ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Identifying Quadratic Residuity Using Legendre-Jacobi Symbol

Chitra G.Desai [1],Rupali Bhakkad [2],Sonal Sarnaik[3]

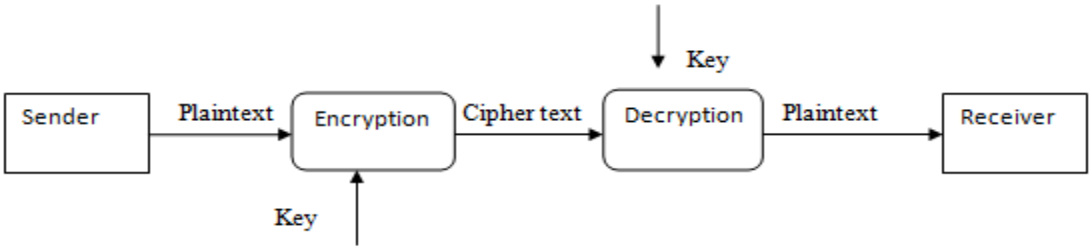
Professor and Head of the Department, Department MCA[1],Marathwada Institute of Technology,Aurangabad, India[1],
Assistant Professor Department MCA[2] , Marathwada Institute of Technology,Aurangabad, India[2] ,
Assistant Professor Department MCA[3], Marathwada Institute of Technology,Aurangabad, India[3]

Abstract: Cryptography is the study of "Mathematical Systems" involving two kinds of security protocols: Privacy and Authentication. The mathematical concepts from the branch of number theory known as Modular arithmetic, Quadratic residue are significantly useful in cryptography. Cryptography Deals with large number integers i.e. integers as big as hundred digits and more. In such situation identifying whether an integer **"a"** is quadratic residue modulo **"p"** where p is Prime can be achieved using Legendre and Jacobi Symbol.
This paper introduces to the mathematical concepts of Quadratic Residue, Fermat's little theorem, Euler's criterion and Legendre and Jacobi symbol. However it has been observed that Jacobi symbol in case of some example fails to give correct result and therefore the Limitation for predicting the quadratic residue.

Keywords: Cryptography, Quadratic residue, Legendre Jacobi symbol

I. INTRODUCTION

Cryptography is the study of exchange of information between sender and receiver over an insecure channel is such a way that the opponent (any third user) cannot understand what is being said [2][13][18].The actual information sender wants to send is called as "Plaintext", sender converts this plaintext in "Cipher text" (by using different techniques) by applying Key to it. This cipher text is very difficult to read, need mathematical knowledge to read it. At receiver this cipher text gets converted into plaintext by applying key (same or different) to it, so receiver can read it. The conversion from plaintext to cipher text is called encryption and from cipher text to plaintext is called as decryption[13][20].



Cryptosystem is a pair of algorithm that takes a key and converts plain text to cipher text and back. Cryptosystem can be categorized as Symmetric cryptosystem and Asymmetric cryptosystem.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Symmetric cryptosystem uses a shared secret key in the encryption process as well as in decryption process .for example DES (Data Encryption Standard)[12][13][18][20], AES(Advance Encryption Standard) [8][18][20],Blowfish[1]. It has few limitations such as key distribution, compromised KDC (Key Distribution Center), random number generation, placement of encryption function.
Asymmetric cryptosystem uses public key for encryption and a private key for decryption, there is no need for a shared secrete [3][20]. Examples of this are Diffie-Hellman [14], RSA [7][12] and Elgamal [5].

All of the techniques used here are based on mathematical concepts of number theory and discrete logarithms. Particularly in number theory most important is integer factorization, modular arithmetic's. This paper introduces to the mathematical concepts of Quadratic residue, Fermat's little theorem, Euler's criterion and Legendre and Jacobi symbol. However it has been observed that Jacobi Symbol in case of some example fails to give correct result and therefore the limitation for predicting the quadratic residue.

II. FERMAT'S LITTLE THEOREM.

Fermat's little theorem works in two forms. First form is applicable to all but second form has limitation.

Form 1:-

It states that if p is prime number then for any integer a, the number $a^p - a$ is an integer multiple of p [6][7][9]. In the notation of modular arithmetic this is expressed as,

$$a^p \equiv a \ (mod\ p) \qquad (1)$$

Example (2.1) a=2 , p=7

$\boldsymbol{a^p - a} = 2^7 - 2$
$= 128\text{-}2$
$=126$
$=7*18$
↳ It is p

$\boldsymbol{a^p \equiv a\ (mod\ p)}$
$2^7 \bmod 7 \equiv 2\ (mod\ 7)$
$128 \bmod 7 \equiv 2\ (mod\ 7)$
$2 \equiv 2$
↳ Condition Satisfy

Form 2:-

If p does not divide a then $a^{p-1} - 1$ is an integer multiple of P, where p is prime number [6][7][9]. In the notation of modular arithmetic it is

$$a^{p-1} \equiv 1\ mod\ p \qquad (2)$$

Example (2.2) a=2 , p=7

$\boldsymbol{a^{p-1} - 1} = \boldsymbol{2^{7-1} - 1}$
$= 64\text{-}1$
$=63$
$=7*9$
↳ It is p

$\boldsymbol{a^{p-1} \equiv 1\ (mod\ p)}$
$2^{7-1} \bmod 7 \equiv 1\ (mod\ 7)$
$64 \bmod 7 \equiv 1\ (mod\ 7)$
$1 \equiv 1$
↳ Condition Satisfy

Example (2.3) a=10, p=2

Form 1
$\boldsymbol{a^p - a} = 10^2 - 10$

Form 2
$\boldsymbol{a^{p-1} - 1} = 10^{2-1} - 1$

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

= 90
=2*45
It is p

$a^p \equiv a \ (mod\ p)$
$10^2\ mod\ 2 \equiv 10\ (mod\ 2)$
$0 \equiv 0$
Condition Satisfy

=9
= Not Possible to represent 9 in multiples of 2.

In this example **a/p=10/2=5,**

a mod p=10 mod 2=0

i.e. **p** completely divides **a** so Form 2 cannot be used

III. QUADRATIC RESIDUE:

Let a ∈ N and p be an odd prime number such that gcd(p,a) = 1. Then **a** called a quadratic residue modulo **p** if **a** is a perfect square modulo **p**[4][6][9][13][15][16] i.e. there is a number **y** such that,

$y^2 \equiv a \bmod p$ (3)

and **a** is called a quadratic non residue modulo **p** if equation (1) has no solution (i.e there exist no perfect square)

Example (3.1): Let us find if 8 is quadratic residue modulo 17

First we find

8 mod 17 = 8

We have to find out y^2 such that

$y^2 \equiv 8 \bmod 17$

So, we will find square of all the numbers in z_{17} set and find each square modulo 17 then we find that

$5^2 \equiv 8 \bmod 17$

Here a=8 and p=17 and we conclude that **a** is quadratic residue modulo **p**.

Example (3.2): Let us find if 2 is quadratic residue modulo 5

First we find

2 mod 5 = 2

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

We have to find out $\mathbf{y^2}$ such that

$$\mathbf{y^2 \equiv 2 \bmod 5}$$

So, we find square of all the numbers in $\mathbf{z_5}$ set and find each square modulo 5,here we find that there is no such perfect square exist. Here a=2 and p=5 and we conclude that **a** is quadratic non residue modulo **p**.

Finding whether **a** is quadratic residue modulo **p** becomes a tedious task for large integers. It is therefore necessary that we first identify whether there exists such **y** which satisfies $\mathbf{y^2 \equiv a \bmod p}$

This can be achieved through Legendre and Jacobi symbol. However, we need to first understand Euler's criterion as discussed in next section.

IV. EULER'S CRITERION

Let P be an odd Prime and a be any positive integer then a is quadratic residue modulo p if and only if[6][9][13] ,

$$\boldsymbol{a^{(p-1)/2} \equiv 1 \ (mod\ p)} \quad (4)$$

a is quadratic non residue modulo **p** if,

$$\boldsymbol{a^{(p-1)/2} \equiv -1 \ (mod\ p)} \quad (5)$$

a is said to be a multiple of **p** is the congruence given below is satisfied

$$\boldsymbol{a^{(p-1)/2} \equiv 0 \ (mod\ p)} \quad (6)$$

Example(4.1):a=8 , p=17

$$\mathbf{8^{(17-1)/2}} \equiv 1 \ (mod\ 17)$$
$$8^{(8)} \equiv 1 \ (mod\ 17)$$
$$1 \equiv 1$$

So, We can say that **a** is quadratic residue modulo **p**.

Example(4.2):a=2 , p=5

$$\mathbf{2^{(5-1)/2} mod\ 5} \equiv -1 \ (mod\ 5)$$
$$2^{(2)}\ mod\ 5 \equiv -1 \ (mod\ 5)$$
$$4 \equiv 4$$

So, we can say that **a** is quadratic non residue modulo **p**.

Example(4.3) :a=21 , p=7

$$\mathbf{21^{(7-1)/2}} \equiv 0 \ (mod\ 7)$$
$$21^{(4)} \equiv 0 \ (mod\ 7)$$
$$0 \equiv 0$$

So, we can say that **a** is multiple of **p**.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

V. LEGENDRE SYMBOL.

Suppose p is an odd prime no for any integer a define the Legendre symbol $\frac{a}{p}$ [6][10][12][13][17]as follows

$$\left(\frac{a}{p}\right) = (a \mid p) \equiv \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases} \quad (7)$$

Example(5.1) :a=2 ,p=7

$\frac{a}{p} = \frac{2}{7} = \ a^{(p-1)/2} mod\ p$ ----------($a^{(p-1)/2} mod\ p \equiv 1\ mod\ p$)

$= 2^{(7-1)/2}\ mod\ 7$

$= \ 2^3 mod\ 7$

= 8 mod 7

=1

So we can say that **a** is quadratic residue modulo **p**.

Example(5.2) : a=6 ,p=7

$\frac{a}{p} = \frac{6}{7} = \ a^{(p-1)/2} mod\ p$ ----------($a^{(p-1)/2} mod\ p \equiv -1\ mod\ p$)

$= 6^{(7-1)/2}\ mod\ 7$

$= \ 6^3 mod\ 7$

= 216 mod 7

= 6

= -1 mod 7

So we can say that **a** is quadratic non residue modulo **p**.

VI. JACOBI SYMBOL.

It is generalization of Legendre symbol [6][10][11][13].suppose n is and odd positive integer , and the prime power factorization of n is ,

$$n = \prod_{i=1}^{k} {p_i}^{ei}$$

Let a be an integer the Jacobi symbol $\frac{a}{n}$ is defined to be

$$\frac{a}{n} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{ei}$$

Example(6.1) : $\left(\frac{9}{25}\right)$

$$\left(\frac{9}{25}\right) = \left(\frac{9}{5*5}\right) = \left(\frac{9}{5}\right)\left(\frac{9}{5}\right)$$

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Using Euler's Criterion for each term

$$\left(\frac{9}{5}\right) = \mathbf{9^{(5-1)/2} mod\ 5 = 1 = 1\ mod\ 5}$$

Putting these values in above equation we get,

$$= \left(\frac{9}{5}\right)\left(\frac{9}{5}\right)$$

$$= (1)(1)$$

$$= 1$$

Hence we can say that 9 is quadratic residue modulo 5.i.e $\mathbf{3^2 \equiv 9\ mod\ 2}$

Example(6.2) : $\left(\frac{6278}{9975}\right)$

First step is to find out prime factorization of $9975 = 3 * 5 * 5 * 7 * 19 = 3 * 5^2 * 7 * 19$

$$\left(\frac{6278}{9975}\right) = \left(\frac{6278}{3 * 5^2 * 7 * 19}\right) = \left(\frac{6278}{3}\right)\left(\frac{6278}{5}\right)^2\left(\frac{6278}{7}\right)\left(\frac{6278}{19}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right)^2\left(\frac{6}{7}\right)\left(\frac{8}{19}\right)$$

Using Euler's Criterion for each term

$\left(\frac{2}{3}\right) = 2^{(3-1)/2} mod\ 3 = 2 = -1\ mod\ 3$ ---------- hence it is -1

$\left(\frac{3}{5}\right) = 3^{(5-1)/2} mod\ 5 = 4 = -1\ mod\ 5$ ---------- hence it is -1

$\left(\frac{6}{7}\right) = 6^{(7-1)/2} mod\ 7 = 6 = -1\ mod\ 7$ ---------- hence it is -1

$\left(\frac{8}{19}\right) = 8^{(19-1)/2} mod\ 19 = 18 = -1\ mod\ 19$ ---------- hence it is -1

Putting these values in above equation we get,

$$= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right)^2\left(\frac{6}{7}\right)\left(\frac{8}{19}\right)$$

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

$$= -1$$

Hence we can say that 6278 is quadratic non residue modulo 9975.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Similarly we will check whether **5 is quadratic residue modulo 21 or not.**

Example(6.3) : $\left(\frac{5}{21}\right)$

First step is to find out prime factorization of 21=7*3

$$\left(\frac{5}{21}\right) = \left(\frac{5}{7*3}\right) = \left(\frac{5}{7}\right)\left(\frac{5}{3}\right)$$

Using Euler's Criterion for each term

$\left(\frac{5}{7}\right) = 5^{(7-1)/2} mod\ 7 = 6 = -1\ mod\ 7$ ---------- hence it is -1

$\left(\frac{5}{3}\right) = 5^{(3-1)/2} mod\ 3 = 2 = -1\ mod\ 3$ ---------- hence it is -1

Putting these values in above equation we get,

$$= (-1)(-1)$$
$$= 1$$

Hence by Legendre and Jacobi symbol we can say that 5 is quadratic residue modulo 21, But we does not get any perfect square modulo 21 which satisfies the congruence **y2 ≡ a mod p.**

VII. CONCLUSION

Cryptography has been built over the mathematical concept to construct hard problems to increase the efficiency of cryptographic algorithms. Quadratic residue is one such important concept used in cryptography. In this paper we have demonstrated how we can identify where an integer **a** is quadratic residue modulo **p** (p is prime) using Legendre and Jacobi symbol. Also with the help of example we have shown our observation that the results of Legendre Jacobi Symbol in some cases do not agree with the actual expected results of quadratic residuity.

REFERENCES

[1] Bruce Schneier,*"The Blowfish Encryption Algorithm",* Dr. Dobb's Journal of Software Tools, pp. 4, 38, 40, 98, 99, 1994.
[2] Chitra Desai," *A Novel Approach for Digital Signature Scheme Based on Solving Two Hard Problems"* IJCMSA: Vol. 6, No. 3-4, July-December 2012, pp. 95– 100.
[3] Chitra Desai, Manisha Patil, and Bharti Gawali,*"Review of Digital Signature Schemes, International Journal of Mathematics",* Computer Sciences and Information Technology, ISSN: 0974-5580 , Vol. 3, No. 2, pp. 387-402, (July-December 2010).
[4] Chris Monico, Michele Elia,*" Note on an Additive Characterization of Quadratic Residues Modulo p"*, January 27, 2006.
[5] ElGamal, T," *A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithm"*, IEEE Transaction Information Theory IT, 31: 469-472, 1985 http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C84/10.PDF .
[6] Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *"Disquisitiones Arithmeticae"* (Second, corrected edition), New York: Springer, ISBN 0-387-96254-9.
[7] James Robinson, Fermat's Little Theorem,*"Elaboration On History Of Fremat's Theorem And Implications Of Euler's Generalization By Means Of The Totient Theorem"*, copyright © James Robinson.
[8] Joan Daemen and Vincent Rijmen," *Rijndael for AES"*., AES Candidate Conference, pp. 343–348, 2000.
[9] Lindsay N. Childs *"A Concrete Introduction to Higher Algebra"*, ISBN: 978-0-387-98999-0 (Print) 978-1-4419-8702-0 (Online).

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

[10] Menezes, Alfred J; van Oorschot, Paul C.; Vanstone, Scott A. (2001),*"Handbook of AppliedCryptography"*,[Online] Available: http://www.cacr.math.uwaterloo.ca/hac/about/chap2.pdf.
[11] R. Crandall, C. Pomerance.*"Prime Numbers, A Computational Perspective*", New York: Springer, 2001
[12] Rivest, R., A. Shamir and L. Adleman,"*A Method for Obtaining Digital Signature and Publickey Cryptosystem Communications"*ACM. 21: 120-126. 1978 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.5588.
[13] Stinson, Douglas Robert (2006),"*Cryptography: Theory and Practice (3rd ed.)*", London: CRC Press.
[14] Whitfield Diffie and Martin E. Hellman,"*New Directions in Cryptography",* IEEE Transactions on Information Theory, 22(6):644-654, 1976.
[15] ftp://ftp.disi.unige.it/person/MoraF/MaterialeCTC/Quadratic.pdf
[16] *en.wikipedia.org/wiki/Quadratic residue*.
[17] David Angell(10/2012)" Evaluation of Certain Legendre Symbols", publishes by MAA (http://www.jstor.org/stable/10.4169/amer.math.monthly.119.08.690).
[18] G. JULIUS CAESAR and JOHN F. KENNEDY ," Cryptography". Security Engineering: A Guide to Building Dependable Distributed Systems.
[19] Ken Bogart, Scot Drysdale and Cliff Stein " Discrete Math for Computer Science Students".(http://www.cse.iitd.ernet.in/~bagchi/courses/discrete-book/fullbook.pdf)
[20] William Stallings , "Cryptography And Network Security: Principles And Practices, 4Th Ed.".

BIOGRAPHY

Dr. Chitra Ganesh Desai[1] is basically a science graduate and completed her Masters of Computer Application from Government Engineering College Aurangabad in 2000. She Qualified SET examination in 2004. She has been awarded with Ph.D (2006) in the subject of Computer Science with the study area in Software Reliability. She also completed M.Tech by research (Network Security) from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.

She has 27 international and 15 national publications in various journals and proceedings of conferences. She has completed minor research project in the area of GIS. Recently she has associated with Oceanography project supported by National Institute of Oceanography and INCOIS, Hyderabad. She has written two books in Databases and E-Commerce respectively bearing ISBN Number. She is a recognized guide from Pune University . Two students have been awarded Ph.D in Computer science under her guidance and five students are pursuing Ph.D. As a professional member she is associated with CSI, IEEE, Fellow IETE, ISTE. Dr. Chitra has total experience of 13 years in teaching. Her interest in administration inclined her to pursue MBA in Human Resource. Presently working as the Professor and Head of the Department of MCA at Marathwada Institute of Technology (Engineering), Aurangabad, has also coordinated several workshops in association with IIT Bombay, Under the National Mission for Education and ICT.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Ms.Rupali Bhakkad[2] is basically a science graduate and completed her Masters of Computer Application from Institute of Management studies and Information Technology Aurangabad in 2009. She is presently working as the Assistant Professor in the Department of MCA at Marathwada Institute of Technology (Engineering) from last four years. Her area of interest includes Operating System,Linux and Cryptography.

Miss.Sonal Sarnaik[3] is basically a Engineering graduate in Computer Science from Hi-Tech Institute of Technology, Aurangabad. She is presently working as the Assistant Professor in the Department of MCA at Marathwada Institute of Technology (Engineering) from last three years. Her area of interest includes Cryptography, Mobile Computing and Data Structure.