Extension of Wiener's Approach on Security on Aadhaar Card based ATM System

Rashmi Singh
Department of Computer Science
Babasaheb Bhimrao Ambedkar
University (A Central University)
Lucknow (U.P.) 226025,
India

ABSTRACT
Cryptography is necessary for the security of the data which may in the form of text, audio and video. In general Symmetric and Asymmetric cryptographical methods are used for the above purpose. In which all types of data is converted into the binary number system. Due to non availability of the cryptographical system, hackers may have hack the data. For the strong security, various researcher have used RSA cryptosystem which is widely used in the digital signature. In the present paper, an extension of RSA cryptography is well explained for the three variables. An implementation of the proposed RSA system for three variables is demonstrated through the implementation of the Wiener's extension. Various theorems with proof are given in the paper and implementation is given on the Aadhaar card based ATM system.

Keywords
Cryptography, Digital Signature, Hackers, Symmetric, Asymmetric

1. INTRODUCTION
The cryptosystem is frequently used for providing security and authenticity of digital data and secure remote login session. In the present time, Rivest-Shamir-Adleman (RSA) approach is widely used in various commercial systems [1]. Lots of industries are using secure RSA digital signature for online transaction. In cryptography, Kobliz [2] has studied various approaches of sending messages in different form in such a way that only authorized user can remove distinguish and the original message. Wiener's method of continued fraction finds the new weaknesses in RSA and affecting factors of weak keys to improve the security [3]. The attack of Wiener's approach on RSA cryptosystem with a small deciphering exponent expends to system using other groups such as elliptic curves [4]. Selecting an RSA modulus with a little difference of its prime factors provides developments on the exponent attack of Wiener's approach [5]. A cryptanalytic attack generates the use of short RSA secret exponent and is well defined in literature. This cryptanalytic attack generates the use of an algorithm based on continued fractions that identifies the numerator and denominator of a fraction in polynomial time when a closed enough estimate of the fraction is known. This attack acts as a no threat to the normal case of RSA where the secret exponent is almost having the same size as the modulus [6]. There is a practical survey on principles and implementation of crypto graphical methods for security over network and practical applications that have been implemented to provide security over the network [7]. On the basis of analysis, there are two types of concurrent evolution in cryptography. Various applications of teleprocessing have given advance need for new types of crypto graphic system which reduce the need for secure key distribution channel and provide the identical signature [8].

In the RSA public key cryptosystem, if the private exponent d is less than $N^{0.292}$, then the system is insecure. This is the first advancement over an old effect of Wiener which shows when d is less than $N^{0.25}$, then the RSA cryptosystem is not secure [9]. In the Wiener's theory the verification of the optimum predictor decreases the result of an integral equation, which is improved form of the wiener-Hopf equation. The use of the theory is represented by different practical examples [10]. Encrypted Image-Based Reversible Data Hiding (EIRDH) is a common opinion of information hiding. In this process, there are three entities which take part as image provider, data hider and receiver. A new technique has been proposed for encrypted image-based reversible data hiding using public key cryptography from various expansions. The basics of the proposed technique are to preprocess an image with the quality of various expansions before encryption of an image. This technique gives good payload and improves quality of image [11]. In the data transmission, security is the most significant and important issue over network. In data transmission, Deoxyribo Nucleic Acid (DNA) cryptography plays a crucial role and this concept is not used only to store data but also perform computations. In wireless network DNA cryptography with Secure Socket Layer (SSL) provide a secure channel with secure interchange of information [12]. Some variants of RSA and analysis of cryptanalytic attack against these variants are efficient RSA; dependent RSA provided semantic security to the original RSA and third variants is Carmichael RSA uses the Carmichael function [13]. The RSA algorithm included with the operation of large numbers. The key length is increased for providing significant security [14]. New variants of RSA key generation algorithm give two different key pairs having same public and private exponents. Due to these variants it is known as dual RSA and the use of dual RSA decreases the storage essential for key [15]. The industry standard digital signature scheme is used in different domains in various industries to obtain the security level in various applications [18].

The present work is based on the three variables RSA cryptosystem and implemented in ATM transaction which is based on Aadhaar card and demonstrated by the help of the Wiener's algorithm. This paper deals with the implementation of the Wiener algorithm on the security system. The security system is based on the cash withdrawal from the ATM machine and transaction is based on the unique identification i.e. Aadhaar card number. The purpose of this paper is to provide the authenticity in the transaction from the ATM.

2. MATERIAL AND METHODS

2.1 Wiener's Attack on modified RSA Cryptosystem

Let us consider the three prime number as p, q, r which are used for the Wiener's attack on the RSA cryptosystem which is explained below for the three prime numbers:

We have $N = pqr$, for $r < p < 2r$ be the modulus for RSA, e is the public enciphering exponent and d is the deciphering exponent. If $d \le \frac{N^{\frac{1}{4}}}{\sqrt{6}}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N}$, where $t = \frac{ed-1}{\phi(N)}$,

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

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

$= pqr - qr - pr + r - pq + q + p - 1$

$= N - (qr + pr + pq) + (p + q + r - 1)$

$= ((p+q+r)-1) + N - (A+1)$ Where $A = (pq + qr + rp)$

We have $ed = 1 + t\phi(N)$, here d allows the fraction $\frac{t}{d}$ to be convergent of $\frac{e}{N}$ and $t = \frac{ed-1}{\phi(N)}$

Then $e = \frac{1}{d} + \frac{t}{d}\phi(N)$

Divided by N

$\frac{e}{N} = \frac{1}{dN} + \frac{t}{dN}\phi(N)$

$\frac{e}{N} = \frac{1}{dN} + \frac{t}{dN}(p + q + r - 1) + N - A$

$\frac{e}{N} = \frac{1}{dN} + \frac{(p+q+r)t}{dN} - \frac{t}{dN} + \frac{t}{d} - \frac{At}{dN}$

$\left(\frac{e}{N} - \frac{t}{d}\right) = \frac{(p+q+r-1)}{N}\frac{t}{d} - \frac{At}{dN} + \frac{1}{dN}$

$\left(\frac{e}{N} - \frac{t}{d}\right) = \frac{(p+q+r-1-A)t}{dN} + \frac{1}{dN}$

$\left(\frac{e}{N} - \frac{t}{d}\right) = \frac{p+q+r-1-A}{N} + \frac{1}{dN}$

Also Note that

$\left|\frac{e}{N} - \frac{t}{d}\right| = \frac{(t(N - \phi(N) - 1)}{dN} > 0$ Since N> $\phi(N)$ and $t \ge 1$

$\left|\frac{e}{N} - \frac{t}{d}\right| = \frac{p+q+r-1-A}{N} + \frac{1}{dN}$

$= \frac{p+q+r}{N} - \left[\frac{A}{N} - \frac{1}{dN}\right]$

$< \frac{p+q+r}{N}$

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

$< \frac{3}{6d^2}$ for $d \le \frac{n^{1/4}}{\sqrt{6}}$

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

Hence From the approximation theorem $\frac{t}{d}$ is a convergent of $\frac{e}{N}$. Let us consider a numerical example, let $p = 3, q = 5, r = 11$, then $N = pqr$ =165,
$\phi(N) = (p-1)(q-1)(r-1) = 80$

where $1 < e < \phi(n)$

Now gcd (e,n) =1, where e is public key and find d

Such that d*e= mod $\phi(n) = 1$

d= $e^{-1} \pmod{80}$

let e= 7

d= $7^7 \pmod{80}$

d = 23

public key= (7, 165)

private key= (23, 165)

C= $M^e \pmod{n}$

M= $C^d \pmod{n}$

C= $(15)^7 \pmod{165}$

C= 60

M= $(60)^{23} \pmod{165}$

M=15

2.2 Implementation of Wiener's Extension on modified RSA

Let $d \le \frac{N^{1/4}}{\sqrt{6}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\phi'(N)$= $\frac{ed'-1}{t'}$, x'= $\frac{N - \phi'(N) + 1}{2}$ and y'= $\sqrt{x'^2 - N}$. If $x', y' \in N$, then the private key $(p, q, r, d) = (x' - y', x' + y', 1, d')$

Proof: let $x', y' \in N$ and by definition of y'

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

= $(x' - y')(x' + y')$

Since $(x' - y')(x' + y') \in N$, hence are factors of N.

Then $(x' - y')(x' + y') = 1$, p, q, r or N

Now as q < p and r =1, we have four cases

(i) $1 = x' - y'$ and $N = x' + y'$

(ii) $p = x' + y'$, $q = x' - y'$ and $r = 1$

(iii) $p = 1$, $q = x' - y'$ and $r = x' + y'$

(iv) $p = x'+ y'$, $q = 1$ and $r = x'- y'$

Where $x', y' \in N$

Case 1: Now we will show that case (i) is not possible:

For, if $x'- y' = 1$ and $x'+ y' = N$ then $\frac{N+1}{2} = x'$

Since $x' = \frac{N - \phi(\mathrm{N}) + 1}{2}$, then $\frac{N+1}{2} = \frac{N - \phi'(\mathrm{N}) + 1}{2}$

This implies that $N + 1 = N - \frac{ed'-1}{t'} + 1$

$$\frac{ed'-1}{t'} = 0$$

Then $ed'-1 = 0$

Thus e=1, therefore case (i) is not possible, since e>1

Hence, the case (ii) is possible.

Case 2: $q = x'- y'$ and $p = x'+ y'$, $r = 1$

When ever $x', y' \in N$ (1)

To show d=d'

By definition of x', we have $x' = \frac{N - \phi'(\mathrm{N}) + 1}{2}$

$$\text{Then } \phi'(\mathrm{N}) = \mathrm{N} - 2x' + 1$$
$$= N - (\mathrm{p} + \mathrm{q} + \mathrm{r}) + 1$$
$$= \phi(\mathrm{N})$$

Now $\phi'(\mathrm{N}) = \frac{ed'-1}{t'}$, we have $ed' = 1 \bmod \phi'(\mathrm{N})$

Then $ed' \equiv \bmod \phi(\mathrm{N})$

Which gives $d' \equiv d \bmod \phi(\mathrm{N})$ (2)

Since the sequence of denominators of convergent are strictly increasing d'≯ d

Then $d' \le d$

$d < \phi(\mathrm{N}), \mathrm{d}' < \phi(\mathrm{N})$ from (2) we have

d=d' (3)

From (1) and (3)

the private key (q, p, r, d) = (x'- y', x'+ y', 1,d')

Case 3: $q = x'- y'$, $r = x'+ y'$ and $p = 1$

where ever $x', y' \in N$ (1)

To show d=d'

By definition of x'

$$x' = \frac{N - \phi'(\mathrm{N}) + 1}{2}$$

$$\phi'(\mathrm{N}) = N - 2x' + 1$$
$$= N - (\mathrm{p} + \mathrm{q} + \mathrm{r}) + 1$$
$$= \phi(\mathrm{N})$$

Now $\phi'(\mathrm{N}) = \frac{ed'-1}{t'}$, we have $ed' \equiv 1 \bmod \phi'(\mathrm{N})$

Then $ed' \equiv \bmod \phi(\mathrm{N})$

Which gives $d' \equiv d \bmod \phi(\mathrm{N})$ (2)

Now the convergent of $\frac{t}{d}$ is either $\frac{t'}{d'}$ or occur after $\frac{t'}{d'}$

Since the sequence of denominators of convergent are strictly increasing, d'≯ d.

Then d'≤ d

Since $d < \phi(\mathrm{N})$, $d' < \phi(\mathrm{N})$ and from (2)

we have d= d' (3)

From (1) and (3)

the private key is (q, p, r, d) =(x'- y', 1, x'+ y', d').

Case 4: $q = 1$, $r = x'- y'$, $p = x'+ y'$

where ever $x', y' \in N$ (1)

To show d=d'

By definition of x'

$$x' = \frac{N - \phi'(\mathrm{N}) + 1}{2}$$

$$\phi'(\mathrm{N}) = N - 2x' + 1$$
$$= N - (\mathrm{p} + \mathrm{q} + \mathrm{r}) + 1$$
$$= \phi(\mathrm{N})$$

Now $\phi'(\mathrm{N}) = \frac{ed'-1}{t'}$, we have $ed' \equiv 1 \bmod \phi'(\mathrm{N})$

Then $ed' \equiv \bmod \phi(\mathrm{N})$

Which gives $d' \equiv d \bmod \phi(\mathrm{N})$ (2)

Now the convergent of $\frac{t}{d}$ is either $\frac{t'}{d'}$ or occur after $\frac{t'}{d'}$.

Since the sequence of denominators of convergent are strictly increasing, d'≯ d. (3)

Then d'≤ d

Since $d < \phi(\mathrm{N})$, $d' < \phi(\mathrm{N})$ and from (2) we have

d= d' (3)

From (1) and (3)

the private key is (q, p, r, d) = (1, x'+ y', x'- y', d').

1. Wiener's Extension on RSA

Let $N = pqr$ for $r < p < 2r$ be the modules of RSA with the enciphering exponent e and deciphering exponent d. For Δ= $p - q - r = N^{\beta}$, If $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N + 1 - 2N^{1/2}}$.

Proof: By the definition of e, d there exists a positive integer t such that $ed - t\phi(\mathrm{N}) = 1$. It can be written as

$$\frac{e}{\phi(\mathrm{N})} - \frac{t}{d} = \frac{1}{\phi(\mathrm{N})\mathrm{d}} \qquad (4)$$

(4)

For $r < p < 2r$ the bounds for $\phi(\mathrm{N})$ are

$$N + 1 - \frac{3}{\sqrt{2}} N^{1/2} < \phi(\mathrm{N}) < \mathrm{N} + 1 - 2\mathrm{N}^{1/2} \qquad (5)$$

We have

$$\Delta^2 = (\mathrm{p} + \mathrm{q} + \mathrm{r} - 2\mathrm{N}^{1/2})(\mathrm{p} + \mathrm{q} + \mathrm{r} + 2\mathrm{N}^{1/2})$$

Since

$$\Delta^2 > 0, p + q + r - 2N^{1/2} > 0$$

Therefore $0 < p + q + r - 2N^{1/2} < \dfrac{\Delta^2}{4N^{1/2}}$ (6)

Now

$$\left|\frac{e}{N+1-2N^{1/2}} - \frac{t}{d}\right| \le \left|\frac{e}{N+1-2N^{1/2}} - \frac{e}{\phi(\mathrm{N})} + \frac{e}{\phi(\mathrm{N})} - \frac{t}{d}\right|$$

$$\le \left|\frac{e}{N+1-2N^{1/2}} - \frac{e}{\phi(\mathrm{N})}\right| + \left|\frac{e}{\phi(\mathrm{N})} - \frac{t}{d}\right|$$

$$= e\left|\frac{1}{N+1-2N^{1/2}} - \frac{1}{\phi(\mathrm{N})}\right| + \left|\frac{e}{\phi(\mathrm{N})} - \frac{t}{d}\right| \text{ , since e>0}$$

As $e < \phi(\mathrm{N})$ and $\dfrac{e}{\phi(\mathrm{N})} - \dfrac{t}{d} = \dfrac{1}{\phi(\mathrm{N})\mathrm{d}}$, then

$$\left|\frac{e}{N+1-2N^{1/2}} - \frac{t}{d}\right| < \phi(\mathrm{N})\left|\frac{\phi(\mathrm{N}) - (\mathrm{N}+1-2N^{1/2})}{((\mathrm{N}+1) - 2\mathrm{N}^{1/2})\phi(\mathrm{N})}\right| + \frac{1}{\phi(\mathrm{N})d}$$

$$< \phi(\mathrm{N})\left|\frac{N+1-2N^{1/2} - \phi(\mathrm{N})}{(\mathrm{N}+1-2\mathrm{N}^{1/2})\phi(\mathrm{N})}\right| + \frac{1}{\phi(\mathrm{N})d}$$

$$< \left|\frac{N+1-2N^{1/2} - \phi(\mathrm{N})}{(\mathrm{N}+1-2\mathrm{N}^{1/2})}\right| + \frac{1}{\phi(\mathrm{N})d}$$

$$< \frac{\Delta^2}{4N^{1/2}}\left(\frac{1}{\phi(\mathrm{N})}\right) + \frac{1}{\phi(\mathrm{N})d}$$

Using (5) and substituting $p + q + r = N + 1 - \phi(\mathrm{N})$ in (6)

$\phi(\mathrm{N}) > \dfrac{3}{4} N$, since

$p + q + r < \dfrac{1}{4} N + 1 \quad \forall \quad N^{\frac{1}{2}} > 9$ by (6)

$\phi(\mathrm{N}) = \mathrm{N} + 1 - (\mathrm{p} + \mathrm{q})$

We have $\phi(\mathrm{N}) > \mathrm{N} + 1 - \dfrac{1}{4} N - 1$

$\phi(\mathrm{N}) > \dfrac{3}{4} \mathrm{N}$

Also note

$8d < N \forall N^{1/4} > 8$, since $d < N^{\frac{3}{4}}$. (5)

Therefore,

$\phi(\mathrm{N}) > \dfrac{3}{4} N$ and $N > 8d$

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

and $2\beta - \dfrac{3}{2} < -2\delta \quad \forall \quad \delta < \dfrac{3}{4} - \beta$, we have

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

Therefore, $\dfrac{t}{d}$ is a convergent of $\dfrac{e}{N+1-2N^{1/2}}$ where $\delta < \dfrac{3}{4} - \beta$ holds.

Lemma 1: If $r < p < 2r$ and $\xi(\mathrm{N}) = (\mathrm{p}+1)(\mathrm{q}+1)(\mathrm{r}+1)$ then $2N^{1/2} < \dfrac{3}{\sqrt{2}} N^{1/2}$.

Proof: we have $\xi(\mathrm{N}) = (\mathrm{p}+1)(\mathrm{q}+1)(\mathrm{r}+1)$

$$= pqr + (\mathrm{pr} + \mathrm{pq} + \mathrm{qr}) + \mathrm{r} + \mathrm{q} + \mathrm{p} + 1$$

$$> N + 1 + 2N^{1/2} + A$$

$$(\mathrm{p} + \mathrm{q} + \mathrm{r} + \frac{3}{\sqrt{2}} \mathrm{N}^{1/2})(\mathrm{p} + \mathrm{q} + \mathrm{r} - \frac{3}{\sqrt{2}} \mathrm{N}^{1/2}) < 0 \quad \forall \quad p + q > 2N^{1/2}$$

Then

$\left(p + q + r - \dfrac{3}{\sqrt{2}} N^{1/2}\right)$ should be less than 0 $\forall \quad r < p < 2r$ then

$\xi(\mathrm{N}) = \mathrm{N} + \mathrm{p} + \mathrm{q} + \mathrm{r} + 1 + \mathrm{A} < \mathrm{N} + 1 + \dfrac{3}{\sqrt{2}} N^{1/2}$ as

$p + q + r - \dfrac{3}{\sqrt{2}} N^{1/2} < 0$

$2N^{1/2} < \dfrac{3}{\sqrt{2}} N^{1/2}$

Theorem 1: (Wiener's Extension on RSA over P (Zn)) Let $N = pqr$ are prime number such that $r < p < 2r$ with the enciphering exponents e and deciphering exponents d such

that $\frac{ed-1}{t} = \phi(N)$ .If Δ= p-q-r = N^{β} , $d < N^{\frac{3}{4}-\beta}$, then $\frac{t}{d}$ is a convergent of $\frac{e}{N+1+2N^{1/2}}$.

Proof: We have

$$\left|\frac{e}{N+1+2N^{1/2}} - \frac{t}{d}\right| = \left|\frac{e}{N+1+2N^{1/2}} + \frac{e}{\phi(N)} - \frac{e}{\phi(N)} - \frac{t}{d}\right|$$

$$\leq \left|\frac{e}{N+1+2N^{1/2}} - \frac{e}{\phi(N)}\right| + \left|\frac{e}{\phi(N)} + \frac{t}{d}\right|$$

$$= e\left|\frac{1}{N+1+2N^{1/2}} - \frac{1}{\phi(N)}\right| + \frac{1}{\phi(N)d} \qquad e>0$$

$$= e\left|\frac{1}{N+1+2N^{1/2}} - \frac{1}{\phi(N)}\right| + \frac{1}{\phi(N)d} \text{ as } ed-1 = \phi(N)$$

$$= \phi(N)\left|\frac{\phi(N) - (N+1+2N^{1/2})}{\phi(N)(N+1+2N^{1/2})}\right| + \frac{1}{\phi(N)d} \text{ as } e < \phi(N)$$

$$= \phi(N)\left|\frac{N+p+q+r+1+A-N-1-2N^{1/2}}{\phi(N)(N+1+2N^{1/2})}\right| + \frac{1}{\phi(N)d}$$

$$= \frac{(p+q+r-2N^{1/2})+A}{(N+1+2N^{1/2})} + \frac{1}{\phi(N)d}$$

$$= \frac{A}{N+1+2N^{1/2}} + \frac{\Delta^2}{p+q+r+2N^{1/2}}\frac{1}{N+1+2N^{1/2}} + \frac{1}{\phi(N)d}$$

$$< \frac{\Delta^2}{4N^{1/2}}\left(\frac{1}{N+1+2N^{1/2}}\right) + \frac{A}{N+1+2N^{1/2}} + \frac{1}{\phi(N)d} \text{ as}$$

$N+1+2N^{1/2} > \phi(N)$

$$< \frac{\Delta^2}{4N^{1/2}}\left(\frac{1}{\phi(N)}\right) + \frac{1}{\phi(N)d} \quad \text{Neglecting } \frac{A}{N+1+2N^{1/2}}$$

Therefore

$$\left|\frac{e}{N+1-2N^{1/2}} - \frac{t}{d}\right| < \frac{1}{\phi(N)}\left(\frac{\Delta^2}{4N^{1/2}} + \frac{1}{d}\right)$$

Note that $\phi(N) > \frac{3}{4}N$.

Since $p+q+r < \frac{1}{4}+1 \quad \forall \quad N^{1/2} > 9$ by assuming N is large.

Also Note 8d<N for all $N^{1/4} > 8$, such that $d < N^{3/4}$.

Therefore, for

$\Delta^2 = N^{\beta}$ and $d = N^{\delta}$ and $\phi(N) > \frac{3}{4}N$ and $N > 8d$

We get

$$\left|\frac{e}{N+1+2N^{1/2}} - \frac{t}{d}\right| < \frac{1}{3}N^{2\beta-3/2} + \frac{4}{3Nd}$$

$$< \frac{1}{3}N^{2\beta-\frac{3}{2}} + \frac{1}{6N^{2\delta}}$$

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

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

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

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

Proof: For y'= $\sqrt{(x')^2 - N}$, $N = (x'+y').(x'-y')$. If x', y'ϵ N, then the possible cases are

(i) $(x'-y') = 1$ and $(x'+y') = N$

(ii) $(x'-y') = q$, $(x'+y') = p$ and r=1,as $N = pqr$ and r<p

(iii) $(x'-y') = q$, $1 = p$ and $r = (x'+y')$

(iv) $(x'+y') = p$, $(x'-y') = r$ and q=1

Case (i): For $(x'-y') = 1$ and $(x'+y') = N$,

we have $\frac{N+1}{2} = x'$,then $\phi'(N) - N - 1 = 2x' = N+1$

Thus $2(N+1) = \phi'(N)$

$$= \frac{ed'-1}{t'}$$

$< N+2+\frac{3}{\sqrt{2}}N^{1/2}$ as $\frac{e}{N+2+\frac{3}{\sqrt{2}}N^{1/2}} < \frac{t'}{d'}$, for some t', d' and $\phi(N) < N+1+\frac{3}{\sqrt{2}}N^{1/2}$.

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

Which is a contradiction, as we are choosing a large 'N'. Hence case (1) is not possible.

Case 2: $(x'-y') = q$, $(x'+y') = p$ and r=1

By defining of x', we have $x' = \frac{\phi'(N) - N - 1}{2}$

$$\phi'(N) = 2x' + N + 1$$

$$= p + q + r + N + 1$$

$$= \phi(N)$$

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

Therefore, for $\phi'(N), x', y' \in N$, the private key $(p, q, r, d) = (x'+y', x'-y', 1, d)$.

Case 3: $(x'-y') = q$, $1 = p$ and $r = (x'+y')$

we have $x' = \frac{\phi'(N) - N - 1}{2}$

$$\phi'(N) = 2x' + N + 1$$

$$= p + q + r + N + 1$$

$$= \phi(N)$$

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

Therefore, for $\phi'(N), x', y' \in N$, the private key $(p, q, r, d) = (1, x'-y', x'+y', d)$.

Case 4: $(x'+y') = p$, $(x'-y') = r$ and $q = 1$

We have $x' = \frac{\phi'(N) - N - 1}{2}$

$$\phi'(N) = 2x' + N + 1$$

$$= p + q + r + N + 1$$

$$= \phi(N)$$

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

Therefore, for $\phi'(N), x', y' \in N$,

the private key $(p, q, r, d) = (x'+y', 1, x'-y', d)$.

3. RESULTS AND DISCUSSION

3.1 Demonstration of Proposed Algorithm

The following table 1 shows the conversion of Aadhaar Card Number (Plain Text) into the cipher text with the help of public key and then converting the cipher text into the plain text i.e. Aadhaar Card Number by using the private key. This algorithm takes the following steps:

Step 1:- Break the Aadhaar Card Number (Plain Text) into single digit number and then on that single digit number further operation will take place.

Step 2:- In this step the ASCII value of the individual digit of Aadhaar number (Plain text) is calculated.

Step 3:- Now Cipher text is calculated by using public key, $C=M^e \pmod n$, where M is the plain text i.e. the individual digit of Aadhaar number, e is the public key and n = pqr (where p, q and r are prime numbers).

Step 4:- In this step cipher text which is calculated in previous step is converted in to plain text by using private key, $M=C^d \pmod n$ Where C is the Cipher text, d is the private key and n= pqr. In this step original digit of Aadhaar Card number (plain text) is retrieved i.e. M.

On the basis of above let the Aadhaar Card Number 325942315251 which is used as a Plain Text by the private and public keys. The plain text is encrypted and decrypted. The complete computations are given in following table.

Table 1: Demonstration of Proposed Algorithm on Aadhaar Card Number

Aadhaar Card No.(Plain Text)	ASCII value	$C=M^e \bmod n$	$M=C^d \bmod n$	Plain Text
3	51	6	51	3
2	50	140	50	2
5	53	92	53	5
9	57	18	57	9
4	52	13	52	4
2	50	140	50	2
3	51	6	51	3
1	49	124	49	1
5	53	92	53	5
2	50	140	50	2
5	53	92	53	5
1	49	124	49	1

4. CONCLUSION

The idea of Wiener approach provides the security of Aadhaar Card based ATM system and it is more secure for transaction through ATM machine. In this paper Wiener's idea for certain restrictions allow to obtain a convergent result that is used for finding the various factors used in the algorithm for RSA cryptosystem with enciphering exponent and deciphering exponent. We demonstrated the proposed algorithm on ATM card security by using Aadhaar card which may provide more security with better convergence of results. The results are depicted for considering the private and public keys from the three variables implemented RSA cryptosystem.

5. REFERENCES

[1] D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203-213, 1999.

[2] D. N. Kobliz, "A Course in Number Theory and Cryptography", Springer-Verlag New York Berlin Heidelberg London Paris Tokyo Hong Kong Barcelona Budapest, ISBN 3-578071-8, Second Edition 1987.

[3] S. Maitra and S. Sarkar, "Revisiting Wiener's Attack New Weak Keys in RSA", Springer-Verlag Berlin Heidelberg, Vol. 5222, pp. 228-243, 2008.

[4] R. G. E. Pinch, " Extending The Wiener's Attack to RSA- Type Cryptosystem", Electronics Letters 31 (1995), 1736-1738.

[5] B. de Weger, "Cryptanalysis of RSA with Small Prime Difference", AAECC 13, 17–28 (2002).

[6] M. Wiener, "Cryptanalysis of Short RSA Secret exponents", IEEE Transaction on Information Theory, Vol. 36(3), 553-558,1990.

[7] W. Stallings (1998) "Cryptography and Network Security", Third Edition, 2006.

[8] W. Diffie and M. E. Hellman "New Directions in Cryptography", IEEE Transaction on Information Theory, 1978.

[9] D. Bonch, G. Durfee "Cryptanalysis of RSA with private key d less than N0.292", IEEE Transaction on Information Theory, Vol. 46, (4), 1339-1349,2000.

[10] L.A. Zadeh and J. R. Ragazzini "An Extension of Wiener's Theory of Prediction", Journal of Applied Physics, IEEE Xplore Vol. 21, (7), 645-655,.

[11] C.W. Shiu, Y. C. Chen and W. Hong "Encrypted image-based reversible data hiding with public key cryptography from difference expansion", Signal processing: Image Communication, Vol. 39,226-233, 2015.

[12] Monika and S. Upadhyaya "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks", 4th International Conference on Eco-friendly computing and communication systems, Procedia computer science, 70, (2015) 808-813.

[13] K. Balasubramanian, "Variants of RSA and their cryptanalysis", Communication and Network Technologies (ICCNT), 2014 International Conference on, Sivakasi, pp. 145-149, 2014.

[14] Chu-Hsing Lin; Jung-Chun Liu; Cheng-Chieh Li and Po-Wei Chu, "Parallel Modulus Operations in RSA Encryption by CPU/GPU Hybrid Computation," in Information Security (ASIA JCIS), 2014 Ninth Asia Joint Conference on , vol., no., pp.71-75, 3-5 Sept. 2014.

[15] Hung-Min Sun; Mu-En Wu; Wei-Chi Ting; Hinek, M.J., "Dual RSA and Its Security Analysis," in Information Theory, IEEE Transactions on, vol.53, no.8, pp.2922-2933, Aug. 2007.

[16] R. C. Das, P. P. Purohit, T. Alam and M. Chowdhury, "Location based ATM locator system using OpenStreetMap," Software, Knowledge, Information Management and Applications (SKIMA), 2014 8th International Conference on, Dhaka, ,pp. 1-6, 2014.

A. M. Antony, R. Aswathy and K. H. Keerthana, "3G ATM," Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on, Coimbatore, pp. 421-423, 2013,.

[17] Roy A. and Karforma S., "A survey on Digital Signatures and its Applications". J. of Comp. and I.T. Vol. 3(1and2), 45-69 ,2012.

[18] Hinek M. J., Low, M. K., Taske, E., "On Some Attacks on Multi-prime RSA", proceeding in SAC '02 Revised Papers from the 9th Annual International Workshop on Selected Areas in cryptography, pp. 385-404, 2002.

[19] P.A. kameswari, L. Jyotsana, "Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic Curves", British Journal of Mathematics & Computer Science, Vol. 14, pp. 1-8, 2016.