IJCTA, 9(41) 2016, pp. 1289-1294 ISSN: 0974-5572

APPLICATION OF GENETIC ALGORITHM ON RSA ALGORITHM

Varsha Singh*, and Purushottam Sharma,**

Abstract: The RSA (Rivest-Shamir-Adleman), a public-key cryptographic technique known as asymmetric cryptography is said to be one of the best known technique. This approach can be made more efficient by the use of genetic algorithm. Genetic algorithm performs knowledgeable usage of random exploration in order to determine optimized result. Even if it's randomized exploration, genetic algorithm considers factual knowledge to obtain the result in the given area for optimized outcome. The paper high lights on how RSA algorithm be combined with genetic algorithm to provide with better performance.

Key Words: *Encryption, security, prime number, crossover, mutation.*

1. INTRODUCTION

Cryptography is an investigation of securing information data by changing it into mixed up arrangement called cipher text. It incorporates, for example, microdots, consolidating words with pictures and diverse methods for shroud data in transition and storage. Cryptography worries with four goals: secrecy, uprightness, Non- repudiation and verification.

Cryptography has different component like cipher text, plain text, encryption and decryption. Encryption calculations change the plain text to the cipher text; a decoding calculation changes cipher text to the plain text. In the Cryptography the encryption and decryption algorithm are public, the keys are private. The Cryptography is divided in two groups: Asymmetric-key and Symmetric-key. In the Symmetric key Cryptography the key is implemented for sender (Encryption) and the receiver (Decryption).The key is shared for both.

RSA is cryptography for the public-key encryption and is extensively uses for securing sensitive information data particularly while being sent over a slight framework for instance the internet or web. The RSA Cryptosystem is extensively used public-key Cryptography estimation as a major aspect of the framework which can be used for scramble the information without the exchange as private-key independently. The RSA computation could use for together public-key encryption and digital sign. The security depends on which trouble of considering extensive numbers.

In the cryptography the encryption-key is public and contrast from the decryption-key which is kept riddle. The RSA is a decently direct figuring and by virtue of this it is less normally used to clearly scramble the client data. The RSA algorithm incorporates four phases: Key-generation, Key-distribution, Encryption and Decryption.

* Amity University, Uttar Pradesh, Noida, India, 201313
varsha.singh502@gmail.com
** Amity University, Uttar Pradesh,Noida,India, 201313
psharma5@amity.edu

2. PROPOSED ALGORITHM

The RSA incorporates public-key and a private-key. Public-key can be known by everyone and used for scrambling messages. The objective is that information data encrypted by general public-key must be decrypted in the sensible measure of time using the private-key .The RSA is working on this pattern:-

‘n=qp’

Where q and p are two different Prime numbers

φ = (p-1)(q-1)

e < n where as gcd[e,φ]=1 d = (e-1)modφ

c = memod n where1<m<n. m = cdmod n

For the encryption c = me(mod n);

For the decryption cd = (me(mod n))d = m(mod n);

RSA is a the absolute most helpful tool for building cryptography-protocols. Algorithm which works on RSA are as:

Let PR is the set of prime numbers p and q such that

PR= {p1,q1,p2,q2,…..pn,qn}

Divide PR into subsets S={s1,s2,….Sn}such that each Si Contains a limited numbers of primes.

Each Si = {psi1,psi2, …..psin}

Select any two prime numbers from PR

Where n = p*q

Ø (n) = (p-1)*(q-1)

Assume public-key is ‘e’ and private-key is‘d’

Encryption, C = me(mod n)

Decryption, m = Cd(mod n)

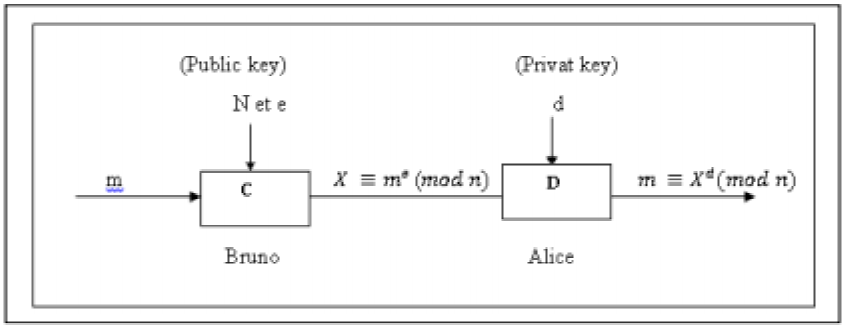

Fig1: Encyption and dycription algorith

If c = m then

Sender operation:

1. Choose d1 of the one of subsets Si in S for the secure class
2. Choose d2 inside Si to pick one alternative prime p'
3. Evaluate n’ = q'*p'
4. Evaluate Ø (n') = (q'-1)*(p'-1)
5. Choose alternative public key, lets e'
6. Generate the corresponding private key d’
7. Compute the cipher text C'=me’mod n'
8. Combine the agreement factor ‘f’ with the new cipher text and send C’ as:

C’ = [C’, f]

RSA is the absolute most helpful tool for building cryptographic protocols. In this type we decrease the excesses messages occurred in RSA strategy.

Genetic Algorithms are heuristic search procedures which are footed on Charles Darwin theory of hypothesis of the survival of the fittest. Genetic Algorithm (GA) is a classification of evolutionary algorithm [1]. The idea driving these calculations was to mirror the arbitrariness of nature. Thus, Genetic Algorithms (GAs) tries to take after nature as it were. GAs is an appropriate in situation where the issue space is huge and time take to inquire thorough as discussed [2]. GAs creates a populace in a manner that the trait which is popular, that has higher wellness esteem that repeated more, as done by the nature. This is likewise the major idea driving development. Along these lines, these calculations are additionally eluded to the developmental calculations. Genetic calculations endeavor to parallel the procedure of organic advancement to discover better arrangement so it is a well-known strategy for evading neighborhood optima in enhancing look The best single arrangement experienced so far will dependably be a piece of the populace, yet every era will likewise incorporate a range of different arrangements.

In a perfect world, all will be achievable, and some might be almost as great in the target work as the brute other may have very poor solution values. New arrangements are made by consolidating matches of people in the populace. Nearby optima are less successive in light of the fact that this consolidating handle does not focus completely on the best current arrangement.

Genetic Algorithm implemented with two types of the conceptive framework administrator-crossover and mutation.

Prempratap Singh et al. [5], gives another method for security that is internet-security with the help of GA and pseudorandom course of action, just to encode and unscramble the information data. Pictures on web or whatever other transmission medium can be secured by this method. Sindhuja K et al.[6]., gives a symmetric-key Cryptosystem with the assistance of GA, firstly plain text is changed in the form of matrix that is key-matrix and text-matrix, further additive matrix is produced by adding both the text and key-matrix. Dr. Dilbagh Singh et al. [7] verification that when an abnormal state of security is required, Asymmetric and Symmetric techniques does not work. For acquire an impeccable output inside smallest- time, Author proposed an estimation in which GA is combined with Cryptography what’s more, yield of that blend is a perfect course of action.

Aarti Soni, et al. [8] proposed another strategy in which a key is made by pseudorandom number generator and these self-assertive numbers will be produced with the help of current time of the PC structure. Nitin Kumar Rajendra et al.[9]., merges GA and BRAIN-MU – WAVES for the encryption of information data which finally gives better security, classification and uprightness of the information data set away in information data. Pseudorandom twofold progression is consolidated with the cerebrum mu waves for the encryption what's more unscrambling of information data.

For implementing the crossover operator their parents must be paired. There are a few distinct sorts of crossover operator however the sorts accessible rely on upon what representation is used for the individuals. For which the binary string individuals, One-point, Two-point, and consistent crossover function and mutation is applied. The fundamental point of mutation operator is to simulate the impact of error which can occur with low likelihood.

3. PROPOSED SYSTEM

In order to increase the efficiency of RSA, we are applying genetic algorithm at in generating prime numbers. Along with this we are making use of prime numbers of 'n' length. It is comparatively easy to disintegrate large number of prime numbers which decreases the security of the network this is the reason of using prime numbers of 'n' length increasing the efficiency and security of the network.

According to the proposed system, the pseudo code would be given as follow:

Step 1: Picking up two prime-numbers 'p' and 'q'.

Step 2: Calculating the data-value of 'n' as-

$n = (p*q)$

Step3: Converting the value of 'n' into binary form.

Step4: Key Generation Picking up another set of prime numbers 'r' and 's' and calculating the value of 't' as-

$t = (r*s)$; and converting it into binary form.

Step5: taking XOR of n and t then again converting the result into decimal form.

Step6: Determining the Fitness function and comparing it with XOR result.

Step7: If the value of XOR doesn't fulfill the fitness function then genetic algorithm is applied, which is carried out in the flow as:

1. Selection
2. Crossover
3. Mutation

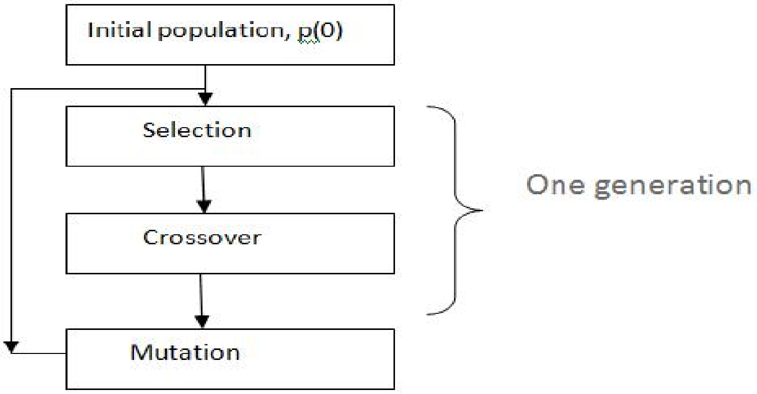

Fig.1 Flow chart of genetic algorithm

After mutation process, the result is XOR with the key and then again Fitness Function is checked, and same procedure is followed.

Step8: If the value of XOR fulfills the fitness function, algorithm is carried forward.

Step9: Totient (t) is calculated as (q-1)(p-1), variable 'e' is chosen on which the value of 'd' is evaluate as follow:

d*e = (1 mod t)

Step10: Once these values are computed, plain text (message) is converted into integer format. For example we have message 'ÝEAH' [3]

YEAH is converted into integer form as 25 5 1 8

Step11: Now message is encrypted by the formula C = Me(mod n)

And after encryption, encrypted message is forwarded to the receiver.

At the receiver site decryption is carried out with the formula of Cd(mod n)[4].After applying given formula the receiver is able to get the original message .In this way RSA can be used efficiently with more security thereby reducing the chances of vulnerable threats to the message during transmission along the network.

The flowchart of the proposed system is:

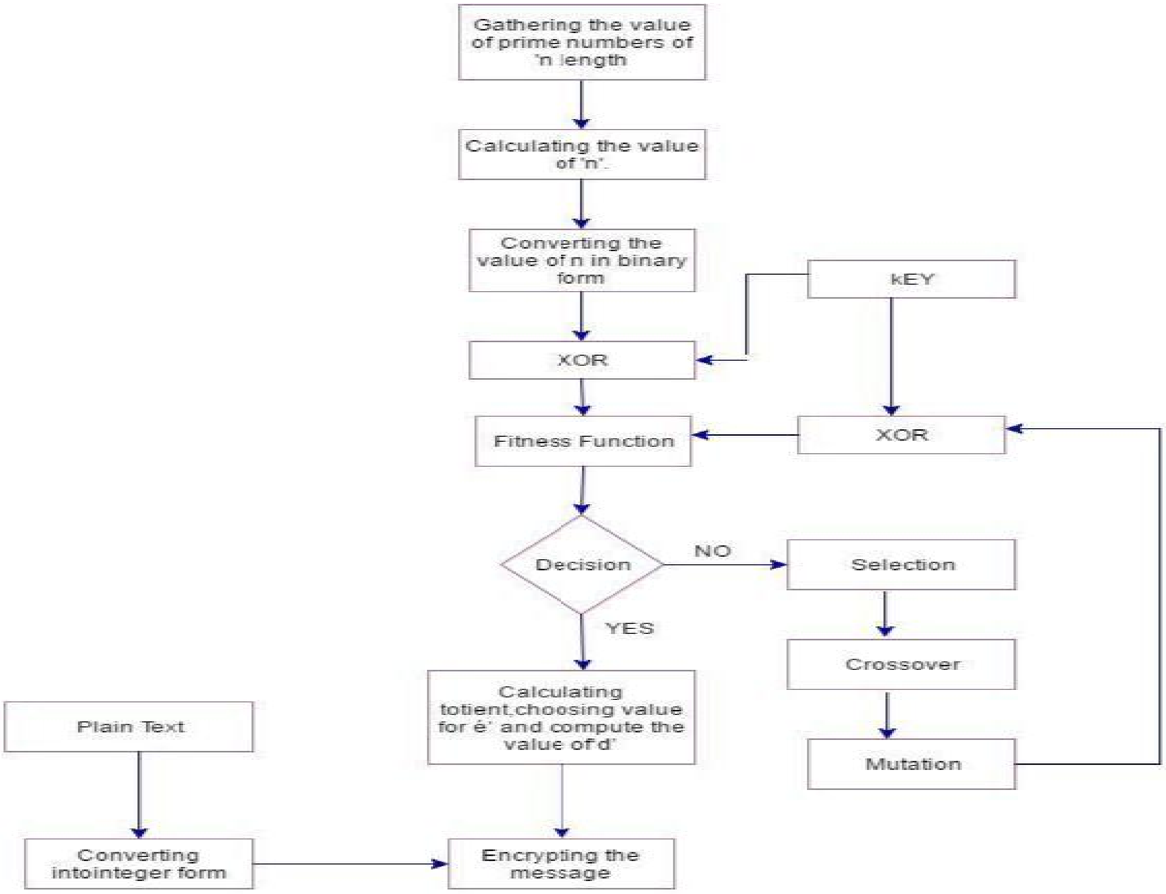
Gathering the value of prime numbers of 'n length
Calculating the value of 'n'.
Converting the value of n in binary form
kEY
XOR
Fitness Function
XOR
Decision
NO
Selection
YES
Crossover
Calculating totient,choosing value for é' and compute the value of'd'
Mutation
Plain Text
Converting intointeger form
Encrypting the message

Fig.2 Flow chart of the proposed system.

Our approach applied to new RSA algorithm: The first step in our research is to understand a different operations of RSA algorithm, study a factory problem, and how can we find p and q to cryptanalysis of RSA. This algorithm will help us to have a product of n = p*q two big number with k figures. Now and for the first time we work of how to apply genetic algorithm in cryptanalysis of RSA. For that we decide to use different operations of GA (coding, selection, crossover, mutation and replacement) to generate a new population with two individual p and q to use them in cryptanalysis of RSA.

CONCLUSION

Here in the paper we utilized prime number of 'n' length which is given the security over the systems. In which we tried to get the quality that make less demanding the cryptography to have a decent utilization of 'n' prime numbers. Along with this, using the concept of genetic algorithm makes our system optimized. This paper proposes another methodology for information security. It employments the idea of genetic algorithm I order to expand the complexity of key. In coming future we are planning to apply genetic algorithm at the receiver site i.e. during decryption.

References

[1] Goldberg D E(1989) Genetic algorithm in search optimization and a machine learning ,Addisson Wesley Publishing Co.

[2] Yang Shengxiang ,Cheng Hui and Wang Fang(2010),Genetic algorithm with immigrants and memory scheme for dynamic shortest path routing problem in mobile AdHoc network ,IEEE Transaction on the system ,man and cybernetics and application and review vol 40 ,no1.

[3] ApplicationRSAcryptography,http://www.andreashoalmstrom.org/teaching/sma205/lecturenotes/ s ma205 pages 59to65.pdf.

[4] Don:RSAEncryptionExplainedsimplyhttp://www.pagedon.com/rsaexplainedsimply/my_progra m ming/,(2010).

[5] P.Singh, G. Gosawi, S. Dubey 4 (2014). "GA: A technique for cryptography real time data transmission"at binary journal of data miming and networking 37-40.

[6] Sindhuja K, P. Devi2014,414-416.,"A symmetric key-encryption technique using GA" at IJCSIT, volume 5(1).

[7] Dr. D. Singh,P.Rani, Dr. R. Kumar2013.," To design a GA for cryptography to enhance the security" at issue 2April 2013.

[8] A.Soni, S.Aggarawal2012.,"Using GA for symmetric key generation in image encryption" at IJARCET 2012.

[9] N. Rajendra, B. Rajneesh Kaur2011.,"A new approach for data encryption using GA and brain mu waves" at IJSER 2011.

[10] Purushottam, ., Saxena, K., & Sharma, R. (2016). Modular Approach for Heart Disease Prediction. Indian Journal Of Science And Technology, 9(45). doi:10.17485/ijst/2016/v9i45/106367