Three Novel Theorems for Applied Cryptography

Rahul Yadav
Scholar (Master of Technology)
Department of CS, SunRise University, Alwar
Rajasthan, India

Deepak Chaudhary
Assistant Professor
Department of CS, IET, Alwar
Rajasthan, India

ABSTRACT
With advancements in computing capabilities public key cryptosystems are going to be more complex yet vulnerable over the modern day's computer networks and associated security mechanism, especially those based on novel approaches of applied mathematics. This paper explores three novel theorems derived while studying and implementing RSA algorithm, one of the strongest public key cryptosystem. The proposed Theorems are best suited and adequate for RSA algorithm yet being applicable to some of other existing algorithms and theorems of applied mathematics. The first theorem deals with concept of ambiguity while calculating multiplicative inverse of encryption key which in some of instances returns undesirable negative numbers not useful as decryption key . Second theorem deals with unconcealed multiplicative inverses, unconcealed are values which remain unchanged after any mathematical transformations. Concept of unconcealed multiplicative inverses is useful in key generation for RSA cryptosystem. Third theorem deals with the concept of unconcealed exponentiation modulo quite useful in finding unconcealed signature and messages to form UM Matrix for RSA.

General Terms
Cryptography, Public Key Cryptosystem, RSA Algorithm, Novel Theorems, & Applied Mathematics for Computers

Keywords
Quarter division of Ring, Unconcealed Transformation, Ambiguous Values, Bézout's identity, Extended Euclid algorithm

1. INTRODUCTION
Most of the modern day's Public Key Cryptosystems are applications of mathematical approaches designed for data security, especially public key cryptosystem. While dealing with implementation of RSA we found many applied algorithms as conceptual base of RSA approach of data security, which includes Prime Number generation & their testing (like Miller-Robin Test [1]), Multiplication algorithms (like Booth multiplication [2]), Totient Function, Multiplicative Inverses of the form Bézout's identity. Euclid's Extended Algorithm is one which is capable of easing major computation part of RSA Algorithm's Key generation part. Additionally it's a fact that Fermat's Little Theorem, Euler's Theorem and Totient Function lies on the heart of this cryptosystem.

1.1 RSA ENCRYPTION & DECRYPTION APPROACHES

To encrypt a message *M* with RSA approach, using a public encryption key *(e,n),* proceed as follows. (Here e & *n* are a pair of integers positive in nature.) In very first step, represent the message as an integer between 0 & *n* — 1. (Break a long message into a series of blocks, & represent each block as such an integer.) Users are advised to use any standard notation. Main purpose here is nothing to do with encryption of the message but solitary to get it into the numeric form necessary for enciphering. Then, encrypt the message by raising it to the eth power modulo *n.* That is, the result (the cipher text *C)* is the remainder when *M* is divided by *n. e*

To decrypt the cipher text, raise it to another power *d,* further modulo *n.* The encryption & decryption algorithms *E & D* are thus:

$$C = E(M) = M^e \ (mod\ n), for\ a\ message\ M. \ldots\ldots (1)$$

$$D(C) = C^d \ (mod\ n), for\ a\ cipher\ text\ C. \quad \ldots\ldots (2)$$

Encryption does not result into increased size of a message; both the message & the cipher text are integers in the range 0 to *n* — 1. The *encryption key* is thus the pair of positive integers *(e,n).* Similarly, the *decryption* key is the pair of positive integers *(d, n).* Each user makes his encryption key public, & keeps the corresponding decryption key private. (These integers should properly be subscripted as in, U_A, e_A, & d_A, since each user has his own set. nevertheless, we will solitary consider a typical set, & A will omit the subscripts.) How should you choose your encryption & decryption keys, if you want to use RSA approach?

Users first compute *n* as the product of two prime numbers *p & q:*

$$n = p * q.$$

These prime numbers are very large, "random" prime numbers. Although you will make *n* public, the factors *p & q* will be effectively hidden from everyone else due to the enormous difficulty of finding factors of *n.* It also enables to hide the way *d* can be derived from e.

You then pick the integer *d* to be a large (in terms of digit / bit count), randomly chosen integer which is relatively prime to totient function of n i.e. *(p* — 1) * *(q* — 1). That is, check that *d* satisfies:

$$gcd(d, (p — 1) * (q — 1)) = 1$$

The integer e is calculated using *p, q, & d* to be the "multiplicative inverse" of *d,* modulo *(p* — 1) • *(q* — 1). Thus we have

$$e * d \equiv 1 \ (mod\ (p — 1) * (q — 1)).$$

We prove in the next section that this guarantees that (1) & (2) hold, i.e. that *E & D* are in verse permutations. The aforementioned approach should not be confused with the "exponentiation" technique presented by Diffie & Hellman to solve the key distribution issue. Their technique permits two users to determine a key in common to be used in a normal

crypto-logical system, and this algorithm is not based on a trap-door one-way permutation

1.2 THE UNDERLYING MATHEMATICS

We demonstrate the rightness of the deciphering algorithm using an identity due to Euler & Fermat: for any integer (message) *M* which is relatively p rime to *n*,

$M^{\varphi(n)} = 1\ (mod\ n)$. …… (3)

Her φ(n) is the Euler Totient function giving number of positive integers less than *n* which are relatively prime to *n*. For prime n umbers *p*,

$\varphi(n) = p - 1.$

In RSA case, we have by elementary properties of the Totient function:

$$\varphi(n) = \varphi(p) * \varphi(q)$$

$= (p - 1) * (q - 1)$…… (4)

$= n - (p + q) + 1.$

Since *d* is relatively prime to, it h as a multiplicative inverse e in the ring of φ(n) integers modulo φ(n)*:*

$e * d \equiv 1\ (mod\ \varphi(n))$. …… (5)

We now prove that equations (1) & (2) hold (that is, that deciphering works rightly if e & *d* are chosen in proper).

$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d (mod\ n) = M^{ed} (mod\ n)$

$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e (mod\ n) = M^{ed} (mod\ n)$

And $M^{ed} \equiv M^{k*\varphi(n)+1} (\text{mod } n)$

$M^{ed} \equiv M^{k*\varphi(n)+1} (mod\ n)$ ……. (for some integer k):

From (3) we see that for all *M* such that *p* does not divide *M*

$M^{p-1} \equiv 1\ (mod\ p)\ \&\ since\ (p - 1)\ divides\ \varphi\ (n)$

This is trivially true when $M = 0\ (mod\ p)$, so that this equality really holds for *all M.*

Arguing similarly for *q* yields

$$M^{k*\varphi(n)+1} \equiv M\ (mod\ g\ )$$

Together these last two equation s imply that for all *M,*

$$M^{e-d} \equiv M^{k*\varphi(n)+1} \equiv M\ (mod\ n)$$

This implies (1) & (2) for all $M, 0 < M < n$. Therefore *E* & *D* are inverse permutations.

Here is simple listing of those existing concepts which lead to formulation of RSA Algorithm.

Table 1: Support algorithms of RSA cryptosystem

Formulation of RSA Step	**Base Concept & Applied Algorithm**
1. Select large and distinct prime integers 'p' and 'q'.	A. Prime Number generation B. Miller-Robin Test
2. Calculate $n = p * q$	C. Booth's Multiplication
3. Calculate $\varphi(n) = (p - 1) * (q - 1)$	D. Euler's Totient Function
4. Choose e, so that $GCD(e, \varphi(n)) = 1$	E. Euclid's Algorithm
5. Calculate d, so that $d \equiv e^{-1}\ mod\ \varphi(n)$	F. Multiplicative Inverse G. Bézout's identity H. Euclid's Extended Algorithm
$C = M^e\ mod\ n,$ $M = C^d\ mod\ n$ Provide M is Message & C is Cipher	I. Fermat's Theorem J. Euler's Theorem K. Inverse Permutations L. Rich Schroeppel derivation

Major focus of discussion in this paper is on Multiplicative Inverse, Unconcealed Keys & Unconcealed Message resulting into three novel theorems. These approaches may play crucial role while going for robust and reliable implementation of RSA Algorithm. This paper is structured into six sections. This 1st section was about the introductory part. 2nd section deals with terminology and definition of frequently used key terms. 3rd section is core part of this paper where three novel theorems are discussed, these theorems are namely 1: Ambiguous Multiplicative Inverses, 2: Unconcealed Multiplicative Inverses and 3: Unconcealed exponentiation modulo. Further section 4 deals with numerical examples and validation of work discussed in previous section three. Section 5 deals with results and discussion while in the 6th section paper is concluded.

2. DEFINITIONS

2.1 Multiplicative Inverse

Two numbers d and e are said to be Multiplicative Inverse of each other in the ring of integers modulo (n) if and only if they satisfy condition $[d * e\ mod\ n = 1]$.

2.2 Unconcealed Multiplicative Inverses

In the case, value of an Integer map to same value as Multiplicative Inverse in the ring of integers modulo (n); this pair is referred as Unconcealed Multiplicative Inverses.

2.3 Quarter division of Ring of integers modulo (n)

if we divide a ring into 4 equal parts in the manner depicted below then such division is referred as Quarter division.

2.4 Unconcealed Messages

If encrypting any input message M resulting into same cipher C, i.e.$M = C$; then these instances of Messages are referred to be unconcealed.

2.5 UM Matrix

This is set of Unconcealed Message values of any cryptosystem.

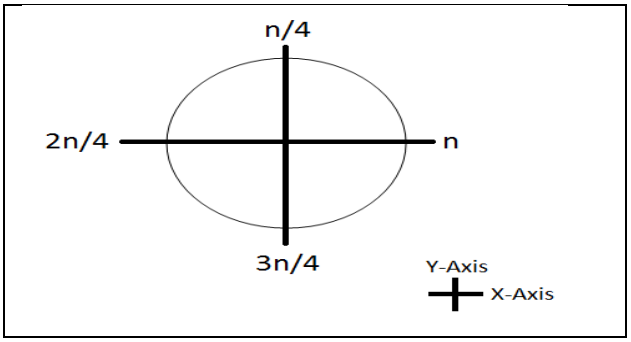

Fig 1: Quarter Division.

3. THEOREMS

3.1 Theorem 1: Ambiguous Multiplicative Inverses

Statement: For all positive integers relatively prime to (n) there are exactly two distinct numbers both having different sign in the ring of integers modulo (n) which satisfy the criteria of Multiplicative Inverse. First of these two numbers says 'F' having lower amplitude [3] can be calculated using Euclid's Extended Algorithm, Second number 'S' having higher amplitude may be defined as:

$$S = F + (n) * \left[F * \frac{-1}{|F|} \right] \quad \text{..... (6)}$$

Proving existence of Ambiguous Multiplicative Inverses:

As in Bézout's identity

$$ax + by = gcd\,(a, b)$$

(Typically either x / y is negative).

A Bézout's identity is the representation of the elements of a finite field under the multiplicative modulo operation.

We can transform the modular multiplicative inverse relation used in RSA [4] into Bézout's identity:

$$d \equiv e^2 mod\ \varphi(n)$$

Implications;

$$d \equiv (1/e)\ mod\ \varphi(n)$$

$$d * e \equiv 1\ mod\ \varphi(n)$$

$$(d * e - 1)\ mod\ \varphi(n) = 0$$

$$(d * e - 1)/\ \varphi(n) = -k \quad /for\ some\ integer\ constant\ k$$

$$de = -k * \varphi(n) + 1$$

$$k * \varphi(n) + de = 1$$

Now $1 = gcd\,(\varphi(n), e)$

$$k * \varphi(n) + de = gcd(\varphi(n), e) \quad \text{..... (7)}$$

The above relation A is of the form Bézout's identity, so for positive values of k, d will be negative.

3.2 Theorem 2: Unconcealed Multiplicative Inverses

Statement: A ring of $positive\ integers\ modulo\ \varphi(n)$, (where φ(n) is totient function of n where $n = p * q$, and p, q are prime [6]) have count of Unconcealed Multiplicative Inverses in the order of 2^{k+1} If we apply Quarter division to any such ring then 4 numbers having Unconcealed Multiplicative Inverses will be in the distance of unity from X-Axis. If Number X Have Unconcealed Multiplicative Inverse then $\varphi(n) - X$ will also have Unconcealed Multiplicative Inverse, [k is count of factor 4 in φ (n)].

3.2.1 Proving existence of Unconcealed Multiplicative Inverses

According to the statement of theorem-2 we have at least 4 Unconcealed Multiplicative Inverses for $\varphi(n) = (p - 1) * (q - 1)$, existence of these four which lies in the distance of unity while applying quarter division can be proved, let $\varphi(n) = g$

According to the theorem 2 & formulation discussed in [15] implementers have these Unconcealed Multiplicative Inverses which are on the distance of unity from X-Axis i.e. position $1, (g/2) - 1, (g/2) + 1, and\ (g - 1)$.

By the analysis of the relation of multiplicative inverse which is $d \equiv e^{-1}\ mod\ \varphi(n)$ we may draw implications as follow,

$$d \equiv (1/e)\ mod\ \varphi(n)$$

$$d * e \equiv 1\ mod\ \varphi(n)$$

$$(d * e)\ mod\ \varphi(n) = 1$$

$$(d * e - 1)\ mod\ \varphi(n) = 0$$

$(d * e - 1)/\ \varphi(n) = f$ //for some integer constant f

$$d = (f * \varphi(n) + 1)/e \quad \text{..... (8)}$$

Now for being unconcealed $e == d$, the practical values of constant f for these unconcealed is given as (::φ(n) = g)

Table 2: Value of fixed multiplier to totient function for some the unconcealed keys

Value of unconcealed	f
1	0
$(g/2) - 1$	$(g/4) - 1$
$(g/2) + 1$	$(g/4) + 1$
$(g - 1)$	$((g - 2)$

Putting these values in relation (2) yields

$(0) * g + 1)/\ 1 = (1)$ ..... (9)

$((g - 2) * g + 1)/\ g - 1 = (g - 1)$ ..... (10)

$(((g/4) - 1) * g + 1)/\ ((g/2) - 1) = (g/2) - 1$ ..... (11)

$(((g/4) + 1) * g + 1)/\ ((g/2) + 1) = (g/2) + 1$ ..... (12)

Proofs:

Unconcealed UCLD(1) denoted by equation (9) is simple $1/1 = 1$ sort of equation hence don't require any proof statement.

Unconcealed UCLD(g-1), denoted by equation (10):

$$(n - 1)^2 = n^2 - 2n + 1$$

$$n - 1 = ((n-2) * n + 1) / (n-1)$$

Unconcealed UCLD(g/2)-1, denoted by equation (11):

LHS =

$= (((g/4) - 1) * g + 1) / ((g/2) - 1)$

$= (((g^2/4) - g) + 1) / ((g/2) - 1)$

$= ((\frac{g}{2})^2 - g + 1) / ((g/2) - 1)$

$= (g/2 - 1) / (g/2 - 1)\ 2$

$= g/2 - 1 = RHS$

Similarly relation …Unconcealed UCLD(g/2)+1, denoted by equation (12) can be proved as

Unconcealed UCLD(g/2)+1:

LHS

$= (((g/4) + 1) * g + 1) / ((g/2) + 1)$

$= (((g^2/4) - g) + 1) / ((g/2) + 1)$

$= ((\frac{g}{2})^2 + g + 1) / ((g/2) + 1)$

$= g/2 + 1 = RHS$

3.3 Theorem 3: Unconcealed exponentiation modulo

Statement: It is impossible to find a Public Key (N, E) of RSA cryptosystem which produce UM Matrix of less than 2^{k+1} members. Unconcealed values are always in group of 8 tuple or in general if X is smallest unconcealed value in group (excluding 1), then group form by X in RSA's UM Matrix is given as:

Table 3: Group formation in unconcealed messages

UM Index	*1:Fixed*	*2*	*3*	*4*
UM Value	1	X	X+1	2X+1
UM Index	*8:Fixed*	*7*	*6*	*5*
UM Value	N-1	N-X	N-X-1	N-2X-1

Proof system of theorem 3 is very much similar to theorem 2 by means of taking help from the analysis of relations in the form of Bézout's identity, and this marginal constrains of this papers are too narrow to fit proof system for it.

4. NUMERICAL EXAMPLES

4.1 Example of Ambiguous Multiplicative Inverses

4.1.1 A simplest example:

Let's have a positive integer e=139 relatively prime to n=160. Now as per the statement of Theorem of Ambiguous Multiplicative Inverses there are exactly two distinct numbers both having different sign in the ring [7] of integers modulo 160 satisfying the criteria of Multiplicative Inverse. First of these two numbers calculated by using Euclid's Extended Algorithm [8] will be F= -61, so Second number 'S' having higher amplitude will be (one can validate results for S*F mod n = 1):

$$S = F + n * [\ (F * -1) / |F|\ ] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

$$= -61 + 160 * [\ (-61 * -1) / |-61|\ ]$$

$$= -61 + 160 * [(+61) / (+61)]$$

$$= -61 + 160 * 1 = 99$$

4.1.2 Validating Result

$(99 * 139)\ mod\ 160 = 13761\ mod\ 160 = 1$; Hence Correct.

4.1.3 Slightly Less Simple Example:

Let's have integer e= 0010 1110 0000 1011 relatively prime to n= 0100 0101 0001 0000, First of multiplicative inverse having lower value calculated using Euclid's Extended Algorithm is F= 0000 0000 0000 0011

Now Calculating S implies

$S = F + n * [\ (F * -1) / |F|\ ]$

$= 000\ 0000\ 0000\ 0011 + 100\ 0101\ 0001\ 0000 * [\ (0000\ 0000\ 0000\ 0011 * -000\ 0000\ 0000\ 0001) / |0000\ 0000\ 0000\ 0011|]$

$= 000\ 0000\ 0000\ 0011 + 100\ 0101\ 0001\ 0000 * [\ (-000\ 0000\ 0000\ 0011) / 0000\ 0000\ 0000\ 0011]$

$= 000\ 0000\ 0000\ 0011 + 100\ 0101\ 0001\ 0000 * -000\ 0000\ 0000\ 0001$

$= 0000\ 0000\ 0000\ 0011 + -100\ 0101\ 0001\ 0000$

$= -\ 100\ 0101\ 0000\ 1101$

Now it's Validation yields

$-\ 100\ 0101\ 0000\ 1101 * 0010\ 1110\ 0000\ 1011\ mod\ 0100\ 0101\ 0001\ 0000$

$= -\ 1100\ 0110\ 1011\ 0100\ 1101\ 1000\ 1111\ mod\ 0100\ 0101\ 0001\ 0000$

$= 1$

Now for the simplicity of readers converting these binary values in simple decimal values let's have e = 11787, n= 17680, F = 3, Calculating S yields S= -17677.

& Validation of these values yields

$-17677 * 11787\ mod\ 17680 = -208358799\ mod\ 17680$

$= 1$

4.2 Examples of Unconcealed Multiplicative Inverses

4.2.1 A simplest example:

In continuation of our previous example for $\varphi(n) = 160$, [9] it have exactly 8 numbers which have Unconcealed Multiplicative Inverses having values $(1, 31, 49, 79, 81, 111, 129, 159)$. Now if Quarter Division is applied to this ring then it results into 4 points$(160, 40, 80, 120)$. Here (160, 80) represents X-Axis and (40, 120) represents Y-Axis. 4 numbers (1, 79, 81, 159) are in the distance of unity from X-Axis, and the rest 4 numbers (31, 49, 111, 129) are in the equal distance 9 from Y-Axis.

4.2.2 Validating values of 4.2.1

$$1^2 \; mod \; 160 = 1 \; mod \; 160 = 1$$

$$79^2 \; mod \; 160 = 6241 \; mod \; 160 = 1$$

$$81^2 \; mod \; 160 = 6561 \; mod \; 160 = 1$$

$$159^2 \; mod \; 160 = 25281 \; mod \; 160 = 1$$

$$31^2 \; mod \; 160 = 961 \; mod \; 160 = 1$$

$$49^2 \; mod \; 160 = 2401 \; mod \; 160 = 1$$

$$111^2 \; mod \; 160 = 12321 \; mod \; 160 = 1$$

$$129^2 \; mod \; 160 = 16641 \; mod \; 160 = 1$$

4.2.3 Slightly Less Simple Example

As in the second example of Theorem II, let's have φ(n) = 17680 which is Totient value [10] (Euler's theory) of n=131*137, Now 4 numbers having unconcealed Multiplicative Inverses which are in distance of unity from X-Axis are (1, 8839, 8841, 17679), All the numbers with unconcealed Multiplicative Inverses of this public key system (PKS) [11] are (1,441,1769,1871,2209,2991,3639,4081,4759, 5201,5849,6631,6969,7071,8399,8839,8841,9281,10609,1071 1,11049,11831,12479,12921,13599,14041,14689,15471,1580 9,15911,17239,17679). (Calculated and validated through various applied approaches [12] discussed in table 1)

4.3 Example of Unconcealed exponentiation modulo

Values can be calculated for all the elements of UM Matrix for RSA cryptosystem having Public Key (187, 3) by using X=33 as smallest unconcealed value (excluding 1). So complete and properly validated [13] UM Matrix for this will be

Table 4: UM Matrix example

UM Index	*1:Fixed*	*2*	*3*	*4*
UM Value	1	X	X+1	2X+1
Calculated	1	33	34	67
UM Index	*8:Fixed*	*7*	*6*	*5*
UM Value	N-1	N-X	N-X-1	N-2X-1
Calculated	186	154	153	120

5. RESULTS AND DISCUSSION

This Paper explores some novel approaches which are quite useful while going for the implementation of RSA cryptosystem and digital signature scheme. All these cryptographic approaches make use of applied mathematics [14]. Some phases like quarter division of ring, UM matrix, and unconcealed multiplicative inverses may be quite non-familiar except those having a deep insight in cryptographic systems. As for the applicability of approaches discussed here is concerned, it is quite relevant to figure out that development and enhancement are the process which are continuous in nature and never ending process.

The concept of ambiguous multiplicative inverses discussed in theorem 1 leads to some sort of ambiguity in RSA key generation. As in the subsequent sections an approach will be discussed, how to avoid the ambiguity in RSA key generation by the use of Theory of multiple multiplicative inverses resides outside the finite field, & will try to find out the relation between these values, & how they will be incorporated in Extended Euclid Algorithm so that it always return a correct positive value.

The principle advantage of using solitary the Extended Euclid algorithm instead of relation (13) in

$$d = (k * \varphi(n) + 1)/e$$

That it sometimes required so long calculation depends on the values of k, which highest value $\varphi(n) - 2$ is dependent on the value of $\varphi(n)$, & this one is not the case for Extended Euclid algorithm. Ambiguity in key generation can be resolved by modifying Extended Euclid algorithm's return value [15].

5.1 Theory of multiple multiplicative inverses resides outside the finite field

As the solution of such kind of ambiguity a hypothesis is observed & the arithmetic proof of it is as per the illustration discussed below, Specified values of e & totient function φ (n) [16] enables us to compute multiple values of d such as

1. User get one of its value falls between 2 to φ (n) which is often used in RSA implementations by the relation,

$$d = k * \varphi(n) + 1 \qquad \text{……. (14)}$$

2. For the some cases when someone use Euclidean approach to find multiplicative inverse he / she get a minimal negative value (d_0), for the cases of the negative Euclidean values if user calculate its corresponding minimal positive value satisfying the criteria of multiplicative inverses, using the relation d = k* φ(n) +1,

User found a relation of the form

$$d_{positive\ \_value} = d_{negative\ \_value} + \varphi(n) \qquad \text{……. (15)}$$

Implementers may generalize the cases & may observe practical proof for it.

The concept described as theorem II - Unconcealed multiplicative inverses discussed in this paper leads to introduction of unconcealed RSA keys, each unconcealed key value fallows one definite relation (11) which is;

$$(e^2 - 1) \; mod \; \varphi(n) = 0 \qquad \text{…… (16)}$$

There may be two approaches to avoid such kind of values,

1. Modifying the structure of Extended Euclid algorithm

2. Placing a check for $(e^2 - 1)\ mod\ \varphi(n) = 0$ in step of selection of key value e, which is step 4 of RSA key generation.

There are few advantages & disadvantages of both of above approaches. If users go for such a check in the calculation of multiplicative inverse [17] in extended Euclid algorithm users have to solitary place a single check of the form $If\ (e == d)$ then return unconcealed & loop back to step number 4, i.e. choose the next value as e so that it is not un-concealed.

……. (17)

In the second case if users go for check in the selection of the key in RSA's step 4 that is

Selecting the value of e such that $gcd(e, \varphi(n)) == 1$

Then the check structure will be of the form;

$(e^2 - 1)\ mod\ \varphi(n) = 0$ Then declare unconcealed & loop back to same step …….. (18)

In the first case it seems to be lengthier task as compared to case second, because program need to loop back after the execution of whole steps of Extended Euclid algorithm, but in the case 2 code need to have a check before the Extended Euclid structure so it don't required lengthier loop back. But if user analyze the complexity of checks, then it will be found that the time & space complexity of (18) is high in a great deal than one in (17), & program have to check for each value of e.

Users will observe the loop back after the execution of Extended Euclid structure in the each unconcealed cases, since there are not too many numbers of unconcealed key values for $\varphi(n) = (p-1) * (q-1)$where p, q prime so this is the case for few values but the performance penalty of relation structure (18) is more high. The relation between performance penalties in both the case conclude that checking the unconcealed values during the calculation of modular [18] multiplicative inverse results into less performance penalty, (approx.)

So it is better practice to check the unconcealed values during the calculation of modular multiplicative inverse e; i.e. case first. Same approach and results are used to design an enhanced version of Extended Euclid algorithm, as described below.

Ex_ Euclid_Modified_RSA_UC(x,y)

{A 1=1, A2=0, A 3=x;

B1=0, B2=1, B3=y;

while(1)

{ if B3 = 0 then return NO_INVERSE;

if B3 = 1 then

{ GCD = B3 and inverse = B2;

if(inverse = = e) then return unconcealed;

// additional check included to discard unconcealed values

else return(GCD, inverse);

}

q=(A3/B3)/1;

T1=A1-(q*B1); T2=A2-(q*B2); T3=A3-(q*B3);

A1=B1; A2=B2; A3=B3; B1=T1; B2=T2; B3=T3;

} }

Same modified version of Extended Euclid algorithm may be used by those implementing RSA, in such a manner which never produces unconcealed key values as these are exclusively handled by modifying the structure of the algorithm used in most of RSA implementation for the purpose of key generation.

Further this version of extended Euclid algorithm was again modified due to effects of theorem I – Ambiguous Multiplicative Inverses, to make use of those key values which were remained unused due to their negative sign. As it was shown that multiplicative inverses over a finite field of integers are also ambiguous in nature and extended Euclid algorithm return only smallest number between those, and it may be either positive or negative, Euclid didn't bothered about its sign.

Ex_ Euclid_Modified_RSA_Uc-NonAmb(x,y)

$\{A\ 1 = 1, A2 = 0, A\ 3 = x;$

$B1 = 0, B2 = 1, B3 = y;$

while(1)

{ if B3 = 0 then return NO_INVERSE;

if B3 = 1 then

$\{\ \boldsymbol{if\ B2} > 0\ then\ GCD = B3\ and\ inverse = B2;$

$\boldsymbol{if\ B2} < 0\ then\ GCD = B\boldsymbol{3\ and\ inverse = B2 + x};$

//Conversion of sign & absolute value is done to prevent extended Euclid algorithm from returning the negative numbers

if(inverse = = e) then return unconcealed; // Additional check included to discard unconcealed values

else return(GCD, inverse);

}

$q = (A3/B3)/1;$

$T1 = A1 - (q * B1);\ T2 = A2 - (q * B2);\ T3 = A3 - (q * B3);$

$\boldsymbol{A1} = \boldsymbol{B1};\ \boldsymbol{A2} = \boldsymbol{B}2;\ A3 = B3;\ B1 = T1;\ B2 = T2;\ B3 = T3;$

} }

The third and last theorem Unconcealed exponentiation modulo require further study, and it seems to having potential strength in the cryptanalysis of RSA cryptosystem. Further it is very much similar to the concept of the unconcealed multiplicative inverses. So one might look for finding the more specific and general relations between unconcealed values, it may be either key or message. By deciding a general formulation about the positioning of the entire unconcealed keys one may be further able to decide the totient function of the composite number n used in RSA cryptosystem.

6. CONCLUSION

Conceptual bases of RSA cryptosystems are identified in this paper. These are the concepts which serve as pillar and over which world's one of the most powerful applied algorithm is designed. Extended Euclid theorem is discussed in details and some modifications into its logical structure are also presented. Further concept of UM Matrix and Quarter Division of Rings is introduced. Some numbers remains unchanged while transformation of any messages through RSA cryptosystem. For those systems where count of factor 4 in φ (n) is exactly 2 (which is likely to happen in maximum of the public key certificates of RSA algorithm as $[p-1]*[q-1]$ are like to produce two even numbers) the relation between the unconcealed messages is discussed by making use of UM Matrix. It is also shown that keys as well as Messages of a Public Key Cryptosystem may be unconcealed. In the core part of this paper three novel theorems are presented which cover Ambiguous Multiplicative Inverses, Unconcealed Multiplicative Inverses and Unconcealed exponentiation modulo. Few modifications in the extended Euclid are also presented as a result of theorems and concepts discussed throughout the contents.

7. ACKNOWLEDGEMENTS

Rahul Yadav: My first thanks to my father Mr. Ram Chandra Yadav and my whole family for their throughout support during all the time of searching of unknown equations and observations of this paper, my gratitude is also extended towards Ms. Monica Tiwari for all her inspirations.Deepak Chaudhary: My thanks to all my family, IET staff and its innovative and quality students always inspiring faculties towards quality of learning.

8. REFERENCES

[1] Miller, Gary L. (1976), "Riemann's Hypothesis and Tests for Primality", Journal of Computer and System Sciences 13 (3): 300–317, http://dx.doi.org/10.1145%2F800116.803773, Ret May 2013.

[2] Stallings, William. Computer Organization and Architecture: Designing for performance, Ninth Edition. ISBN 978-0132936330, New Jersey: Prentice-Hall, Inc. 2012.

[3] Kasana, H.S., Complex Variables: Theory And Applications (3rd ed.), PHI Learning Pvt. Ltd, ISBN 978-8120326415, 2005

[4] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"; Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge; 1978.

[5] Paul Pritchard, "Improved Incremental Prime Number Sieves", Algorithmic Number Theory Symposium, pp. 280–288, 1994.

[6] Wikipedia, the free encyclopedia; Bézout's identity, Modular multiplicative inverse, extended Euclidean algorithm; @ http://en.wikipedia.org/wiki/; ret. June 2013.

[7] Riesel, Hans, Prime Numbers and Computer Methods for Factorization (second edition), Boston: Birkhäuser, ISBN 0-8176-3743-5, 1994.

[8] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Third Edition. MIT Press and McGraw-Hill, ISBN 978-0262033848. Greatest common divisor. July 2009.

[9] Singh, S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999

[10] Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), Untersuchungen uber hohere Arithmetik (Disquisitions Arithmetical & other papers on number theory) (Second edition), New York: Chelsea, ISBN 0-8284-0191-8.

[11] Branchaud, Marc, "A Survey of Public-key Infrastructures", Department of Computer Science, McGill University, Montreal, 1997.

[12] P. Gabrini; CodeWarrior Principles of Programming, Chapter 3. Algorithm, Metrowerks CodeWarrior, Metrowerks Inc. @info.uqam.ca/Members/gabrini_p/ Principles_of_Programming.pdf, Ret. June 2013.

[13] Zeliade W. P.; Model Validation: theory, practice and perspectives. Zeliade White. May, 2011

[14] John Baez; "The Foundations of Applied Mathematics", Theoretic Foundations of Mathematics Workshop @ math.ucr.edu/home/baez/irvine/irvine.pdf. May 2013.

[15] Rahul Yadav, Direndra Yadav, Hriday Gupta, "RSA Operations With Performance Tuning"; Proceedings of ICNICT 2011, KIET, Ghaziabad, Sep 2011.

[16] William Stallings, "Cryptography and Network Security, Principles and Practice", Sixth edition; ISBN 978-0133354690, Prentice Hall, March 2013.

[17] Lemars; Using Multiplicative Inverses to Solve Equations, Lesson 5.6 Pg.247. Nov. 2012. @ lemars.k12.ia.us/webfiles/~/Source/J9B05FAD.pdf.

[18] Boute, Raymond T, "The Euclidean definition of the functions div and mod". ACM Transactions on Programming Languages and Systems (TOPLAS) (ACM Press (New York, NY, USA)) 14 (2): 127–144. http://dx.doi.org/10.1145%2F128861.128862, April 1992.