Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 126 – 132

Procedia
Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Data Encryption and Authetication Using Public Key Approach

SRINIVASAN NAGARAJ[@] Dr.G.S.V.P.RAJU[#] V.SRINADTH*

[@] *Asst.Professor Dept.of CSE, GMR Inst.of.Technology, *Rajam. AP.*

. [#] *Professor , Dept, Of CS&ST ,Andhra University ,Vizag-03.*

Abstract

Today various numbers of diverse applications that include e- payments in secure commerce and payment applications to provide security for their communications and transactions by protecting passwords. Encryption is a fundamental tool for the protection of sensitive information. The purpose is to use encryption is privacy for preventing disclosure or confidentiality in during communications. In this paper, we proposed a new method which is based on the Euler's Totient theorem to produce a set of numbers that encrypt the data stream and then we used our proposed method using an ECC approach to generate the signature key which is added to encrypt data before transmission and decryption operation and a signature can verify at the receiver site.

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication
and Convergence (ICCC 2015)

Keywords:Random,x-Prime,d-PrivateKey,Q-Public Key,DS

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.161

1.INTRODUCTION

Overview of Public Key Cryptography:

Information security is a field of research which aims at defending information from malicious attackers as still allow legal users to manipulate data to all comers. It uses two keys, one is called Private Key and another one is called a Public key. The public key encrypt the message and sent to the recipient for decryption of the message using the private key.

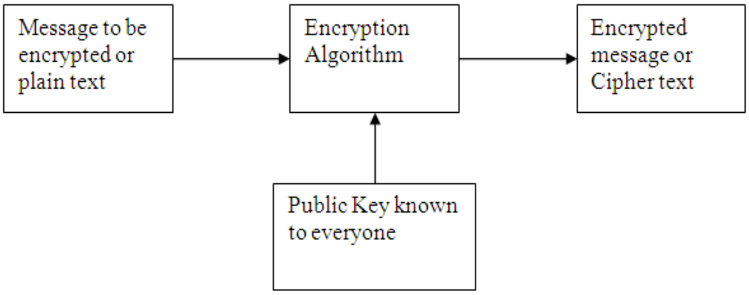

Message to be encrypted or plain text
Encryption Algorithm
Encrypted message or Cipher text
Public Key known to everyone

Fig .1 : The encryption process

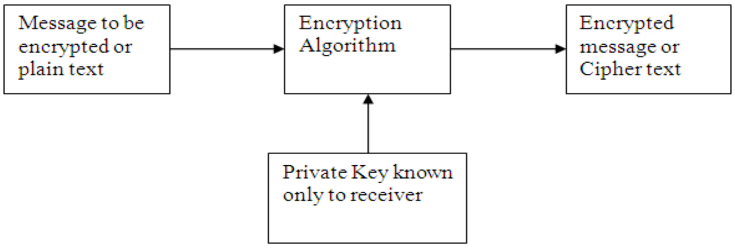

Message to be encrypted or plain text
Encryption Algorithm
Encrypted message or Cipher text
Private Key known only to receiver

Fig.2:The the decryption process

As compared to the shared key cryptography, the public key cryptography is rather slow. but, the public-key cryptography can be used with the shared key cryptography to get the best of both.

Applications for Public-Key Cryptosystems: Refer table shown below

Table 1. Applications for Public-Key Cryptosystems

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Y	Y	Y
Elliptic Curve	Y	Y	Y
Diffie-Hellman	N	N	Y
DSS	N	Y	N

*1.1 **Why Elliptic Curve Cryptography***

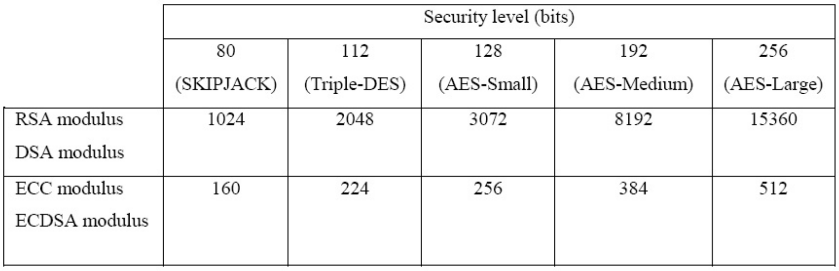
Now a days different technique is developed in cracking encryption algorithms which is the basis for common cryptographic systems includes Diffie-Hellman, RSA and DSA. Experts worried about it that in the next several years, RSA public key cryptography system could even potentially become obsolete. First, let’s take a look at the problem itself. Encryption algorithms ensure security by utilizing the assumption that certain mathematical operations are exponentially difficult, such as the problems of integer factorization and the discrete logarithm, to

prevent the decryption of public and private keys. As the key length increases, it becomes exponentially harder to decrypt.
It took after spent more than 30 years to show little progress, they have developed few faster algorithms for limited versions of the discrete logarithm problem, which has rung the alarm for the entire cryptographic community. It has made us realize that we need to implement a more secure standard is so called Elliptic Curve Cryptography .

Security : solving ECDLP takes more time than integer factorization and DLP when the same key sizes are used. This advantage allows ECC to achieve the same level of security with smaller key sizes and higher computational efficiency. If we use 1024-bit modulus for RSA and DSA, the security level becomes comparable to ECC with 160-bit modulus [GuPaWaEbSh, 2004].

Efficiency:
The parameter sizes, generally called the key sizes are listed in the table below
The listing has been done according to equivalent security levels for RSA, DSA and ECC as symmetric-key encryption schemes, stated in the table. The comparison shows that the elliptic curve cryptography algorithm uses smaller parameter sizes than RSA and DSA for the same security levels. According to the key size, the bandwidth requirements of ECC are said to provide greater efficiency than either integer factorization systems or discrete logarithm systems. This means that higher speeds, lower power consumptions and reduced code size are the advantages of ECC.

Table.1: RSA, DSA and ECC key sizes for equivalent security levels.



	Security level (bits)				
	80 (SKIPJACK)	112 (Triple-DES)	128 (AES-Small)	192 (AES-Medium)	256 (AES-Large)
RSA modulus DSA modulus	1024	2048	3072	8192	15360
ECC modulus ECDSA modulus	160	224	256	384	512

2. PROPOSED METHOD OF IMPLEMENTATION

Elliptic Curve Cryptography

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987)and Victor Miller (Miller 1986)independently proposed the public key cryptosystems using elliptic curve. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation.
The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem.

In the present paper for the purpose of the encryption and decryption using elliptic curves we consider the equation of the form

$$\mathbf{Y^2 = x^3+ax+b}$$

Elliptic Curve Domain Parameters are D = (q, FR, a, b, G, n)

- ***q***: prime power, that is $q = p$ or $q = 2^m$, where p is a prime
- ***FR***: field representation of the method used for representing field elements $\in F_q$
- ***a, b***: field elements, they specify the equation of the elliptic curve E over F_q,
  $y^2 = x^3 + ax + b$
- ***G***: A base point represented by $G= (x_g, y_g)$ on $E (F_q)$
- ***n***: Generated Prime number.

2.1 Sender Side : (Encryption And Ds Generation)

1. Read the n value.
2. Choose x=random(0,n-1), only prime will be selected.

(ENCRYPTION)

3. Apply y=Euler's Totient(x) to produce a set of numbers.
4. Read the data.

5. Select 'y' random characters from the given data.
6. Calculate the below function for each character
   ASCII value of character mod X
   Where, x is the prime number generated.
7. Sum up the results for all characters to generate a long int value.

8. Apply d=SHA(a,x). Where a = result from the above step.
   x = Random prime.

(PUBLIC KEY, PRIVATE KEY & DS generation)

9. Obtain public key Q=G*x
   G = domain of the EC.
   x = Random prime
10. With private key D, and public key Q already obtained,
    Perform, f = d * Public key
11. Use this 'f' in the Elliptic Curve
    Y^3 = x^2 +ax +b
    Where x= f
    a,b= are Curve constants.

12. Y can be obtained from the equation, through which a value of (x, y) can be extracted.
    Then the above value * x = Digital Signature.

    DS, Prime x, And public key is sent.

2.2 Recievers Side: (Decryption & Ds Validation)

1. Since (x,y) * prime = Digital signature,
   Using above equation point (x,y) is found out.
   If point (x, y) leads to the private key, then, the DS is VALID.
   Else is considered to be invalid, and DS validation fails!
   (DECRYPTION)

2. If validation is successful, the receiver would be having private key 'd', random prime 'x'

   So, by applying SHA^{-1}(a,x) using private key 'd', The data can be decrypted.

Example : SENDERS SIDE & DS GENERATION

1. Random prime x= 7
2. Euler Totient (7) = 6 (ENCRYPTION)
3. Reading data: Hai how are you?

4. 6 random characters extracted from the above data:

   H,a,y,u,o,i

5. 99 mod 7 + 69 mod 7 + 123 mod 7 + 117 mod 7 + 108 mod 7 + 100 mod 7 is computed
   A = 1344

6. SHA(a,x) = 42 = private Key

7. Public key = 7 * G =Q (DIGITAL SIGNATURE GENERATION)

8. F = 42 * Q

9. F = 10444

10. Applying $Y^3 = x^2 + ax + b$
    With x = f
    A,b = Curve Constants.
11. Point (x,y) = 42 is obtained.

12. When, 42 * x = Digital Signature.

<u>RECIEVERS SIDE (DECRYPTION & DS VALIDATION)</u>

1. (x,y) * 7 = D.S (DS VALIDATION)

   From the above Equation (x,y) is obtained.
   (x,y) = The private Key 42.

   DIGITAL SIGNATURE IS VALID.

2. Now, (DECRYPTION OF DATA)
   SHA^{-1} (A,X) = 42 is applied.
   And, the data is finally decrypted now.

3.RESULTS

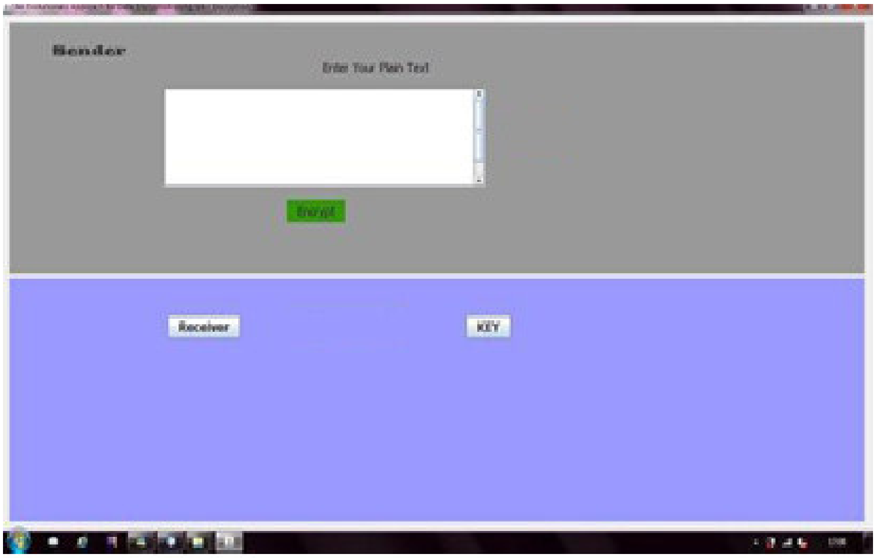
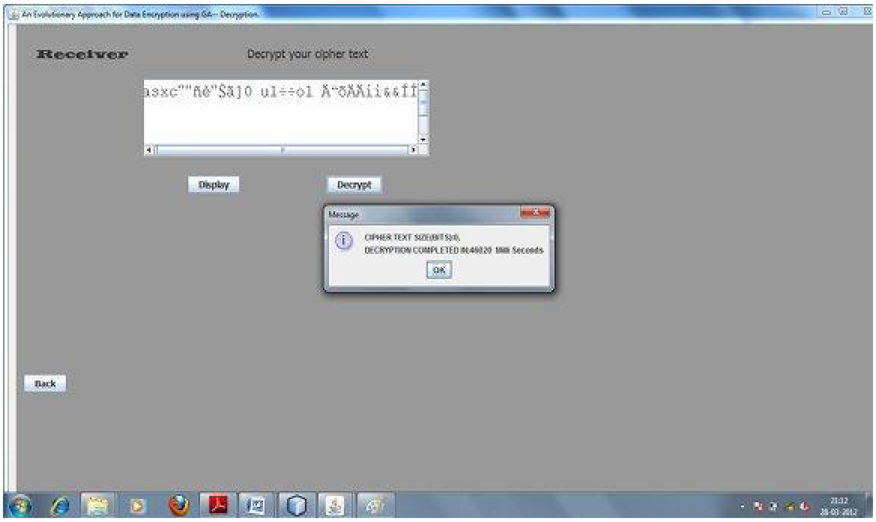


Fig:1 The Sender side home page screen

DECRYPTION:



asxc""ñé"$ãj0 ul÷÷ol Ã¨õÃÃiì&&íí

CIPHER TEXT SIZE(BITS)(0),
DECRYPTION COMPLETED IN:46020 1000 Seconds

Fig:2. Displaying Decrypted

4.CONCLUSION

Our proposed method is comparatively good performance at key generation and the confidential data is highly safe and reliable. The proposed algorithm increases the randomness of the used key. This method provides more security because of random key generation and it is economical to develop when compared to any other public key cryptographic algorithms. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. In future, it can o enhanced by making this method compatible to encrypt multimedia data which have to be transmitted securely over unsecured channels.

References

[1]. Stallings, W.: Cryptography and Network Security: Principles and Practices, 3rd edn. Pearson Education (2004)

[2]. A New Substitution Block CipherUsing Genetic Algorithm,Srinivasan Nagaraj1,D.S.V.P. Raju2, and Kishore Bhamidipati-SPRINGER,2013.

[3]. Koblitz, N.: A course in number theory and Cryptography. Springer-Verlag, New York,Inc. (1994)

[4] Anoop MS, "Public key Cryptography (Applications Algorithm and Mathematical Ex planations)"

[5] P.Ruangchaijatupon, P.Krishnamurthy, "Encryption and power consumption in wireless LANs-n," The Third IEEE workshop on wireless LANS, pp. 148-152, Newton,Massachusetts, sep. 27-28, 2001.

[6] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public- keycryptosystems"z. Communications of the ACM, Feb 1978.

[7].Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo random number genera tor. SIAM J. Compute 15(2), 364–383 (1986

[8]. Cryptanalytic Attacks on Pseudorandom Number Generators John Kelsey*Bruce Schneier* David Wagner *Chris Hally.*

[9] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common En cryption, Algorithms", International Arab Journal of e-technology, vol 2,no.1,January 2011.