British Journal of Mathematics & Computer Science
14(1): 1-8, 2016, Article no.BJMCS.23036
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic Curves

P. Anuradha Kameswari[1*] and L. Jyotsna[1]

[1] *Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India.*

Authors' contributions

This work was carried out in collaboration between both authors. Author PAK designed the study, wrote the protocol and wrote the first draft of the manuscript and managed literature searches. Author LJ managed the analyses of the study and literature searches. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/23036
Editor(s):
(1) Dariusz Jacek Jakbczak, Chair of Computer Science and Management in this Department, Technical University of Koszalin, Poland.
Reviewers:
(1) Anand Nayyar, KCL Institute of Management and Technology, India.
(2) S. K. Rososhek, Tomsk State University, Tomsk, Russia.
(3) Vipin Saxena, Babasaheb Bhimrao Ambedkar University, Lucknow, India.
(4) Anonymous, China University of Mining and Technology, China.
Complete Peer review History: http://sciencedomain.org/review-history/13055

Short Research Article

Received: 11th November 2015
Accepted: 5th January 2016
Published: 23rd January 2016

Abstract

The studies on Wiener's attack on RSA with small deciphering exponents led to the refinement of attack bounds on the deciphering exponent in the paper "Revisiting Wiener's Attack - New Weak Keys in RSA" by Subhamoy Maitra and Santanu Sarkar. Further in the paper " Extending The Wiener's Attack to RSA-Type Cryptosystem" by R. G. E. Pinch, it is proved that Wiener's attack on RSA Cryptosystem with small deciphering exponent may be extended to RSA-like Cryptosystems on elliptic curves. Now in this paper we show that the Wiener's extension on RSA that refines the attack bound on deciphering exponent can also be extended to RSA-like Cryptosystems on elliptic curves.

Keywords: RSA cryptosystem; elliptic curve.

2010 Mathematics Subject Classification: 94A60.

**Corresponding author: E-mail: panuradhakameswari@yahoo.in;*

1 Introduction

RSA Cryptosystem [1] is the first public key Cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977 where the encryption and decryption are based on the fact that if $N = pq$ is the modulus for RSA, p, q distinct primes, if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d, the multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} = m \bmod N$, for any message m, an integer in Z_N. The security [2] of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes.

Wiener [3] showed that RSA Cryptosystem has a weakness if the private deciphering exponent $d < \frac{N^{\frac{1}{4}}}{\sqrt{2}}$. In [4], Boneh and Durfee showed that RSA is weak for $d < N^{0.292}$. In [5] Subhamoy Maitra and Santanu Sarkar shown that RSA is weak when $d = N^{\delta}$, $\delta < \frac{1}{2} - \frac{\gamma}{2}$, where $|\rho q - p| \leq \frac{N^{\gamma}}{16}$, $\gamma \leq \frac{1}{2}$ for $1 \leq \rho \leq 2$ and also for $d < \frac{1}{2}N^{\delta}$ along with a condition on exponent $e = O(N^{\frac{3}{2}-2\delta})$, $\delta \leq \frac{1}{2}$ and some extensions considering the difference $p - q$ are also given. In [6] R.G.E Pinch has shown that the Wiener's attack extends to RSA-like Cryptosystems over elliptic curves. In this paper we show that the Wiener's extension on RSA that refines the attack bound on deciphering exponent can also be extended to RSA-like Cryptosystems on elliptic curves. The study is based on developing certain estimates of Euler function $\varphi(N)$ and $\psi(N)$ an analogue to $\varphi(N)$.

2 Wiener's Attack on RSA Cryptosystem

The main idea of Wiener's attack [3] is that certain restrictions of d allow the fraction $\frac{t}{d}$ to be a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\varphi(N)}$, this follows by using the approximation theorem.

Theorem 2.1. (**Approximation Theorem**): Let r be a real number, for any integer a and b with $\gcd(a, b) = 1$ such that $|r - \frac{a}{b}| < \frac{1}{2b^2}, b \geq 1$ then $\frac{a}{b}$ is convergent of r. [7]

Theorem 2.2. (Wiener's ttack): Let $N = pq$, for $q < p < 2q$ be the modulus for RSA, e be the public enciphering exponent and d be the deciphering exponent. If $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{6}}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N}$, for $t = \frac{ed-1}{\varphi(N)}$.

Theorem 2.3. (**Implementation of Wiener's attack**): Let $d \leq \frac{N^{\frac{1}{4}}}{\sqrt{6}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\varphi'(N) = \frac{ed'-1}{t'}, x' = \frac{N-\varphi'(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.

The idea of Wiener is that certain restrictions of d allow to obtain a convergent of $\frac{e}{N}$ that is useful in finding the factors p, q of N and the deciphering exponent d. In [5] Subhamoy Maitra and Santanu Sarkar proposed Wiener's extension on RSA cryptosystem improving the attack bound for the decryption exponent d. In the following section we recall the corresponding results for Wiener's extension [8].

3 Wiener's Extension on RSA

Wiener's extension on a RSA Cryptosystem, refining the attack bound is based on following theorem [9]. Wiener's extension is the idea of obtaining a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ rather than that of $\frac{e}{N}$, which increases the bound of d, from $N^{\frac{1}{4}}$ to N^{δ}, for $\frac{1}{4} < \delta < \frac{3}{4} - \beta$. These ideas are based on developing certain estimates for $\varphi(N)$.

Theorem 3.1. Let $N = pq$ for $q < p < 2q$ be the modulus of RSA with the enciphering exponent e and the deciphering exponent d. For $\Delta = p - q = N^{\beta}$, if $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$.

Theorem 3.2. (Implementation of Wiener's Extension) Let $d < N^{\frac{3}{4}-\beta}$ for $p - q = N^{\beta}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1-2N^{\frac{1}{2}}}$, take $\varphi'(N) = \frac{ed'-1}{t'}, x' = \frac{N-\varphi(N)+1}{2}$ and $y' = \sqrt{x'^2 - N}$. If $x', y' \in \mathbb{N}$, then the private key $(q, p, d) = (x' - y', x' + y', d')$.

Implementation of extension of Wiener's attack is the same as implementation of Wiener's attack on RSA Cryptosystem.

4 Extending Wiener's Extension to RSA-like Cryptosystems over Elliptic Curves

$E : y^2 = x^3 + Ax + B$ is the Weierstrass form of an Elliptic curve. For any finite field $\mathbb{F}_q$ of characteristic p, $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q; y^2 = x^3 + Ax + B\} \cup \{\infty\}$ is the elliptic curve over $\mathbb{F}_q$. In 1985 Koblitz [10] and Miller [11] independently proposed using the group of points on an elliptic curves over finite fields in discrete log cryptosystems, as there are no sub exponential time algorithms to find the discrete log on elliptic curves.

The elliptic curves considered by Koyama-Maurer-Okamoto-Vanstone [12][13] for KMOV system are the elliptic curves in the form

$$E_b(N) : y^2 = x^3 + b \bmod N \text{ for } N = pq,\ p, q \text{ primes with } p \equiv q \equiv 2 \bmod 3.$$

The curves $E_b(p) : y^2 = x^3 + b \bmod p$ and $E_b(q) : y^2 = x^3 + b \bmod q$ are super singular with orders $\#E_b(p) = p+1$ & $\#E_b(q) = q+1$. Further as the group $E(\mathbb{Z}_{pq})$ is such that $E(\mathbb{Z}_{pq}) \simeq E(\mathbb{Z}_p) \oplus E(\mathbb{Z}_q)$, the order of the group $E(\mathbb{Z}_{pq})$ is given as $\#E(\mathbb{Z}_N) = \#E(\mathbb{Z}_p) \cdot \#E(\mathbb{Z}_q) = (p+1)(q+1)$ [14].

In the KMOV system the receiver chooses primes p, q with $p \equiv q \equiv 2 \bmod 3$ takes $N = pq$ and chooses e such that $1 \leq e \leq (p+1)(q+1)$ with $\gcd(e, (p+1)(q+1)) = 1$ and makes (N, e) public. The sender represents the message $M = (m_1, m_2)$ as a point on elliptic curve $E_b : y^2 = x^3 + b$, for $b = m_2^2 - m_1^3 \bmod N$. The message is encrypted as $C = eM$ and the cipher text C is sent to the receiver. The receiver for decryption uses the decryption exponent d such that $1 \leq d \leq (p+1)(q+1)$ with $ed \equiv 1 \bmod (p+1)(q+1)$ and obtains the message as $dC = deM = M \bmod N$. The computations are carried using the Group laws on elliptic curves [12][15][16][17].

Pinch in his paper [6] showed that Wiener's attack applies to KMOV as well. In [5] Subhamoy Maitra and Santanu Sarkar proposed Wiener's extension on RSA cryptosystem improving the attack bound for the decryption exponent d. In this paper we show that Wiener's extension also applies to the above RSA like cryptosystems over elliptic curves(KMOV). This is done by looking at $\psi(N) := (p+1)(q+1)$ as an analogue of Euler's function $\varphi(N)$. In the above RSA like cryptosystems over the specific elliptic curves $E_b : y^2 = x^3 + b \bmod N$, Wiener's extension is extended by developing certain estimates on $\psi(N)$, we prove the results regarding the estimates for $\psi(N)$ in the following.

Lemma 4.1. *If $q < p < 2q$ and $\psi(N) = (p+1)(q+1)$ then $N+1+2N^{\frac{1}{2}} < \psi(N) < N+1+\frac{3}{\sqrt{2}}N^{\frac{1}{2}}$.*

Proof.

$$\begin{aligned} \text{We have } \psi(\mathrm{N}) &= (p+1)(q+1) \\ &= N + 1 + pq \\ &> N + 1 + 2N^{\frac{1}{2}} \text{ as } \mathrm{p} + \mathrm{q} > 2\mathrm{N}^{\frac{1}{2}} \ldots (1) \end{aligned}$$

Also We have $\left(\mathrm{p}+\mathrm{q}+\frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}\right)\left(\mathrm{p}+\mathrm{q}-\frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}\right)<0$ for $\mathrm{q}<\mathrm{p}<2\mathrm{q}$.

Then $\left(\mathrm{p}+\mathrm{q}-\frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}\right)$ should be less than 0.

Therefore $\psi(\mathrm{N})=\mathrm{N}+1+\mathrm{p}+\mathrm{q}<\left(\mathrm{N}+1+\frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}\right)$ as $\left(\mathrm{p}+\mathrm{q}-\frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}\right)<0$ ...(2).

From (1) and (2) $N+1+2N^{\frac{1}{2}}<\psi(N)<N+1+\frac{3}{\sqrt{2}}N^{\frac{1}{2}}$. □

Theorem 4.2. (Wiener's Extension on RSA over $E(\mathbb{Z}_N)$) Let $N=pq$ for $q<p<2q$ with the enciphering exponent e and deciphering exponents d such that $\frac{ed-1}{t}=\psi(N)$. If $\Delta=p-q=N^{\beta}, d<N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$.

Proof. We have

$$\begin{aligned}
\left|\frac{e}{N+1+2N^{\frac{1}{2}}}-\frac{t}{d}\right| &= \left|\frac{e}{N+1+2N^{\frac{1}{2}}}+\frac{e}{\psi(N)}-\frac{e}{\psi(N)}-\frac{t}{d}\right| \\
&\leq \left|\frac{e}{N+1+2N^{\frac{1}{2}}}-\frac{e}{\psi(N)}\right|+\left|\frac{e}{\psi(N)}-\frac{t}{d}\right| \\
&= e\left|\frac{1}{N+1+2N^{\frac{1}{2}}}-\frac{1}{\psi(N)}\right|+\frac{1}{\psi(N)d}, \text{ as e}>0 \text{ and ed}-1=\psi(\mathrm{N})\mathrm{t}. \\
&< \psi(N)\left|\frac{\psi(N)-(N+1+2N^{\frac{1}{2}})}{(N+1+2N^{\frac{1}{2}})\psi(N)}\right|+\frac{1}{\psi(N)d}, \text{ as e}<\psi(\mathrm{N}). \\
&= \psi(N)\left|\frac{N+1+p+q-N-1-2N^{\frac{1}{2}}}{\psi(N)(N+1+2N^{\frac{1}{2}})}\right|+\frac{1}{\psi(N)d} \\
&= \frac{p+q-2N^{\frac{1}{2}}}{N+1+2N^{\frac{1}{2}}}+\frac{1}{\psi(N)d} \text{ as p}+\mathrm{q}-2\mathrm{N}^{\frac{1}{2}}>0. \\
&< \frac{\Delta^2}{4N^{\frac{1}{2}}}\left(\frac{1}{N+1+2N^{\frac{1}{2}}}\right)+\frac{1}{\psi(N)d}, \\
&\qquad \text{as p}+\mathrm{q}-2\mathrm{N}^{\frac{1}{2}}=\frac{\Delta^2}{\mathrm{p}+\mathrm{q}+2\mathrm{N}^{\frac{1}{2}}}. \\
&< \frac{\Delta^2}{4N^{\frac{1}{2}}}\left(\frac{1}{\varphi(N)}\right)+\frac{1}{\varphi(N)d}, \\
&\qquad \text{as N}+1+2\mathrm{N}^{\frac{1}{2}}>\varphi(\mathrm{N}) \text{ and } \psi(\mathrm{N})>\varphi(\mathrm{N}).
\end{aligned}$$

Therefore $\left|\frac{\mathrm{e}}{\mathrm{N}+1-2\mathrm{N}^{\frac{1}{2}}}-\frac{\mathrm{t}}{\mathrm{d}}\right|<\frac{1}{\varphi(N)}\left(\frac{\Delta^2}{4N^{\frac{1}{2}}}+\frac{1}{d}\right)\ldots(1)$

Now note $\psi(N)>\frac{3}{4}N$, since $p+q<\frac{1}{4}+1$ for all $N^{\frac{1}{2}}>9$ by assuming N is large.

Also note $8d<N$ for all $N^{\frac{1}{4}}>8$, since $d<N^{\frac{3}{4}}$.

Therefore, for $\Delta=N^{\beta}$ and $d=N^{\delta}$ and substitute $\varphi(N)>\frac{3}{4}N$ and $N>8d$ in (1), we get

$$\begin{aligned}
\left|\frac{e}{N+1+2N^{\frac{1}{2}}}-\frac{t}{d}\right| &< \frac{1}{3}N^{2\beta-\frac{3}{2}}+\frac{4}{3Nd} \\
&< \frac{1}{3}N^{2\beta-\frac{3}{2}}+\frac{1}{6N^{2\delta}}
\end{aligned}$$

and as $2\beta - \frac{3}{2} < -2\beta$ for all $\delta < \frac{3}{4} - \beta$, we have

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

Therefore $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{\frac{1}{2}}}$ for $d < N^{\frac{3}{4}-\beta}$. □

Now using the above estimates for $\psi(N)$ we prove the following theorem of implementation of Wiener's extension.

Theorem 4.3. (Implementation of Wiener's extension):Let $d < N^{\frac{3}{4}-\beta}$ for $p - q = N^{\beta}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N+1+2N^{\frac{1}{2}}}$, take $\psi'(N) = \frac{ed'-1}{t'}, x' = \frac{\psi'(N)-N-1}{2}$ and $\mathrm{y}' = \sqrt{(\mathrm{x}')^2 - \mathrm{N}}$. If $x', y' \in \mathbb{N}$, then $\psi'(N) = \psi(N)$ and the private key is $(p, q, d) = (x' + y', x' - y', d')$.

Proof. For $y' = \sqrt{(x')^2 - N}, N = (x' + y') \cdot (x' - y')$.

If $x', y' \in \mathbb{N}$, then the possible cases are

$$\begin{aligned}
&\text{(i)}(\mathrm{x}' - \mathrm{y}') = 1 \text{ and } (x' + y') = N \\
&\text{(ii)}(\mathrm{x}' - \mathrm{y}') = \mathrm{q} \text{ and } (x' + y') = p \text{ , as } N = pq \text{ and } \mathrm{q} < \mathrm{p}. \\
&\text{For } (\mathrm{x}' - \mathrm{y}') = 1 \text{ and } (x' + y') = N, \text{ we have } \frac{\mathrm{N}+1}{2} = \mathrm{x}'. \\
&\text{Then } \psi'(\mathrm{N}) - \mathrm{N} - 1 = 2x' = N + 1. \\
&\text{Thus } 2(\mathrm{N}+1) = \psi'(N). \\
&\qquad = \frac{ed' - 1}{t'} \\
&\qquad < N + 2 + \frac{3}{\sqrt{2}} N^{\frac{1}{2}}, \text{ as } \frac{\mathrm{e}}{\mathrm{N} + 2 + \frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}} < \frac{\mathrm{t}'}{\mathrm{d}'}, \text{ for some } \mathrm{t}', \mathrm{d}' \\
&\qquad\qquad \text{and } \psi(\mathrm{N}) < \mathrm{N} + 1 + \frac{3}{\sqrt{2}}\mathrm{N}^{\frac{1}{2}}. \\
&\text{Therefore } \mathrm{N}^{\frac{1}{2}} < \frac{3}{\sqrt{2}}.
\end{aligned}$$

Which is a contradiction, as we are choosing a large 'N.'

Hence case(i) is not possible.

Therefore, the only possible case is $q = x' - y', p = x' + y'$.

$$\begin{aligned}
\text{By defining of } x', \text{we have } x' &= \frac{\psi'(N) - N - 1}{2} \\
\text{Then } \psi'(\mathrm{N}) &= 2x' + N + 1 \\
&= p + q + N + 1 \\
&= \psi(N)
\end{aligned}$$

Now as $ed' = 1 \bmod \psi'(N)$ and $\psi'(N) = \psi(N), d = d'$.

Therefore, for $\psi'(N), x', y' \in \mathbb{N}$, the private key $(p, q, d) = (x' + y', x' - y', d')$. □

The following example demonstrates the working of KMOV cryptosystem.

Example 4.4. The receiver chooses primes $p = 5, q = 11$ takes $N = pq = 55$. Then he chooses $e = 5$ and makes (N, e) public.

The sender chooses a message $M = (2, 3)$, a point on the elliptic curve $E_b : y^2 = x^3 + 1 \bmod 55$ and enciphers the message as $C = eM \bmod N$ and sends the cipher text C to the receiver. The computations are done by using the group laws on elliptic curves and the algorithms like doubling and adding algorithm [15] may be used for computations

$$\begin{aligned} C = 5M = 5(2,3) &= (1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)(2,3) \\ &= (2(2(2,3)) + (2,3)) \\ &= (2, 52) \bmod 55. \end{aligned}$$

For decryption the receiver computes $29C \bmod 55$ as follows

$$\begin{aligned} 29C &= (1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1.2^0)C \\ &= 2(2(2(2(2,52)))) + 2(2(2(2,52))) + 2(2(2,52)) + (2,52) \bmod 55 \\ &= (2,3) \bmod 55 \\ &= M \bmod 55, \text{ the required message.} \end{aligned}$$

Example 4.5. ***(Implementation of Wiener's extension)***

Let $(N, e) = (10610503, 8916809)$ be the public key.

The continued fraction of

$$\begin{aligned} \frac{e}{N + 1 + 2N^{\frac{1}{2}}} &= \frac{8916809}{10610503 + 1 + 2 \cdot (10610503)^{\frac{1}{2}}} \\ &\sim 0.83985 \\ &= [0; 1, 5, 4, 11, 5, 2, 1, 1, 1 \ldots] \end{aligned}$$

The first five convergents of the above continued fractions are

$$\frac{0}{1}, \frac{1}{1}, \frac{5}{6}, \frac{21}{25}, \frac{236}{281}, \ldots [18][19].$$

The required convergent is $\frac{236}{281}$ as $\psi'(N) = 10617048, x' = 3272, y' = 309$ are such that $\psi'(N), x', y' \in \mathbb{N}$.

Therefore the private key $(p, q, d) = (x' + y', x' - y', d') = (3581, 2963, 281)$.

5 Conclusion

The idea of Wiener is that certain restrictions of d allow to obtain a convergent of $\frac{e}{N}$ that is useful in finding the factors p, q of N and the deciphering exponent d. Further Wiener's extension is the idea of obtaining a convergent of $\frac{e}{N+1-2N^{\frac{1}{2}}}$ rather than that of $\frac{e}{N}$, which increases the bound of d, from $N^{\frac{1}{4}}$ to N^{δ}, for $\frac{1}{4} < \delta < \frac{3}{4} - \beta$. These ideas are based on developing certain estimates for $\varphi(N)$; Looking at $\psi(N) = (p + 1)(q + 1)$ as the analogue of Euler's function $\varphi(N)$ in the RSA like cryptosystems over the specific elliptic curves $E_b : y^2 = x^3 + b \bmod N$, Wiener's extension is extended by developing certain estimates on $\psi(N)$.

Competing Interests

The authors declare that no competing interests exist.

References

[1] Neal Kobliz. A course in number theory and cryprography. ISBN 3-578071-8, SPIN 10893308.

[2] Boneh D. Twenty years of attacks on the RSA cryptosystem.
Available: http://www.ams.org/notices/199902/boneh.pdf

[3] Wiener M. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory. 1990;36(3):553-558.

[4] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. on Information Theory. 2000;46(4):1339-1349.

[5] Subhamoy Maitra, Santanu Sarkar. Revisiting Wiener's attack - New Weak Keys in RSA.
Available: http://eprint.iacr.org/2005/228.pdf

[6] Pinch RGE. Extending the Wiener's attack to RSA-Type cryptosystem. Electronics Letters. 1995;31:1736-1738.

[7] Rosen KH. Elemetary number theory and its applications. Addison-Wesley, Reading Mass; 1984.

[8] Anuradha Kameswari P, Jyotsna L. Wiener's attack and its extensions on RSA cryptosystem. M.Phil dissertation, Department of Mathematics, Andhra University; 2012.

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

[10] Neal Koblitz. Elliptic curves cryptosystems. Mathematics of Computation. 1987;48:203-209.

[11] Miller VS. Use of elliptic curves in cryptography. In H.C. Willianms, editor Advances in Cryptology-CRYPTO 85, Volume 218 of Lecture notes in Computer Science. Springer-Verlag. 1986;417-426.

[12] Lawrence C Washington. Elliptic curves number theory and cryptography. Second edition, Chapman & Hall/CRC; 2008.

[13] Song Y. Yan. Number theory for computing, 2nd edition. Springer, ISBN:3-540-43072-5.

[14] Anuradha Kameswari P, Praveen Kumar L. Encryption on elliptic curves over Zpq with arithmetic on E(Zpq) via E(Zp) and E(Zq). (International Organization of Scientific Research) IOSR Journal of Mathematics, e- ISSN: 2278-5728. 2014;10(6).

[15] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography. Springer, ISBN:978-0-387-77993-5.

[16] Anuradha Kameswari P, Praveen Kumar L. Implementation of GCD attack with Projective Coordinates on Demytko's Cryptosystem. International Journal of Computer Applications. 2015;124(6):33-40. ISSN: 0975-8887.

[17] Anuradha Kameswari P, Praveen Kumar L. Implementation of signature scheme with projective coordinates on elliptic curve cryptosystem. International Research Journal of Mathematics, Engineering and IT. 2015;2(7):1-15. ISSN: 2349-0322.

[18] Burton D. Elementary number theory, Sixth edition. Mc Graw Hill, New York; 2007.

[19] Devenport H. The higher arithmetic, Eight edition. Cambridge University Press, ISBN-13 978-1-107-68854-4.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/13055