



International Journal of Management, IT & Engineering

(ISSN: 2249-0558)

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
<u>1</u>	Community Participation In Water Supply Schemes In Oke-Ogun Zone, Oyo State, NIGERIA. Toyobo Adigun Emmanuel, Tanimowo N. Bolanle and Muili A.B	<u>1-14</u>
<u>2</u>	The current situation, future prospect of Poverty and inequality in Sudan. Dr. Ali Musa Abaker and Dr. Ali Abd Elaziz Salih	<u>15-31</u>
<u>3</u>	Performance Evaluation of On-demand AODV and DSR Routing Protocols in Mobile Ad-hoc Network. Muhammad Ashraf, Ahsan Raza Sattar, Tasleem Mustafa, Muhammad Inam Shahzad and Ahmad Adnan	<u>32-57</u>
<u>4</u>	Enhancement of Security for Initial Network Entry of SS In IEEE 802.16e. Ahmad Adnan, Fahad Jan, Ahsan Raza Sattar, Muhammad Ashraf and Inaam Shehzad	<u>58-72</u>
<u>5</u>	The Role Social Capital Components on Entrepreneurship of Parsabad SMEs. Gholamreza Rahimi (Phd) and Ghader Vazifeh Damirch (MA)	<u>73-97</u>
<u>6</u>	Factors of default in Small and Medium Enterprise: an Application of Cluster Analysis. Subroto Chowdhury	<u>98-125</u>
<u>7</u>	Implementing Construction Projects on Schedule – A Real Challenge. Prof (Dr.) Debabrata Kar	<u>126-142</u>
<u>8</u>	A Study On Employee Stress Management In Selected Private Banks In Salem. Ms. A. Sharmila and Ms. J. Poornima	<u>143-161</u>
<u>9</u>	Elliptic Curve Cryptography With Secure Text Based Cryptosystem. Anju Gera, Dr. Ashutosh Dixit and Sonia Saini	<u>162-176</u>
<u>10</u>	Handling Of Synchronized Data Using JAVA/J2EE. Ankur Saxena	<u>177-194</u>
<u>11</u>	Forensic Tools Matrix: The Process of Computer Forensic for Digital Evidence Collection. Dr. Jigar Patel	<u>195-209</u>
<u>12</u>	Corporate Merger & Acquisition: A Strategic approach in Indian Banking Sector. Madhuri Gupta and Kavita Aggarwal	<u>210-235</u>
<u>13</u>	Loss Reduction in Radial Distribution Systems Using Plant Growth Simulation Algorithm. V. Raj kumar, B. Venkata Ramana and T.Ramesh Babu	<u>236-254</u>
<u>14</u>	Off Page Optimization Factors For Page Rank and Link Popularity. Dr. Yogesh Yadav	<u>255-268</u>
<u>15</u>	A Node Disjoint Multipath Routing Protocol in Mobile Ad Hoc Network. R.K. Kapoor, M.A. Rizvi, Sanjay Sharma and M.M. Malik	<u>269-285</u>
<u>16</u>	VLSI Implementation Of Systolic Array For Discrete Wavelet Transform. Prof. Sonali R.Tavlare and Prof. P. R. Deshmukh	<u>286-309</u>
<u>17</u>	HIGHER ORDER MUTATION TESTING (RESULT- EQUIVALENT MUTANTS). Shalini Kapoor and Rajat Kapoor	<u>310-327</u>

Chief Patron

Dr. JOSE G. VARGAS-HERNANDEZ

Member of the National System of Researchers, Mexico

Research professor at University Center of Economic and Managerial Sciences,

University of Guadalajara

Director of Mass Media at Ayuntamiento de Cd. Guzman

Ex. director of Centro de Capacitacion y Adiestramiento

Patron

Dr. Mohammad Reza Noruzi

PhD: Public Administration, Public Sector Policy Making Management,

Tarbiat Modarres University, Tehran, Iran

Faculty of Economics and Management, Tarbiat Modarres University, Tehran, Iran

Young Researchers' Club Member, Islamic Azad University, Bonab, Iran

Chief Advisors

Dr. NAGENDRA. S.

Senior Asst. Professor,

Department of MBA, Mangalore Institute of Technology and Engineering, Moodabidri

Dr. SUNIL KUMAR MISHRA

Associate Professor,

Dronacharya College of Engineering, Gurgaon, INDIA

Mr. GARRY TAN WEI HAN

Lecturer and Chairperson (Centre for Business and Management),

Department of Marketing, University Tunku Abdul Rahman, MALAYSIA

MS. R. KAVITHA

Assistant Professor,

Aloysius Institute of Management and Information, Mangalore, INDIA

Dr. A. JUSTIN DIRAVIAM

Assistant Professor,

Dept. of Computer Science and Engineering, Sardar Raja College of Engineering,

Alangulam Tirunelveli, TAMIL NADU, INDIA

Editorial Board

Dr. CRAIG E. REESE

Professor, School of Business, St. Thomas University, Miami Gardens

Dr. S. N. TAKALIKAR

Principal, St. Johns Institute of Engineering, PALGHAR (M.S.)

Dr. RAMPRATAP SINGH

Professor, Bangalore Institute of International Management, KARNATAKA

Dr. P. MALYADRI

Principal, Government Degree College, Osmania University, TANDUR

Dr. Y. LOKESWARA CHOUDARY

Asst. Professor Cum, SRM B-School, SRM University, CHENNAI

Prof. Dr. TEKI SURAYYA

Professor, Adikavi Nannaya University, ANDHRA PRADESH, INDIA

Dr. T. DULABABU

Principal, The Oxford College of Business Management, BANGALORE

Dr. A. ARUL LAWRENCE SELVAKUMAR

Professor, Adhiparasakthi Engineering College, MELMARAVATHUR, TN

Dr. S. D. SURYAWANSHI

Lecturer, College of Engineering Pune, SHIVAJINAGAR

Dr. S. KALIYAMOORTHY

Professor & Director, Alagappa Institute of Management, KARAIKUDI

Prof S. R. BADRINARAYAN

Sinhgad Institute for Management & Computer Applications, PUNE

Mr. GURSEL ILIPINAR

ESADE Business School, Department of Marketing, SPAIN

Mr. ZEESHAN AHMED

Software Research Eng, Department of Bioinformatics, GERMANY

Mr. SANJAY ASATI

Dept of ME, M. Patel Institute of Engg. & Tech., GONDIA(M.S.)

Mr. G. Y. KUDALE

N.M.D. College of Management and Research, GONDIA(M.S.)

Editorial Advisory Board

Dr. MANJIT DAS

Assistant Professor, Deptt. of Economics, M.C.College, ASSAM

Dr. ROLI PRADHAN

Maulana Azad National Institute of Technology, BHOPAL

Dr. N. KAVITHA

Assistant Professor, Department of Management, Mekelle University, ETHIOPIA

Prof C. M. MARAN

Assistant Professor (Senior), VIT Business School, TAMIL NADU

Dr. RAJIV KHOSLA

Associate Professor and Head, Chandigarh Business School, MOHALI

Dr. S. K. SINGH

Asst. Professor, R. D. Foundation Group of Institutions, MODINAGAR

Dr. (Mrs.) MANISHA N. PALIWAL

Associate Professor, Sinhgad Institute of Management, PUNE

Dr. (Mrs.) ARCHANA ARJUN GHATULE

Director, SPSPM, SKN Sinhgad Business School, MAHARASHTRA

Dr. NEELAM RANI DHANDA

Associate Professor, Department of Commerce, kuk, HARYANA

Dr. FARAH NAAZ GAURI

Associate Professor, Department of Commerce, Dr. Babasaheb Ambedkar Marathwada University, AURANGABAD

Prof. Dr. BADAR ALAM IQBAL

Associate Professor, Department of Commerce, Aligarh Muslim University, UP

Dr. CH. JAYASANKARAPRASAD

Assistant Professor, Dept. of Business Management, Krishna University, A. P., INDIA

Technical Advisors

Mr. Vishal Verma

Lecturer, Department of Computer Science, Ambala, INDIA

Mr. Ankit Jain

Department of Chemical Engineering, NIT Karnataka, Mangalore, INDIA

Associate Editors

Dr. SANJAY J. BHAYANI

Associate Professor, Department of Business Management, RAJKOT, INDIA

MOID UDDIN AHMAD

Assistant Professor, Jaipuria Institute of Management, NOIDA

Dr. SUNEEL ARORA

Assistant Professor, G D Goenka World Institute, Lancaster University, NEW DELHI

Mr. P. PRABHU

Assistant Professor, Alagappa University, KARAIKUDI

Mr. MANISH KUMAR

Assistant Professor, DBIT, Deptt. Of MBA, DEHRADUN

Mrs. BABITA VERMA

Assistant Professor, Bhilai Institute Of Technology, DURG

Ms. MONIKA BHATNAGAR

Assistant Professor, Technocrat Institute of Technology, BHOPAL

Ms. SUPRIYA RAHEJA

Assistant Professor, CSE Department of ITM University, GURGAON

Title

**ELLIPTIC CURVE CRYPTOGRAPHY WITH
SECURE TEXT BASED CRYPTOSYSTEM**

Author(s)

Anju Gera

*Computer Science &
Engineering*

*B.S.A. Institute of
Technology & Management*

Faridabad, India

Dr. Ashutosh Dixit

*Department of computer
Engineering*

*Y.M.C.A. University of
Science & Technology*

Faridabad, India

Sonia Saini

*Computer Science &
Engineering*

*B.S.A. Institute of
Technology & Management*

Faridabad, India

Abstract:

The paper discusses public key cryptography such as ECC, RSA and also gives mathematical explanations on the working of these algorithms. The paper also proposed an ECC algorithm for secure text based cryptosystem.

Keywords: Elliptic curve cryptography, RSA

1 INTRODUCTION:

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong [2, 4]. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement.

A Public key scheme has five ingredients.

- Plaintext: This is the message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
- Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption
- Cipher text: This is the scrambled message produced as output.
- Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the output.

Public-key cryptography is a cryptographic approach which involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The most widely used public key cryptosystem is RSA, ECC.

2 RSA:

RSA is one of the most popular and successful public key cryptography algorithms. The algorithm has been implemented in many commercial applications. It is named after its inventor's Ronald L. Rivest, Adi Shamir, and Leonard Adleman. They invented this algorithm in the year 1977. It is very simply to multiply numbers together, especially with computers. But it can be very difficult to factor numbers. It is based on the following idea [3].

- **Prime generation is easy:** It's easy to find a random prime number of a given size. Prime numbers of any size are very common, and it's easy to test whether a number is a prime.
- **Multiplication is easy:** Given p and q , it's easy to find their product, $n = pq$.
- **Factoring is hard:** Given such an n , it appears to be quite hard to recover the prime factors p and q .
- **Modular root extraction** the reverse of modular exponentiation is easy given the prime factors.
- **Modular root extraction** is otherwise hard.

2.1 RSA ALGORITHM

- Generate a pair of large, random primes p and q .
- Compute the modulus n as $n = pq$.
- Select an odd public exponent e between 3 and $n-1$ that is relatively prime to $p-1$ and $q-1$.
- Compute the private exponent d from e , p and q .
- Output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the e^{th} power modulo n :

$$c = \text{ENCRYPT}(m) = m^e \bmod n.$$

The decryption operation is exponentiation to the d^{th} power modulo n :

$$m = \text{DECRYPT}(c) = c^d \bmod n.$$

3 ELLIPTIC CURVE CRYPTOGRAPHY:

Elliptic Curve Cryptography (ECC) is a public key cryptography [8, 3]. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G , the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that $kP = Q$, where k is a scalar. Given P and Q , it is computationally infeasible to obtain k , if k is sufficiently large. k is the discrete logarithm of

Q to the base P. Hence the main operation involved in ECC is point multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

The basic EC operations are point addition and point doubling. Elliptic curve cryptographic primitives require scalar point multiplication

4 TEXT BASED CRYPTOGRAPHY USING ECC:

This paper describes the text based elliptic curve cryptosystem. The attractiveness of using elliptic curves arises from the fact that similar level of security can be achieved with considerably shorter keys. In text based cryptosystem first transforming the message into affine point on the elliptic curve (EC), over the finite field. In ECC we normally start with base points called $p(x, y)$ & message points which lies on the elliptic curve. This paper investigates the process of encryption/decryption of a text message, improves the algorithms for these operations with the goal of increasing the speed and decreasing the required memory. It also presents elliptic curves over finite fields. Use some addition & doubling equations for encrypt & decrypt the messages.

The typical Elliptic Curve is represented by

$$Y^2 \text{ mod } 23 = x^3 + x \text{ mod } 23$$

Points on the curve can be found as shown in Table 1

(0,0)	(0,0)	(16,8)	(16,15)
(1,5)	(1,18)	(17,10)	(17,13)
(9,5)	(9,18)	(18,10)	(18,13)
(11,10)	(11,13)	(19,1)	(19,22)
(13,5)	(13,18)	(20,4)	(20,19)

To do operations with EC points in order to encrypt and decrypt the points are to be generated first.

4.1 ECC OPERATIONS

To determine $2P$, P is doubled. This should be an affine point on EC. Use the following equation.

Equation for doubling

$$S = [(3Xp^2 + a)/2yp] \text{ mod } p$$

Then $2P$ has affine coordinates (XR, YR) given by:

$$XR = (S^2 - 2 Xp) \text{ mod } p$$

$$YR = [S (Xp - XR) - yp] \text{ mod } p$$

Now to determine $3P$, we use addition of points P and $2P$. Now the Equation is:

Equation for addition

$$S = [(YQ - yp) / (XQ - Xp)] \text{ mod } p$$

$$XR = (S - Xp - XQ) \text{ mod } p$$

$$YR = [(S (Xp - XR) - yp)] \text{ mod } p$$

The scalar point multiplication is the main operation in EC. Therefore we apply doubling and addition depending on a sequence of operations determined for 'l'. Every point (XR, YR) evaluated by doubling or addition is an affine point (points on the Elliptic Curve). The base point P is selected as $(0, 1)$. Base point implies that it has the smallest (x, y) co-ordinates which satisfy the EC. p is another affine point, which is picked out of a series of affine points evaluated for the given EC. In ECC we normally start with an affine point called $P(x, y)$. These points may be the Base point (G) itself or some other point closer to the Base point. Base point implies it has the smallest (x, y) co-ordinates, which satisfy the EC.

4.2 PROPOSED ALGORITHM FOR TEXT BASED ECC

```

Enter the string to be encrypted

//a ASCII value

//M message point

//Nm new message point

Calculate String length

Then calculate Nm=a*M

//Encryption

// P is the base point of EC

// ka is the private key

// l is random no

// kaP is public key of receiver

Cipher Text= {C1, C2}

Encryption C1=l*P & C2= (l*kaP+ Nm) to user A.

```

This subtraction is another ECC procedure involving doubling and addition. But the only difference is that the negative term will have its y co-ordinate preceded by a minus sign.

4.3 EXAMPLE OF PROPOSED WORK

Let the string be “Welcome”.

The first character whose ASCII value is calculated is ‘W’. The ASCII value of W=87.

Therefore

$$Nm = 87 * M$$

Where, M is the message point. Let it be (17, 13). Nm=New Message Point

So $NM = 87 * (17, 13)$;

Now Addition and doubling will be used to calculate this product.

The following values will be calculated:

$M = 17, 13$

Apply Doubling to find 2M

Apply Doubling to find 4M

Apply Addition to find 5M

Apply Doubling to find 10M

Apply Doubling to find 20M

Apply Addition to find 21M

The multiplication of the points is implemented by the repeated addition and doubling strategy of ECC technique.

All these steps will be covered in the Scalar Multiplication Function.

Now the New message point corresponding to Character 'W' is $Nm = 87M$.

This is stored in 1st position of array $Nm []$. Thus, $Nm [0] = 87M$.

Now, user B sends 2 coordinates: $C1 = 1 * P$ & $C2 = (Nm + I * \text{kap})$ to user A.

4.4 ADVANTAGES OF THE PROPOSED WORK

By this new approach, many benefits can be achieved which are summarized as:

- Security: The Proposed method provides the better security. The smaller key size makes possible much more compact implementations for a given level of security, which means faster cryptographic operations.

- Decreased memory space. with the help of algorithms convert the integer key to character value. Because character takes less space as compared to integer.

5 DISCUSSIONS & CONCLUSION:

In this paper, Text based Elliptic Curve Cryptosystem is presented. This investigates and improves the algorithms for these operations with the goal of increasing the speed and decreasing the required memory. In text based cryptography in which each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the EC, by using a starting point. Transformation of the plaintext ASCII value by using an affine point is one of the contributions of this work.

REFERENCES:

- N.Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, volA8, 1987, pp.203-209.
- M.Aydos, T.Yanik and C.K.Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor," IEE Proc Commun., Vol. 148, No.5, pp. 273-279, October 2001.
- Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.
- Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field," International journal of network security, VolA, No.1, PP.99-106, Jan. 2007.
- Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-385/sec1_final.pdf
- Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf
- N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computations, 48, 203-209 (1987) of Computation, vol. 77, no. 262, pp. 1075–1104, 2008.

- Anoop MS, “Elliptic curve Cryptography”, available at <http://security.ittoolbox.com/research/elliptic-curvecryptology>, 5 Jan 2007
- R.L. Rivest, A. Shamir, L.M. Adleman, A Method for obtaining digital signatures and public key cryptosystem, Communications of the ACM 21 (1978) 120–126.
- W. Diffie and M. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory, 22:644-654, 1976

