $x = [a_0, a_1, ...a_n]$ be a continued fraction expansion of x. If X and Y are co-prime integers such that $\left|x - \dfrac{X}{Y}\right| < \dfrac{1}{2Y^2}$, then $\dfrac{X}{Y}$ is one of the convergent of x .

Theorem 3.: $(Chen$ et al., 2009$)$. Let p and q be prime numbers satisfying $p < q < 2p$. Let $|ap - bq| = N^r$. If the ratio of $\dfrac{q}{p}$ and $\dfrac{b}{a}$ are close and $\left(b\left(a^2+1\right)p - a\left(b^2+1\right)q\right)(ap - bq) > 0,$ then the secret key $d < N^{\frac{3}{4}-\gamma}$ can be obtained from the convergent of continued fraction expansion of $\dfrac{e}{N - \dfrac{a+b}{\sqrt{ab}}\sqrt{N} + 1}$.

Theorem 4: $(Abubakar$ et al. 2019$)$: Let p and q be prime numbers satisfying $p < q < 2p$ and $N = pq$. For a given public key pair (e, N) where $e < \varphi(N)$ and a private key tuple (d, p, q), let $\left|b^2 p - a^2 q\right| < N^r$. if $\dfrac{q}{p}$ is close to $\dfrac{b^2}{a^2}$ such that the relation

$\left(a^2\left(b^4+1\right)p-b^2\left(a^4+1\right)q\right)\left(b^2p-a^2q\right)>0$ holds and the secret key $d<\frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, then $\frac{k}{d}$ can be recovered from $\frac{e}{N-\frac{a^2+b^2}{ab}\sqrt{N}+1}$ for $d>k$ and positive integers (a,b) are less than $\log N$.**3.0**

RESULTS AND DISCUSSION

This section presents our findings on this research. This section comprises two parts, the first part reported a short decryption exponent attack on the variant $N=p^2q^2$ where prime difference $\left|bp^2-aq^2\right|<N^{\gamma}$ with $q<p<2q$ was analyzed and came up with good approximation of $\varphi(N)\approx N-\frac{a+b}{\sqrt{ab}}\sqrt{N}$. We show that $\frac{k}{d}$ can be obtain as one of the convergent of continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}$ if $d<\frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$ which subsequently led to polynomial time factorization of the modulus N .

Lemma1: Let p and q be prime factors of the multi prime power modulus $N=p^2q^2$. if $q<p<2q$ and $p^2q+pq^2-pq>p^2+q^2$, then $\varphi(N)<N-(p^2+q^2)$

Proof: Taken $N=p^2q^2$ and $q<p<2q$ where $\varphi(N)=p^{2-1}q^{2-1}(p-1)(q-1)$ then

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

but $p^2q+q^2p>p^2+q^2$

Then $\varphi(N)<N-(P^2+q^2)$

.

Lemma 2: Let p and q be a distinct prime numbers and the multi prime power modulus $N=p^2q^2$. If there exist two small positive integers a and b such that $\frac{b}{a}$ is close to $\frac{q^2}{p^2}$ for $a>b$, $p>q$ and $\left(bq^2-ap^2\right)\left(bp^2-aq^2\right)<0$, then $\varphi(N)<N-\frac{a+b}{\sqrt{ab}}\sqrt{N}$.

Proof : Since $\left(bq^2-ap^2\right)\left(bp^2-aq^2\right)<0$, then

$$\left(b^2p^2q^2-abq^4-abp^4+a^2q^2\right)<0$$
$$\left(a^2+b^2\right)p^2q^2<ab\left(p^4+q^4\right).$$

Adding $2abp^2q^2$ to both sides we have

$$\left(a+b\right)^2p^2q^2<ab\left(p^2+q^2\right)^2$$
$$\left(a+b\right)^2N<ab\left(p^2+q^2\right)^2$$

Then $\varphi(N) < N - \frac{(a+b)\sqrt{N}}{\sqrt{ab}}$

Lemma 3: Let multi prime power modulus $N = p^2q^2$ such that $q < p < 2q$. If there exist $\left[a(b^2+1)q^2 - b(a^2+1)p^2\right](bq^2 - ap^2) > 0$, then $\frac{(a+b)\sqrt{N}}{\sqrt{ab}} - \left(p^2+q^2\right) < \frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}$

Proof: We first compute $\left(\frac{a+b}{\sqrt{ab}}\sqrt{N} - (p^2+q^2)\right)\left(\frac{a+b}{\sqrt{ab}}\sqrt{N} + (p^2+q^2)\right) - \left(bq^2-ap^2\right)^2$

Expanding the brackets we have $\frac{(a+b)^2}{ab}N - (p^2+q^2)^2 - \left(bq^2-ap^2\right)^2$

$$(a+b)^2 N - ab(p^2+q^2)^2 - ab\left(bq^2-ap^2\right)^2$$

$$= -\left(a^3b+ab\right)p^4 + \left(a^2+2a^2b^2+b^2\right)p^2q^2 - \left(ab^3+ab\right)q^4$$

$$= \left(-ab^3q^4 - abq^4 + a^2b^2p^2q^2 + b^2p^2q^2\right) + \left(a^2b^2p^2q^2 + a^2p^2q^2 - a^3bp^4 - abp^4\right)$$

$$= bq^2\left(-ab^2q^2 - aq^2 + a^2bp^2 + bp^2\right) - ap^2\left(-ab^2q^2 - aq^2 + a^2bp^2 + bp^2\right)$$

$$= -\left[a(b^2+1)q^2 - b(a^2+1)p^2\right]\left(bq^2-ap^2\right)$$

Since $\left[a(b^2+1)q^2 - b(a^2+1)p^2\right](b^2p - a^2q) > 0$, we get

$$\left(\frac{a+b}{\sqrt{ab}}\sqrt{N} - (p^2+q^2)\right)\left(\frac{a+b}{\sqrt{ab}}\sqrt{N} + (p^2+q^2)\right) - \left(bq^2-ap^2\right)^2 < 0$$

$$\frac{a+b}{\sqrt{ab}}\sqrt{N} - \left(p^2+q^2\right) < \frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}\sqrt{N} + N + -\varphi(N)\right)}$$

$$\frac{a+b}{\sqrt{ab}}\sqrt{N} - \left(p^2+q^2\right) < \frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}$$

Theorem 6: Let p and q be prime numbers where $q^2 < p^2 < 2q^2$ and $N = p^2q^2$ be RSA variant. Given (e, N) for $e < \varphi(N)$ as a public key pair and (d, p, q) as a private key tuple and prime difference $\left|bq^2 - ap^2\right| < N^{\gamma}$. If $\frac{q^2}{p^2}$ is close to $\frac{b}{a}$ such that the relation $\left[a(b^2+1)q^2 - b(a^2+1)p^2\right](bq^2-ap^2) > 0$ holds and $d < \frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$ then $\frac{k}{d}$ can be obtained efficiently from a convergent of the continued fraction expansion of $\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N}}$ for $k < d$ and (a, b) are positive integers less than $\log N$.

Proof: Since $\left[a(b^2+1)q^2-b(a^2+1)p^2\right](bq^2-ap^2)>0$, and $(bq^2-ap^2)<N^{\gamma}$,then from Lemma 3 it was shown that $\left(\frac{a+b}{\sqrt{ab}}\sqrt{N}-(p^2+q^2)\right)<\frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}$

$$\left(\frac{a+b}{\sqrt{ab}}\sqrt{N}-N+\varphi(N)\right)<\frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}$$

Using RSA key equation $ed=k\varphi(N)+1$ where $k\in Z$ we have

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

Applying $N-\frac{a+b}{\sqrt{ab}}\sqrt{N}$ as approximation of $\varphi(N)$, this gives

$$\left|\frac{e}{\varphi(N)}-\frac{k}{d}\right|=\left|\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}-\frac{k}{d}\right|$$

$$=\left|\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}-\frac{e}{\varphi(N)}+\frac{e}{\varphi(N)}-\frac{k}{d}\right|$$

$$\leq\left|\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}-\frac{e}{\varphi(N)}\right|+\left|\frac{e}{\varphi(N)}-\frac{k}{d}\right|$$

$$=\frac{e\left|\varphi(N)-(N-\frac{a+b}{\sqrt{ab}}\sqrt{N})\right|}{\varphi(N)\left(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}\right)}+\frac{1}{d\varphi(N)}$$

$$\frac{e\left|\frac{\left(bq^2-ap^2\right)^2}{\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}\right|}{\varphi(N)\left(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}\right)}+\frac{1}{d\varphi(N)}$$

Since $\left|bq^2-ap^2\right|<N^{\gamma}$ and $1<e<\varphi(N)$, then

$$\left|\frac{e}{\varphi(N)}-\frac{k}{d}\right|<\frac{N^{2\gamma}}{\left(N-\frac{a+b}{\sqrt{ab}}\sqrt{N}\right)\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}}+\frac{1}{d\varphi(N)} \quad \ldots\ldots\ldots\ldots(x)$$

Assuming $N-\frac{a+b}{\sqrt{ab}}\sqrt{N}>\frac{4ab}{(a+b)^2}N$, $\left(\frac{a+b}{\sqrt{ab}}+2\right)\sqrt{N}>\frac{(a+b)^2}{ab}\sqrt{N}$, $\varphi(N)>\frac{3}{5}N$ and $N>6d$ where a and b are small integers. Plugging these conditions into inequality (x)

$$\left|\frac{e}{\varphi(N)}-\frac{k}{d}\right|<\frac{N^{2\gamma}}{\frac{4ab}{(a+b)^2}N\left(\frac{a^2+b^2}{ab}+2\right)\sqrt{N}}+\frac{5}{18d^2}<\frac{N^{2\gamma-\frac{3}{2}}}{\frac{4ab}{(a+b)^2}.\frac{(a+b)^2}{ab}}+\frac{5}{18d^2}$$

$$<\frac{N^{2\gamma-\frac{3}{2}}}{4}+\frac{5}{18d^2}.$$

Since $d<\frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$, then

$$\frac{N^{2\gamma-\frac{3}{2}}}{4}+\frac{5}{18d^2}<\frac{1}{2d^2}$$

Hence, we have $\left|\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}-\frac{k}{d}\right|<\frac{1}{2d^2}$ •

.

This shows that $\frac{k}{d}$ is one of the convergent of the continued fraction expansion of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}$ This terminates the proof.

Example 1: This example illustrates how the prime power modulus $N=p^2q^2$ is factored when the value of γ is given as $\frac{1}{2}$.

Let

$N=1076060967016122033182913896002315629966322054830178062970609$.

$e=396898986798534714299500290526269737654920338179640762622987$.

$a=3, b=2$ and taking continued expression of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}$ gives

$$\left[\begin{array}{l}0,2,1,2,2,6,8,9,8,8,7,1,57,2,11,1,28,1,1,2,4,1,108,66,1,1,1,2,8,1,2,1,6,12,1,1,14,52,2,1,1,10,3,18,1,2,1,2,\\2,1,3,5,2,58,24,3,1,17,2,11,1,9,1,1,1,1,4,3,1,5,27,10,17,2,2,1,1,37,2,5,1,7,1,1,8,2,21,1,2,2,3,2,3,79,2,1,\\16,2,2,2,1,3.\end{array}\right]$$

While the corresponding convergents are given as

$$\left[0,\frac{1}{2},\frac{1}{3},\frac{3}{8},\frac{7}{19},\frac{45}{122},\frac{567}{995},\frac{3348}{9077},\frac{27151}{73611},\frac{220556}{597965},\frac{1571043}{4259366},\frac{1791599}{4857331},\frac{103692186}{281127233},\frac{209175971}{567111797},.....\right]$$

Taking $\frac{k}{d}=\frac{1791599}{4857331}$ and from $ed-k\varphi(N)=1$ we have $\varphi(N)=\frac{ed-1}{k}$

$$\varphi(N)=107606096701611991430175281727798327359141853794875563401 8704$$

$$N-\varphi(N)+1=211888116107872442235637470351688142242895 1906$$

Also, $\gcd(\varphi(N),N)=\lambda$

$$\lambda=10373335852155380943037996913 53$$

Finally solving the quadratic equation $x^2-(N-\varphi(N)+1)x+\lambda=0$ lead to the factorization of the variant N which successfully reveals primes p and q as

$$p=945526668191029$$

$$q=1097096063086357\,.$$

However, by taking $\gamma=0.5$, it was shown that $1791599<4857331..$ Also our result indicated that the short decryption exponent bound obtain is greater than that of Wiener (1990) $d<\frac{1}{3}N^{\frac{1}{4}}$. This shows that $\frac{1}{3}N^{\frac{1}{4}}<d<\frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$,

Numerically, $3.394985820\times10^{14}<4857331<9.602469980\times10^{14}$. Furthermore, the result of Abdullah and Ariffin (2015) was extended from $d<\frac{1}{2}N^{\frac{1}{4}}$ to $d<\frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$ .which also numerically represented as $5.092478730\times10^{14}<4857331<9.602469980\times10^{14}$

4.0 CONCLUSION

This paper established cryptanalytic attacks on variant $N=p^2q^2$ that can be used to factor the modulus in polynomial time using prime difference of $\left|bq^2-ap^2\right|<N^{\gamma}$. This paper also provided an improve bound $d<\frac{2\sqrt{2}}{3}N^{\frac{3}{4}-\gamma}$ using an approximation of parameter $\varphi(N)\approx N-\frac{a+b}{\sqrt{ab}}\sqrt{N}$ where $\frac{k}{d}$ was found by taking the convergent of the continued fraction expression of $\frac{e}{N-\frac{a+b}{\sqrt{ab}}\sqrt{N}}$.

REFERENCES

Abdrahman, N. N., and Ariffin, M. R..K. (2016). New Practical Attack on RSA Modulus of $N=p^2q$. *International journal of Pure and Applied Mathematics*, ***110*** **(4)**, 587 – 80. https://www.ijpam.eu/contents/2016-110-4/3/3

Abubakar, S. I. (2020). Factoring of RSA Modulus $N=pq$ Using Small Prime Difference Method. Ph.D. Thesis, Universiti Putra Malaysia, Selangor, Malaysia,

Abubakar, S. I., Ariffin, M. R. K., and Asbullah, M. A. (2019). A New Improved Bound for Short Decryption Exponent on RSA Modulus $N=pq$ Using Wiener's Method. Malaysian Journal of Mathematical Sciences, 13(s), 89 - 90. https://www.researchgate.net/publication/334519827

Abubakar, S. I., Shehu, S., and Zaid (2021). Technique of Factoring Multi Prime Power Modulus $N = p^2q^2$. Caliphate Journal of Science and Technology, (CaJoST), https://cajost.com.ng/index.php/files/article/download/98/107

Abd Rahman, .N. N., and Ariffin, M. R. K. (2016). New Week Findings upon RSA Modulo Type $N = p^2q$. Global Journal of Pure and applied Mathematics, 12, 3159 – 3185.

Ariffin, M. R. K., Abubakar, S. I., Yunos, F. and Asbullah, M. A. (2019). New Cryptanalytic Attack on RSA modulus $N = pq$ Using Small Prime Difference Method. Journal of cryptography, https//doi.org/1013390/crypto3010002

Asbullah, M. A., and Ariffin, M. R. K. (2015). New Attack on RSA with Modulus N = p2q Using Continued Fraction. Journal of Physics, Conference Series, Pp 2 - 8. https://iopscience.iop.org/article/10.1088/1742-6596/622/1/012019

Chen, C. Y., Hsueh, C. C;, and Lin, Y. F. (2009). A Generalization of de Weger's Method. IEEA, 1, 344 – 47.

Lenstra, A. K., Lenstra, H. W., and Lovasz, L. (1982). Factoring Polynomials with Rational Coefficients. Mathemasche, Annelen, 261, 515 – 534. http://doi.org/10.1007/BF01457454

Lu, Y., Peng, L., and Sarkar, S. (2017). Cryptanalysis of RSA Variant with Moduli. De Gruvter, 11(2), 117 – 130.

Nitaj, A. (2013). Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem. In Artificial Intelligence, Evolutionary Computing and Metheuristics; Springer, 139–168. https://link.springer.com/chapter/10.1007/978-3-642-29694-9_7.

Olzak, T. (2012). Chapter 7: The role of Cryptography in information security https://resources.infosecinstitute.com

Shehu, S., and Ariffin, M. R. (2017). New Attack on Prime Power $N = p^rq$ Using Good Approximation of $\varphi(N)$. Malaysian Journal of mathematical Sciences II(s), 121 – 138. https://mjms.upm.edu.my/fullpaper/2017-August-11(S)/Shehu,%20S.-121-138.

Shehu, S., Abubakar, S. I., and Ibrahim, Z. (2020). Polynomial time Attacks for Modulus $N = p^2q^2$. Journal of Applied Mathematics and Computation, 4(4), 230 – 240. https://wap.hillpublisher.com/ArticleDetails.aspx?cid=439.

Takagi, T. (1998). Fast RSA – Type Cryptosystem Modulo $N = p^kq$. In Advance in Cryptography- CRYPTO '98, Lecture note in Computer Science, Pp 317 -326 Springer. https://link.springer.com/chapter/10.1007/bfb0055738

Wiener, M. (1990). Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inform. Theory, 36, 553 – 558. https://link.springer.com/chapter/10.1007/3-540-46885-4_36