International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 585-588 www.ijaem.net ISSN: 2395-5252

Implementing Modified Rsa Algorithm Using Multiple Keys with Extended Euclidean Algorithm

S. Om Prakash[1] N. Lalitha Mounica[1], S. Tarun Teja Reddy[2], V. V. N Shreyas[3],V. Ravi Teja[4]
Department of computer science and engineering[1234]
Raghu Institute Of Technology(A), Visakhapatnam, Andhra Pradesh, India

Submitted: 01-06-2022 Revised: 05-06-2022 Accepted: 08-06-2022

ABSTRACT
In the present situation there is a drastic change in the internet world. Sensitive information can be shared through internet, but this information sharing is susceptible to certain attacks. To resolve this issue Cryptography was introduced. Cryptography is an art and the science of creating secret code. Substitution and transposition are the two technique used for encoding and decoding the text. It is easy to find when we will use these techniques individually. This can be overcome by combining these two techniques. So, in this project Caesar cipher from substitution and the keyed transposition and the columnar technique from transposition is used. By combining these two techniques the fundamental weakness can be overcome and the cipher text become very hard to track.

I. INTRODUCTION :

The art of secret writing is known as cryptography. Cryptography has an ability to send the data between the participants in such a way that it prevents others from reading it. Cryptography is an art of performing an action on the data in an unintelligible manner.

The original form of the message is called as plain text or clear text. The data which comes out after performing some action is called as ciphertext. The process of producing cipher text from plain text is known as encryption. The process of producing plain text from cipher text is known as decryption.

The cryptographic systems contain both algorithm and a secret value. The secret value which is obtained is called as key. This key is used in this algorithm mainly to grasp the data such that it is difficult to explain when a new devised algorithm to the person with whom we would like to start our communication.

Single key is used in secret key cryptography .The message which is sent i.e. the plain text during encryption process it produces a data called as cipher text. The same key is used for the process of decryption.Secret key cryptography is called as symmetric cryptography and public key cryptography is called as asymmetric cryptography.

II. LITERATURE SURVEY

Intheliterature survey, we provide a briefsummary of the different methods that havebeen proposed for clustering over the periodof2013and2019.Wehavebeenthroughseveralpaperseachof which has a uniqueapproachtowardssegmentationinsomeparameterortheother.Thesummariesofeachofthepapersareprovidedbelow.

we have done an efficient implementation of RSA algorithm using two public key pairs and using some mathematical logic rather than sending the e value directly as a public key. Because if an attacker has opportunity of getting the e value they can directly find d value and decrypt the message[1].

Internet of Things (IoT) is a challenging and promising system concept and requires new types of architectures and protocols compared to traditional networks. Security is an extremely critical issue for IoT that needs to be addressed efficiently. Heterogeneity being an inherent characteristic of IoT gives rise to many security issues that need to be addressed from the perspective of new architectures such as software defined networking, cryptographic algorithms, federated cloud and edge computing[2].

we propose a new approach for encryption that is based on RSA main algorithm while using more encryption keys with smaller sizes in addition

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 585-588 www.ijaem.net ISSN: 2395-5252

to extra security information component (known as the Security Card, SeCa). Our results show that the use of multiple-shorter keys with the SeCa component produces significant improvements in the performance of RSA algorithm in terms of increasing security and reducing the computation overhead by decreasing encryption and decryption times[3].

This research paper aims to endeavours modified method of RSA algorithm so the more secure RSA algorithm can be developed. RSA algorithm provides the security service to every user who is connected through the network. Many cryptographic algorithms are used to exchange the information over network. RSA cryptosystem algorithm is widely used cryptographic algorithm in network security but it has problem of integer's factorisation for small numbers. Researchers have proposed many modifications to improve the security of traditional RSA. In this research various modifications are presented and compared to figure out new approaches of RSA cryptosystem, which try to improve the security and speed up the time of key generation encryption and decryption process[4].

This paper proposed an enhanced and modified approach of RSA cryptosystem based on "n" distinct prime number. This existence of "n" prime number increases the difficulty of the factoring of the variable "N" which increases the complexity of the algorithm. In this approach, two different public key and private key Page | 11 generated from the large factor of the variable "N" and perform a double encryptiondecryption operation which affords more security. Experiment on a set of a random number provided that the key generation time, analysis of variable "N", encryption and decryption will take a long time compared to traditional RSA. Thus, this approach is more efficient, highly secured and not easily breakable[5].

III. METHODOLOGY

In an organization several computers are connected in network. This network may connect to the internet. So, the message transmissions. This is the criteria of providing network security. The authorisation of access to the data can be done by network security by choosing the user name, password or any other authenticating data that will allow the user to access their own data and their programs within their authority. This security covers both public and private networks.This can be done by simply protecting the network by assigning a unique name and a unique password.

If the attacker wants to attack a particular network then if in case it is not been encrypted then the will be lost but if the actual network is already encrypted by cryptography then the data will not be lost. So that the attackers cannot attack our network and cannot read our messages. The main goal of cryptography is to ensure security and authentication to the networks by not allowing the hackers to steal our personal data. Network security is widely used in organisations, enterprises, institutions, etc. security is directly related todependability and this includes availability, reliability, maintainability, confidentiality, and integrity.

3.1 Existing techniques :

The RSA cryptosystem is invented by R. Rivest, A. Shamir, and L. Adleman, is widely most used public key Cryptosystem. RSA algorithm is the first algorithm suitable for encryption and decryption; The RSA algorithm used the multiplication modular and exponentiation. The algorithm of RSA is a cipher block which the plaintext and cipher text are integers between 0 and n-1 for some n. this algorithm is one of the best cryptosystem known asymmetric key for exchange key or digital signatures or encryption block of data, which uses prime numbers.The two techniques used in RSA cryptographic system are substitution technique and transposition technique.

IV. IMPLEMENTATION

4.1 Substitutiontechnique:

It is the encryption model where the characters in the initial stage are replaced by other characters or numbers or by symbols. When we take a string of bits this technique will restore the bit pattern of plain text with respect to bit pattern of cipher text. Some of the substitution ciphers are

- Monoalphabetic cipher
- Polyalphabetic cipher
- One - time pad
- Caesar cipher
- Playfair cipher

4.2 Transposition technique:

It is the cryptographic algorithm where the order of letters will be rearranged to form a cipher text. The process of converting the mapped plain text into cipher text using transposition technique is known transposition cipher.Some of the transposition cipher are

- Rail fence transposition
- Columnar transposition
- Improved columnar transposition
- Book Cipher/Running Key Cipher

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 585-588 www.ijaem.net ISSN: 2395-5252

4.3 Key generation :

1) Obtain two large numbers prime p and q of relatively same size such that their product n = pq is required bit length for example 1024.
2) Compute n = pq and φ(n) = (p − 1)(q − 1).
3) Choose a random integer encryption such that gcd[e, φ(n)] = 1 and 1 < e < φ(n).
4) Compute the exponent secret d in the range 1 < d < φ such that: ed = 1 mod φ(n).
5) The public key is (e, n) and the private key is (d, n).
The private values are d, p, q and φ.
1) Here, n refers to multiplication of the prime numbers.
2) Here, e refers to exponent public.
3) Here, d refers to exponent private.

4.4. Encryption :

Encryption is the process in which the data is converted into secret code which will hide the data's through meaning. In computer language, unencrypted data is termed as plain text or clear text and the encrypted data is turned as cipher text.
There are two types of encryption

- Symmetric encryption
- Asymmetric encryption

4.4.1. RSA Encryption :

- RSA encryption process is done by the sender.
- The sender will determine the public key.
- The plain text is encrypted and represented as an integer positive.
- Sender will calculate the cipher text by using the formula C = Me mod (n).
- Now, the text is received as cipher text by the receiver.

4.5. Decryption :

The conversion of cipher text to plain text is termed as Decryption. This is generally known as reverse process of encryption. This only uses a secret key to decrypt the data so only the author can access it.

4.5.1. RSA Decryption :

- RSA decryption process is done by the receiver.
- The receiver uses the private keys (n, d) to perform computation on plain text M = C d mod (n).
- Now the receiver will extract the clear text from the message representating M.

V. OBJECTIVE OF THIS PAPER :

The Objective of this Paper Enhancement the performance of RSA and increase the security and evaluated the security according to Randomness testing (using NIST statistical tests) has developed a package of 15 statistical tests to assure the randomness of a cryptography algorithm, The NIST Test Suite is developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence, the 15 tests are:

1) The Frequency (Mon obit) test
2) Frequency test within a block
3) The Run test
4) Tests for the longest-Run-of-ones in a block
5) The Binary matrix rank test
6) The Discrete Fourier transform test
7) The Non-overlapping template matrix centre
8) The Overlapping template matching test
9) Maurer's "Universal statistical" test;
10) The Linear complexity test
11) The Serial test
12) The Approximate entropy test
13) The cumulative sums test
14) The Random excursions test
15) The Random excursions variant test

VI. CONCLUSION AND FUTURE WORK:

The proposed system uses a combination of transposition and substitution techniques hence it will provide better security for text. However, the used algorithms can be improved to get better results. This modified RSA algorithm has increased its performance by ensuring more security than the old RSA algorithm . Security provided by this algorithm can be enhanced further by using it with one or more different encryption techniques so that the drawbacks of the existing system are overcome in the modified RSA algorithm.

REFERENCES :

[1]. Ayele, A. A., &Sreenivasarao, V. " has proposed a modified RSA encryption technique based on multiple keys .International journal of Innovative research in Computer Communication Engineering vol 1, 2013.
[2]. Hussain, A. K . "has proposed a Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm". IJISETInternational Journal of Innovative Science, Engineering & Technology, vol. 2, 2015.
[3]. Hassan, A. K. S., Shalash, A. F., &Saudy, N. F. " has proposed MODIFICATIONS ON

RSA CRYPTOSYSTEM USING GENETIC OPTIMIZATION". International Journal of Research and Reviews in Applied Sciences, vol. 19, 2014.

[4]. Dhakar, R. S., Gupta, A. K., & Sharma, P." has proposed a Modified RSA encryption algorithm (MREA)". Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.

[5]. Patidar, R., & Bhartiya, R." has proposed a Modified RSA cryptosystem based on offline storage and prime number". In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference, IEEE, 2013.