IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Asymmetric based algorithm using LC - PRNG as basic primes for security corroboration

P.Kalpana[1], E.Prabha[2] and Mr. N. Karthikeyan[3]

[1]Department of ECE, UG Student, University College of Engineering, Ramanathapuram, Tamil Nadu, India

[2]Department of ECE, UG Student, University College of Engineering, Ramanathapuram, Tamil Nadu, India

[3]Department of ECE, Asst. Professor, University College of Engineering, Ramanathapuram, Tamil Nadu, India

Abstract

With the explosion of networks and huge amount of data transmitted along securing data content is becoming more and more important. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, accountability, authenticity, non repudiation. Many cryptographic symmetric and asymmetric algorithms are proposed. But symmetric key have some weakness such as suffering brute force, de-synchronization. To get rid of that weakness and reduce the system workload, we adopt Rivest Shamir Adleman (RSA) to construct an asymmetric key. Pseudo random numbers are used in a number of areas such as cryptography, scientific statistical simulation. In cryptography the pseudorandom number is a crucial element in the secret keys for cryptography algorithms and protocols. In this paper we have introduced new concept of RSA algorithm is based on PN (Prime Numbers). These PN are selected from PRN sequence. This technique is implemented by MATLAB.

Keywords–*RSA,PRNG,PRN,PR,LCG,BBSG,PN, AES.*

1.Introduction

The open system interconnection security architecture provides a systematic framework for defining security attacks, mechanism, and services. Security attacks are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of files, and denial of service.

Security mechanisms any process that is designed to detect, prevent, or recover from a security attack. Security services include authentication, access control, data confidentiality, data integrity, non repudiation and availability. The security services are achieved by using cryptographic algorithms[2].RSA (Rivest Shamir Adleman) algorithm is an asymmetric algorithm. In this algorithm, is performed by using the different keys (public key, private key) for encryption and decryption. Normal algorithms are symmetric algorithm (AES, DES, etc…) which is performed by using same key for encryption and decryption[12]. In RSA algorithm use of two keys has profound consequences in the areas of confidentiality, authenticity, integrity, accountability.

PRNG (Pseudo Random Number Generator) is a random number generator. PRNG produce endless strings of numbers which gives randomness and unpredictable. More security is achieved by using PRNG. PRN (Pseudo Random number) have been incorporated in a wide range of cryptographic and data security applications. Several methods are available in PRNG such as Primitive Root (PR), Linear congruential Generators (LCG), and BlumBlumShub Generator (BBSG). We have generated PRN sequence by using LCG. The PR sequence of numbers is as input to the RSA.

Security of the data is achieved by implementing the RSA algorithm using PRNG. This algorithm implementation is done by MATLAB.

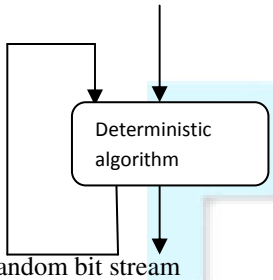
2. PRNG (Psuedo Random Number Generator)

An algorithm that is used to produce an open ended sequence of bits is referred to as a PRNG. A PRNG takes as input a fixed value called the seed. And produces a sequence of output bits using a deterministic algorithm. PRNG is used for a cryptographic application, and then a basic requirement is that an adversary who does not know the seed is unable to determine the PR string. PRNG requirements are randomness, unpredictable [1]. Randomness gives uniformity and scalability. Unpredictability means intruder cannot predict the random numbers[11]. Several methods are used to generate the PRN sequence. But the LC method is used here.

2.1. Linear Congruential method

We are generated the PRN using this method. Because LC has been subjected to more thorough testing than any other PRNG. It is frequently recommended for statistical and simulation work.

Seed



Psuedo random bit stream

Fig 1. Linearcongruentialgenerator (LCG)

Procedure for LCG

Choose four integers
Step 1: seed X_n– starting value.
Step2: modulus m-maximum possible value
Step 3: multiplier a-such that 2<a<m.
Step 4: increment c-between 0 and m.
Formula: Xn+1= (aX_n+c) mod m

3. RSA (Rivest Shamir Adleman)

One of the first successful respond to the challenge was developed by RON RIVEST, ADI SHAMIR and LEN ADLEMAN at MIT. The RSA algorithm has a key length of an above 1024 bits[4]. Most used key length is 512 bits. It is having the longer key length when compared to other algorithm[13]. So it has more security.

3.1 Cryptography types

- Symmetric key cryptography
- Asymmetric key cryptography

It is the ASYMMETRIC KEY cryptosystem. It used pair of keys. One is used for enciphering (encryption) and another one is used for deciphering (decryption).Plain text is the readable message or data that is fed into the algorithm as input. Cipher text is the scrambled message produced as output. It depends on the plain text and the key. For a given message, two different keys will produce two different cipher texts. Encryption algorithm performs various transformations on the plain text. Decryption algorithm accepts the cipher text and the matching key and produces the original plain text[3]. Public and private keysare a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption[10]. The exact transformation performed by the algorithm depends on the public or private key that is provided as input.

3.2Description of the algorithm

Encryption process: C=M^e mod n
Decryption process: M=C^d mod n

Both sender and receiver must know the value of ‘n’. Sender knows the value of e, and only the receiver knows the valued of‘d’. Thus, this is a public key encryption algorithm with a public key of PU= {e, n} and a private keyof PR= {d, n}[5]. For this algorithm to be satisfactory for public key encryption, the following requirement must be met.

- It is possible to find values of e,d, n such that M^e mod n=C for all M<n.
- It is relatively easy to calculate M^e mod n andC^d mod n for all values of M<n.
- It is infeasible to determine d given e and n.

The preceding relationship holds if ‘e’and‘d’ are multiplicative inverses modulo phi_n. Where phi_n is

the Euler totientfuction. The relationship between the 'e'and'd' can be expressed as
e*d mod phi_n= 1(1)
This is equivalent to saying
e*d = 1 modphi_n
d=e^(-1)mod phi_n (2)

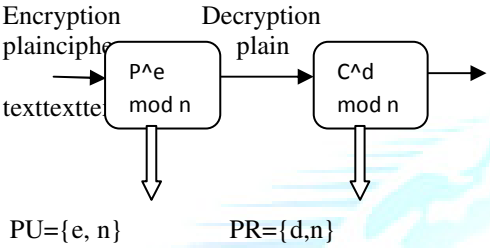


Fig 2. RSA encryption and decryption

a)Key generation
- Select p,q (p and q both prime,p!=q)
- Calculate n=p*q
- Calculate phi_n=(p-1)(q-1)
- Select integer e
- gcd(phi-n,e)=1;1<e<phi_n
- Calculate'd'. d=e^-1(mod phi_n)

Public key PU={e,n}
Private key PR={d,n}

b)Encryption
Plain text: M<n
Cipher text: C=M^e mod n

c)Decryption
Cipher text: C
Plain text: M=C^d mod n

4. Existing method

Symmetric types of algorithm with their advantages and disadvantages are given below.

4.1Substitution Techniques

A substitution technique is one which the letters of plaintext are replaced by other letters or by symbols[7].

1) Cease Cipher
It is the simplest algorithm. Ceaser cipher involves three places further down the alphabet.
Eg.plain: meet me after the toga party
Cipher: PHHE PH DIWHU WKH WRJD SDUWB
a)Disadvantages
- The encryption and decryption algorithms are known.
- There are only 25 keys to try.
- The language of the plain text is known and easily recognizable.

2) Play fair Cipher

The best known multi letter encryption cipher is the playfair, which treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams. The playfair algorithm is based on the use of a 5*5 matrix of letters constructed using a keyword[6].

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Step 1: In this case the keyword is monarchy.The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plain text is encrypted two letters at a time, according to the following rules:
Step 2: Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as 'ba lx lo on'.
Step 3: Two plain text letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
Step 4: Two plain text letters that fall in the same column are each replaced by the letter beneath, with the top element on the column circularly following the last[8].
Step 5: Otherwise, each plain text letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plain text letter.

4.2Transposition techniques

The simpler such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and the read off as a sequence of rows.
For example, to encipher the message "meet me the toga party" with a rail fence of depth 2, we write the following:
Plain: meet me the toga party
Cipher:MEMARTHTGPRAYETEFETEOAAT

4.3 AES (Advanced Data Encryption)

The cipher text takes a plaintext block of size 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes. The algorithm is referred to as AES-128, AES-192, or AES-256 depending on the key length. The input to the encryption and decryption algorithm is a single 128 bit lock. This block is depicted as a 4*4 square matrix of bytes[15].

1)AES structure

a) AES processes the entire data block as a single matrix during each round using substitution and permutation.
b) The key that is provided as input is expanded into an array of forty four 32 bit words. Four distinct words serve has a round key for each round.
c) Four different stages or used, one of the permutation and three of substitution:
   - Substitutes bytes
   - Shift rows
   - Mix columns
   - Add round key
d) For both encryption and decryption, the cipher begins with an add round key stage, followed by nine round that each includes all four stages, followed by a 10^{th} round of three stages.
e) Each stage is easily reversible. For the substitute type, shift rows and mix columns stages, an inverse function is used in the encryption algorithm. For the add round key stage, the inverse is achieved by XOR ing the same round key to the block.
f) As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This consequence of the particular structure of AES[14].
g) Once it is established that all four stages reversible, it is easy to verify that decryption does recover the plain text.
h) The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible.

2)Advantages

- The key length is very small.
- The same key is used for both encryption and decryption.

3)Disadvantages

- To generate different shared key. It generates the problem with managing and ensuring security.
- Origin and authenticity of message cannot be guaranteed.
- Opponent can be finding the shared key. The intruder can be easily finding the original message. And security can be easily broken by adversary.
- Secure key distribution is difficult.
- Some security services are difficult to implement.
- Cannot be used for Authentication service (Digital Signature).

5. Proposed method

5.1Asymmetric RSA algorithm using PRNG

A capability with application to a number of cryptographic functions is random or pseudorandom number generation. The principle requirement for this capability is that the generated number stream be unpredictable. First to generate the PRN sequence by using the LC method. For that first we choose the seed value. It is also one of the inputs of the random number generator[9]. And we choose the modulus m, multiplier a and increment c. Finally the PRNG generates the stream of numbers.

We select the perfect prime numbers from PRNG sequence. This prime numbers are given to the input of RSA algorithm. The mathematical concept of RSA

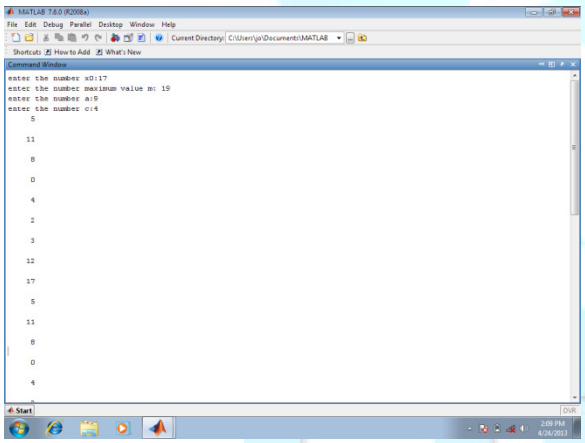
algorithm is already we have seen. So the plain text is converted into cipher text by using encryption process[11]. And cipher text is also converted into plain text by decryption process.

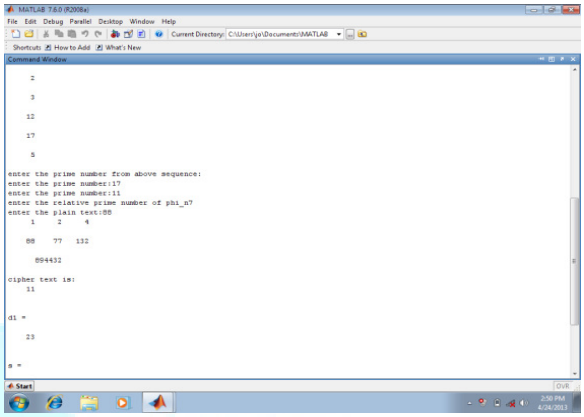
1)Advantages

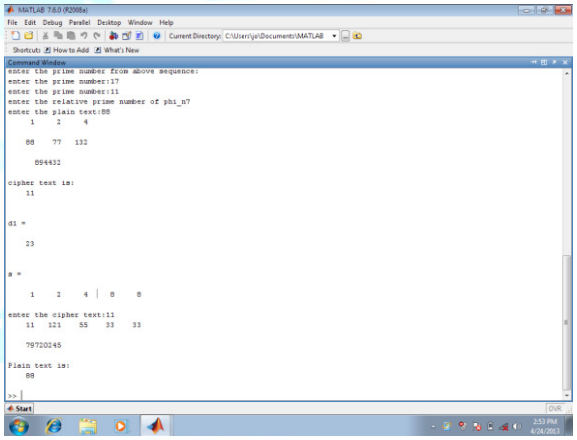
- Asymmetric has two keys. So it is very
- Convenience for transferring secret data.
- The intruder cannot be finding the private key. Because it's more securable and sensible. The private key does not share to anyone.
- The sender 'signs' a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message. It gives authenticity of the sender.

6. Simulation result

The sequence of PRN numbers are generated by MATLAB. And RSA algorithm also implemented by MATLAB.







7. Conclusions

In this paper, the RSA algorithm using PRNG sequence has been developed. The main advantage of the proposed technique is that they can provide more security to information. We conclude that from all of the cryptographic technique the proposed asymmetric algorithm has excellent integrity compared to other symmetric algorithm. RSA algorithm using PRNG was performed by MATLAB and corresponding output was obtained. In future, the RSA algorithm will also be compared with the existing and proposed algorithm.

References

[1] Bruce Schneier, Applied Cryptography – Protocols, Algorithms and Source Code in C, Second Edition, John Wiley and Sons, New York, 1996.

[2] Burnett S. and Paine S. McGraw-Hill. "RSA Security's OfficialGuide to Cryptography", 2001.

[3] Ching Chao Yang, dept. of Electron.Eng., "A new RSA cryptosystem hardware design based on Montgomery's algorithm", pp-908-913, IEEE 1998.

[4] Hang Qing, "The large prime numbers based on genetic algorithm", (ICISIE) pp-434-437, IEEE 2011.

[5] Haldir."The Reverse Engineering Team, How to crack a Linear Congruential Generator", December 2004.Available online at http://www.reteam.org/papers/ e59.pdf.

[6] Hinek. M.,"Cryptanalysis of RSA and Its Variants", 2010.

[7] M. K. Khan and J. S. Zhang "Investigation on pseudorandom properties of chaotic stream cipher",*Proc. IEEE*International Conference on Engineering of Intelligent Systems, 2006, pp. 1-5.

[8] Kumar. R, Dept. of Compute. Sci. and Eng, "An advanced secure (t, n) threshold proxy signature scheme based on RSA cryptosystem for known signers", pp 293-298, IEEE 2010.

[9] Mustak E. Yalcin, Johan A. K. Suykens and JoosVandewalle, "True Random Bit Generation From a Double-Scroll Attractor", IEEE Transactions on Circuits and Systems, Vol. 51, No.7, July 2004, pp 1395-1404.

[10] Park Stephen K. and Keith W. Miller, "Random Number Generators: Good ones are hard to find", Communications of the ACM, October1988, pp.1 192-201.

[11] Ren-Junn, H.Wang, Dept. of Computer.sci and Inf.En.g, "An efficient decryption method for RSA cryptosystem", pp-585-590, IEEE 2005.

[12] N. Ruggeri. The University of Chicago,"Principles of Pseudo-Random Number Generation in Cryptography, VIGRE Program", August 2006. Available online at http://www.math.uchicago.edu/~may/VIGRE/VIGRE2006/PAPERS/Ruggeri.pdf

[13] Sonal Sharma, RSA algorithm using modified subset sum cryptosystem, "computer and communication technology" (ICCCT), pp-457-461, IEEE 2011.

[14] International Cryptology Conference (CRYPTO), ser. Lecture Notes in Computer Science, vol. 3152, Santa Barbara, CA, Aug. 2004, pp. 123–139.

[15] National Institute of Standards and Technology (NIST), Secure Hash Standard, FIPS PUB 180-1, www.itl.nist.gov/fipspubs/fip180-1.htm.