E - Commerce for Future & Trends

Volume 1, Issue 1
www.stmjournals.com

Plain Text Encryption and Decryption Time Comparison Using ECC

O. Srinivasa Rao[1]*, A. Charan[2], Sumit Rauniyar[1], Pujitha Sannapareddy[1], Indhira Mudrageda[1]

[1]UCE(A), JNTUK, Kakinada, India
[2]Software Engineer, Hyderabad, India

Abstract

The increased use of computer communication systems has increased risk of data theft. Cryptography is the most important aspect of communication, security and becoming an important building block for computer security. Elliptic curve cryptography is one of the most widely used public key algorithms for secure exchange of information. In this paper, the authors present time comparison of encryption and decryption using ECC for text messages.

Keywords: *Cryptography, elliptic curve cryptography (ECC), encryption, decryption*

****Author for Correspondence*** E-mail: osr_phd@yahoo.com

INTRODUCTION

Koblitz [1] and Miller [2], independently proposed the elliptic curve cryptosystem in 1985, which is becoming the choice for mobile communication. In 1991, Koblitz [1] suggested special family of elliptic curves, which are widely studied in the academia and have been included in certain standards [2–4].

Elliptic curve cipher use very small key size and computationally is very efficient. One can use an elliptic curve group that is smaller in size while maintaining the same level of security. The result is smaller key sizes, bandwidth savings, and faster implementations – features that are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, personal digital assistants, and wireless devices. Elliptic curve cryptographic protocols for digital signatures, public-key encryption, and key establishments have been standardized by numerous standards organizations including:

- American National Standards Institute (ANSI X9.62 [3], ANSI X9.63 [4])
- Institute of Electrical and Electronics Engineers (IEEE 1363-2000 [5])
- International Standards Organization (ISO/IEC 15946-3 [6])
- US government's National Institute for Standards and Technology (FIPS 186-2 [7])
- Internet Engineering Task Force (IETF PKIX [7], IETF OAKLEY [8])
- Standards for Efficient Cryptography Group (SECG [9])

The vast majority of products and standards that use public-key cryptography for encryption and digital signatures use RSA [10]. As we have seen, the bit length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. Recently, a competing system that has emerged is elliptic curve cryptosystem (ECC) [4, 11].

Elliptic Curve Cryptography

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves defined over Zp and binary curves constructed over GF (2 m). Fernandez [12] points out that prime curves are best suited for

© STM Journals 2014. All Rights Reserved

software applications, as the extended bit-fiddling operations needed by binary curves are not required; and that binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful and fast cryptosystem. In this paper, prime curves defined over Zp have been used for analysis purpose.

Mathematical Review

We consider an elliptic curve over prime fields which are of the form:

$E: y^2 = x^3 + ax + b \bmod p$ where $a, b \in Fp$ and $4a^3 + 27b^2 \neq 0 \bmod p$

The addition of two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ is calculated by:

$R(x_3, y_3) = P + Q$ where: $x_3 = \lambda^2 - x_1 - x_2$,

$y_3 = \lambda(x_1 - x_3) - y_1$,

$\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$

$\lambda = (3x_1^2 + a)/2y_1$ if $P = Q$

ECC Encryption (at Sender Side)

1. Take plain text X,
2. Each character of X, i.e., assigned as message Pm, can be converted into the point coordinate (Xm, Ym) on EC
3. Encryption/decryption system require a point on G and an elliptic group Ep(a, b). User A selects a private key nA and generates a public key PA = nA × G. To encrypt and send pixel Pm, to B, A chooses a random positive integer k and produces the cipher text Cm consisting of the pair of points:

Cm = {kG, Pm + kPB}, where PB is the public key of user B.

ECC Decryption (at the Receiver Side)

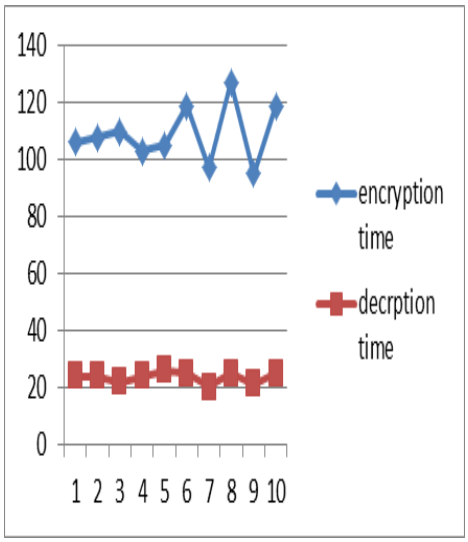
1. To decrypt the cipher pixel, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

Pm + kPB–nB(kG) = Pm + k(nBG)–nB(kG) = Pm

For practical purpose, the authors have taken an elliptic curve $E_{487}(1,1)$ in the prime field and the alpha-numerical characters are mapped [13, 14] to the points of the EC. The mapped points are encrypted [15, 16] and computed encryption time and for decryption time, from which the authors found that the encryption time is always more than decryption time irrespective of size input. The results are shown in Tables 1–3 and their graphical representation is shown in Graphs 1–3.

Table 1

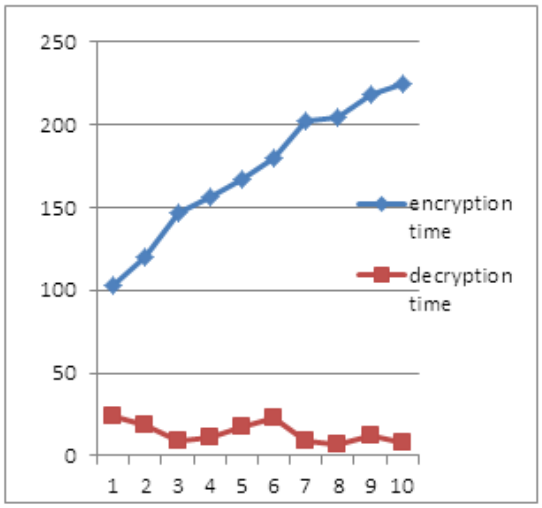
String	Encryption time (ms)	Decryption time (ms)
pqrs	106	24
ijkl	108	24
dczy	110	22
word	103	24
rock	105	26
salt	119	25
crow	97	20
duck	127	25
card	95	21
ugly	119	25



Graph 1

Table 2

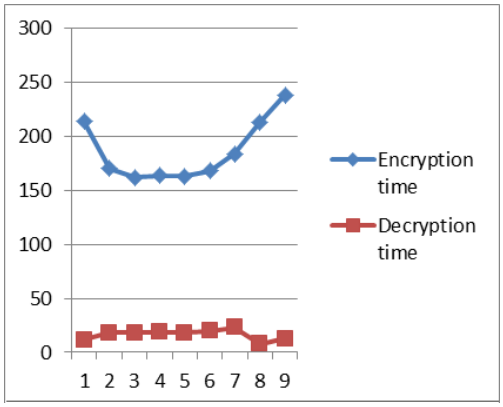
String	Encryption time (ms)	Decryption time (ms)
abcd	103	24
abcde	120	19
abcdef	147	9
abcdefg	156	11
abcdefgh	167	18
abcdefghi	180	23
abcdefghij	202	9
abcdefghijk	204	7
abcdefghijkl	218	12
abcdefghijklm	225	8



Graph 2

Table 3

String	Encryption time (ms)	Decryption time (ms)
cryptography	213.7	12
document	170.5	18
pendrive	162	18
graphics	163.5	19
harddisk	163	18.5
flowchart	168	20
jntucekkd	184	23
information	213	8
computemetwork	238.5	13



Graph 3

CONCLUSIONS

The authors developed GUI application using Java and the results are computed on Intel Core –i5 2410M, 2.3 Ghz , 3G B RAM, Windows-7 , 64-bit OS. From the results, it is concluded that the encryption time is always more than decryption time irrespective of size input

REFERENCES

1. Koblitz Neal. Elliptic curve cryptosystem. *Journal of Mathematics Computation*. Jan 1987; 48(177): 203–9p.
2. Miller V. Uses of elliptic curves in cryptography. *Advances in Cryptology-Crypto '85, Lecture Notes in Computer Science.* 218
3. Certicom Corp. *An Introduction to Information Security*. March 1997; 1.
4. ANSI X9.63. *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Protocols.* Ballot Version. May 2001.
5. Internet Engineering Task Force. *The OAKLEY Key Determination Protocol, IETF RFC 2412*. November 1998.
6. ISO/IEC 15946–3. *Information Technology–Security Techniques–Cryptographic Techniques Based on Elliptic Curves*, Part 3. Final Draft International Standard (FDIS). February 2001
7. National Institute of Standards and Technology. *Digital Signature Standard, FIPS Publication*. 2000; 186–2.
8. Jacobson M, Koblitz N, Silverman J, et al. Analysis of the xedni calculus attack. *Designs, Codes and Cryptography*. 20 (2000), 41–64 (1986), Springer-Verlag; 417–426p.
9. *Standards for Efficient Cryptography Group, SEC 1: Elliptic Curve Cryptography, version 1.0*. 2000. Available at http://www.secg.org
10. Rivest RL, Shamir A, Adleman LM. Method for Obtaining Digital Signatures and Public–key Cryptosystems. *Communications of the ACM*. February 1978; 21: 120–6p.
11. Arita S. Weil descent of elliptic curves over finite fields of characteristic three. Advances in Cryptology–Asiacrypt 2000. *Lecture Notes in Computer Science*. Springer-Verlag; 1976 (2000); 248–59p.
12. Fernandes A. Elliptic Curve Cryptography. *Dr. Dobb's Journal*. December 1999.

13. Srinivasa Rao O, Pallam Setty S. Efficient mapping methods of elliptic curve crypto systems. *International Journal of Engineering Science and Technology*. 2010; 2(8):3651–6p.
14. Vigila S, Muneeswaran K. Implementation of text based cryptosystem using elliptic curve cryptography. *Advanced Computing, 2009. ICAC 2009. First International Conference.* 13–15 Dec. 2009; 82–5p.
15. Gupta K, Silakari S, Gupta R, et al. An ethical way of image encryption using ECC. *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference.* 23–25 July 2009; 342–5p.
16. Rajaram Ramasamy R, Amutha Prabakar M, Indra Devi M, et al. Knapsack based ECC encryption and decryption. *International Journal of Network Security*. Nov. 2009; 9(3): 218–26p.