IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VIII (May-Jun. 2014), PP 31-35
www.iosrjournals.org

Prospective Utilization of Elliptic Curve Cryptography for Security: Authentication, Encryption and Decryption

Shabnoor Qureshi[1], Prof. Somesh Dewangan [2]
[1](Computer Science and Engineering, Disha Institute of Management And Technology, Raipur, India)
[2](Computer Science and Engineering, Disha Institute of Management And Technology, Raipur, India)

Abstract : *Public key cryptography is typically used in the field of mathematical, which consist of factors decomposition problem of huge numbers and discrete logarithm problem in finite field. For huge numbers in public key cryptography, factors decomposition problems RSA cryptography is generally used, but in the field of hardware and high-performance computing technology RSA has encountered some difficulties. To overcome such type of difficulties the elliptic curve discrete logarithm is introduced, which provides advantages, whose public key is short, network bandwidth is small and ability to defend against to attack is strong. This paper presents the design principles of elliptic curve public key cryptography, Authentication, Encryption and Decryption with shorter key of RSA.*

Keywords: *Elliptic curve, RSA key generation, Elliptic curve cryptography, Diffie-Hellman key exchange, Authentication, Encryption, Decryption.*

I. Introduction

"The new direction of cryptography" [3] is entitled by Diffie-Hellman, to began the research process on public key cryptography in 1976.Cryptography has been derived security measure. Keys can be transmitted once a secure channel exists and the security can be comprehensive to other channels of high bandwidth or slighter delay by encrypting the messages sent on them.

Factor decomposition problem of huge numbers and discrete logarithm problem in finite field is concerned in public key cryptography. In public key cryptography, RSA is based on factor decomposition problem. In certain incident, RSA 1024 bits are not extremely secure. 2048 bits will be used where high security is required. But the bandwidth is improved and the encryption efficiency decreases. To improve this situation, Victor Miller [4] and Neal Koblitz [5] introduce elliptic curve cryptography. Whose public key is short, network bandwidth is small and ability to defend against to attack is strong [6].

In this paper, RSA is used with the shorter key and combined it with the elliptic curve cryptography for obtaining more powerful result. Combination of elliptic curve cryptography and RSA is used for generating cipher text from plain text.

II. Implementation Of Elliptic Curve Cryptography

In cryptography, Miller and Koblitz introduced elliptic curves at the mid of 1980s, and Lenstra showed how to apply elliptic curves to factor integers. From that instance, elliptic curves have played a progressively more significant role in many cryptographic situations. It provides advantages, offer a level of security equivalent to traditional cryptosystems that use much larger key sizes. For example, elliptic curve systems use 313-bits which replaced the 4096-bits key size of certain conventional system. In hardware implementations, using much shorter numbers can signify a large savings.

A good elliptic curve E could be the graph of the equation

$$E: x^3 + ax + b, \text{ and denoted by } E_p(a, b)$$

Historical point: Elliptic curves are not ellipses. They received name from their relation to elliptic integrals such as

$$\int_{z_1}^{z_2} \frac{dx}{\sqrt{x^3 + ax + b}} \quad and \quad \int_{z_1}^{z_2} \frac{xdx}{\sqrt{x^3 + ax + b}}$$

That arises in the computation of the arc length of ellipses.

A. Addition operations in EC

The addition rules over the elliptic group E_p (a, b) are:

1. Let the points $P_1=(x_1, y_1)$ and be in $P_2=(x_2, y_2)$ the elliptic group E_p (a, b), and O is the point at infinity .

$P_1 + P_2 + P_3 = (x_3, y_3)$

$$X_3 = \lambda^2 - x_1 - x_2 \bmod p$$

$$Y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

$$\text{where slope } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

2. $P + 0 = 0 + P = P$

3. If $x_2 = x_1$ and $y_2 = y_1$ that is

$P_1=(x_1, y_1)$ and $P_2=(x_2, y_2) = (x_2, -y_1) = -P_1$,

Then $P_1+P_2 =0$

B. Multiplication in EC

The actual multiplication over a good elliptic curve group E p (a, b) is very similar to the modular exponentiation in RSA.

Let $P=(3,10) \in E_{23}(1,1)$. Then $2P=(x_3, y_3)$ is equal to:

$$2P = P + P = (x_1, y_1) + (x_1, y_1)$$

Since $P = Q$ and $x_2 = x_1$, the values of λ, x_3 and y_3 are given by:

$$\lambda = \frac{3x_1^2 + a}{2v.} \bmod p$$

C. Security of ECC

In elliptic curve cryptography, security could be the most attractive characteristic. RSA, DSA along with Diffie-Hellman key change algorithm are a lesser amount of computationally efficient seeing that compare to elliptic curve cryptosystems. Figure1 gives estimated comparable key sizes for ECC and RSA algorithm. From the figure1, ECC affords the identical security as RSA while using extensively smaller key sizes. At all levels of security, ECC has smaller public key sizes than both RSA and DSA/DH in figure1. For the reason of the smaller key size, ECC outperforms both equally RSA and DSA/DH for most usual operations even though offering similar amounts of security. The reason being ECC offers greater efficiency regarding computational overheads, key sizes and bandwidth. With implementations, these personal savings mean higher data transfer speeds, lower power ingestion. Throughout implementations, these personal savings mean higher data transfer speeds, lower power consumption. For efficient cryptosystem implementation ANSI (American national standard institute) and NIST (national Institute of standard and technology) are producing requirements and technology [13] [14].

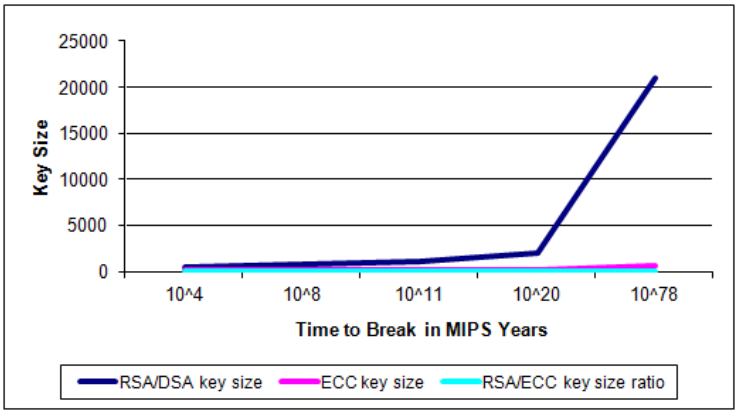

Figure 1. Key Size Strength (Suggested by NIST)

D. Implanted plaintext to points in EC

We are able to represent letters with the Roman alphabet by simply distinct points about the elliptic curve, once we have below:

N	1	2	3	4	5	6	7	8	9	10	…..
PM	(3,10)	(7,12)	(19,5)	(17,3)	(9,16)	(12,4)	(11,3)	(13,16)	(0,1)	(6,4)	…..
Letter	A	B	C	D	E	F	G	H	I	J	…..

In most cryptographic systems, we should have a opportunity for mapping our original message into a numerical value upon which we can accomplish mathematical operations. As a way to use elliptic curves, we need a way for mapping an message onto a point while on an elliptic curve. Elliptic curve cryptosystems after that use elliptic curve operations on that point to yield a fresh point that will assist as the cipher text.

The issue of encoding plaintext communications as points by using an elliptic curve isn't as simple as it was in the traditional case. In specific, there is not any known polynomial time period, deterministic algorithm for recording points on the arbitrary elliptic contour E (mod p). Nonetheless, there are fast probabilistic methods to finding points, and these may be used for encoding communications. These methods possess the property that along with small probability they will fail to make a point. By properly choosing parameters, this probability is usually made arbitrarily smaller, say on the order of $1/2^{30}$. Here is a single method, due to be able to Koblitz. The idea is the following. Let E: $y^2 = x^3 + ax + b$ (mod p) are the elliptic curve. The message m (already represented like a number) will be embedded in the x-coordinate of a point. However, the probability is about ½

Which $m^3 + m + b$ is often a square mod p. Therefore, we adjoin a few bits by the end of m in addition to adjust them until we receive a number x in ways that $x^3 + ax + b$ is often a square mod p.

More precisely, let K be considered a large integer to ensure a failure pace of $1/2^K$ is acceptable when wanting to encode a message as a point. Assume that m satisfies (m+1) K<p. The message m will be represented by a number x=mK+j, where $0 \leq j < k$. Intended for j=0, 1... K-1, compute $x^3 + ax + b$ and try to calculate the square root $x^3 + ax + b$ (mod p). If there is often a square root y, then we get P_m (x, y); otherwise, we increment j by one in addition to try again while using the new x. We do this again until either we discover a square root or j=K. If j ever equals K, then fail to map a message into a point. Since $x^3 + ax + b$ is often a square approximately half almost daily, we have of a $1/2^K$ potential for failure. In order to recover the message on the point P_m (x, y) we merely calculate m by

$$m=[x/K],$$

Where [x/K] denotes the highest integer less than or corresponding to x/K.

III. RSA Key Generation Algorithm

Public key cryptography is really a popular method providing with security, identification and authorization in such secure systems. Various observations just stated form the cornerstone for the RSA public-key cryptosystem that is invented at MIT with 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. A competent method for making the large random prime numbers is usually proposed that considerably reduces the complete time required for generating a key pair. The key generation process will be based upon selecting a proper public key from a few pre-defined public keys and computing this private key when using the Euclid's extended algorithm.

Public key in this cryptosystem includes the value n, which is known as the modulus, and also the value e, to create the public exponent. The private key includes the modulus n and also the value d, to create the private exponent.

An RSA public-key / private-key pair can be generated by the next steps:

1. Generate a set of large, random primes g and q.
2. Compute the modulus n as n = pq.
3. Select a peculiar public exponent e between 3 and n-1 that may be relatively prime to p-1 and q-1.
4. Compute the private exponent d coming from e, p along with q. (See underneath.)
5. Output (n, e) because the public key along with (n, d) because the private key.

IV. Diffie-Hellman Key Exchange Protocal

Whitfield Diffie and Martin Hellman discovered what exactly is now known as the Diffie-Hellman (DH) algorithm in 1976. It is a fantastic and ubiquitous algorithm present in many secure connectivity protocols online. In real-time, over an untrusted network, DH is a method for securely interchanging a shared magic formula between two parties. A shared secret is important between two parties who would possibly not have ever communicated previously, so that they can encrypt their communication.

With this discussion, use Alice and Bob, two of one of the most widely traveled Internet surfers in cyberspace, to show the DH essential exchange. The goal on this process is intended for Alice and Bob to be able to agree upon the shared secret that an eavesdropper will not be able to determine. This shared secret is needed by Alice and also Bob to independently generate keys for symmetric encryption algorithms that are to be used to encrypt the data stream between these. The "key" feature is that none the shared secret nor the encryption keys never travel over this network.

Step of Diffie-Hellman key exchange protocol:

(1) Sharing parameter: select a large prime number p (over 200 bits), and one generator.
(2) A selects a private key $x_A<p$, calculate key $y_A=\alpha^{x_A} \bmod p$, and make y_A open.
(3) B selects a private key $x_B<p$, calculate key $y_B=\alpha^{x_B} \bmod p$, and make y_B open
(4) Calculate sharing key: $K_{AB}=(\alpha^{x_B})^{x_A} \bmod p = y_A \bmod p$ (B calculation) = $y_B \bmod p$ (A calculation), K_{AB} can be used for symmetry encryption key.

V. Conclusion

Elliptic Curve Cryptography provides highest strength-per-key-bit regarding any known public-key method of first technology techniques like RSA. However, the fact that the elliptic curve cryptosystem implementation is really a lot more complicated as well as requires deeper numerical understanding.

In this particular paper, elliptic curve cryptography is joined with RSA, in this RSA is utilized with shorter key. For obtaining more powerful key and with the help of this key perform authentication, encryption as well as decryption.

Acknowledgements

I am very much thankful to Department involving Computer Science and Engineering, Disha Institute of Management And Technology to present me opportunity to work on cryptography process. I sincerely convey my gratitude to Mr. Somesh Dewangan involving Dept. of M. Tech Computer Science and Engineering, Disha Institute of Management And Technology for giving constant inspiration for this work. I am also thankful to Mrs. Preeti Tuli, Dept. involving Computer Science and Engineering, Disha Institute of Management And Technology for helping me directly and indirectly within this work.

References

[1] Bai Qing-hai, Zhang Wen-bo, Jiang Peng, Lu Xu1, "Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation" IEEE 2012
[2] Sonali Nimbhorkar, Dr.L.G.Malik, "Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement", International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 1, January 2013.
[3] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory 22(1976), no.6, 644-654.
[4] Miller V. "Use of Elliptic Curves in Cryptography". In Cryptology Springer-Verlag, 1986, 417-426.
[5] Koblitz N. "Elliptic Curve Cryptosystems". Mathematics of computation, 1987, 48(177):203-209.
[6] Zhang Xiu-ai. "Study of Elliptic Curve Cryptography. Communications Technology", 2009, 05,208-209,212.
[7] JIA Ying-Tao. "The research of implementation technology based on elliptic curve cryptosystem and public key cryptography". Master's degree paper, Xiamen University, China, 2007, 23-24.
[8] Julio López and Ricardo Dahab, "An Overview of Elliptic Curve Cryptography", Relatorio Tecnico IC-00-10, May 2000.
[9] M. Muni Babu, S. Mp. Qubeb, V. Sunil Babu, "A Comparative Study of Elliptic Curve Cryptography and RSA to Kerberos Authentication Protocol", International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009, Volume- 1, Issue-3, Jan.-2014.

[10] Kristin Lauter, Microsoft Corporation, "The Advantages of Elliptic Curve Cryptography for Wireless Security", IEEE, February 2004.
[11] Marisa W Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko, "Issues in Elliptic Curve Cryptography Implication", International Indonesia Journal, Vol. 1/No. 1, 2009.
[12] Certicom. Certicom ECC Challenge, 1997. Available at http://www.certicom.com.
[13] William stallings "cryptography and network security principles and practice" fifth edition , Pearson ,2011
[14] Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem", RSA Laboratories.
[15] Prasant Singh Yadav et al., "Implementation of RSA algorithm using Elliptic Curve Algorithm for security and performance enhancement," International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.
[16] Sami A. Nagar and Dr. Saad Alshamma, "Efficient Implementation of RSA Algorithm with MKE".
[17] David A. Carts, "A Review of the Diffie-Hellman Algorithm and its use in Secure Internet Protocols", SANS Institute, November 5, 2001.