ISSN:0975-9646

Modified RSA Algorithm for (Wi-Fi) Security Protocol

T.Venkata Satya Vivek, D.Anandam , Ganta Anil,B.Sreenivasulu, V.Lakshma Reddy, M Rao Batchnaboyina

Computer Science And Engineering, PACE Institute of Technology & Sciences,Ongole, India.

***Abstract*— To secure data or information by a modified RSA cryptosystem based on 'n' prime. This is a new technique to provide maximum security for data over the network. It involves encryption, decryption, and key generation. Prime number used in a modified RSA cryptosystem to provide security over the networks. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this Research Paper we introduced the security in Wi-Fi technology. Also we presented solutions for some of these security vulnerabilities. The solution is based on Random number generation process & several encryption & decryption Algorithm.**

***Keywords*— Wi-Fi, Random Number Generation, Key Generation, Modified RSA Algorithm.**

I. INTRODUCTION

Wi-Fi is a set of product compatibility Standards for Wireless Local Area Networks (WLAN) based on IEEE 802.11. Wi-Fi is intended to be used for mobile devices and LANs, but is now often used for Internet access [1]. It enables a person with a wireless-enabled computer or personal digital assistant to connect to the Internet when in proximity of an access point. WiFi is the wireless way to handle networking [2]. It is known as 802.11 networking and wireless networking. And using this technology we can connect computers anywhere in a office or home without the need of any wires [3]. Computers connect to the network using radio signals and they can be up to 100 feet or so apart. It allow to connect to the internet from virtually anywhere at speeds of up to 55 Mbps. Computers or handsets enabled with this technology use radio technologies based on the IEEE802.11 standard to send and receive data anywhere within the range of a base station [4]. WiFi goes beyond wirelessly connecting computers, it also connects people.

What is Wi-Fi:- Wi-Fi refers to wireless networking technology that allows computers & other devices to communicate over a wireless media. It describes all network components that are based on one of [2] the 802.11 standards, including 802.11a, 802.11b, 802.11g, 802.11n. These standards These standards are developed by the IEEE and adopted by Wi-Fi Alliance.

The Objective of this paper is to identify the following characteristics:1 Identifying security vulnerabilities in the Wi-Fi System. 2) Produce a secure authentication process by using Random Number Generator. 3)Provide a secure Encryption and Decryption Algorithm.

Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA cryptosystem of MIT in 1997.it was described in 1978. Some of the famous secur ity system which is composed of three faces: such as prime Key generation, Encryption and Decryption phase.In this technique we used RSA cryptosystem algorithm. In which included the private key and public key. The public key only used for encrypt the messages and it can be seen to all. It is not secret key. The private key is used for decrypt the messages. Private Key is also called the secret key. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provides security. In which two techniques are used like encryption and decryption. The encryption technique which is used to convert original (plain text) data to cipher text. The plain text is also called the clear text. The plain text is easily read by anyone. Second technique is decryption which is used to convert cipher text to plaintext (readable format).cipher text is also called the unreadable form.

II. DIFFERENT SECURITY VULNERABILITIES

A. Authentication Vulnerability

Secure access of network services is becoming an important issue for the present communication system. Any attempts of an intruder to create a chaos or to get registered with the network inllegimately in it is possible if the user authentication and authorization is compromised.

B. Interleaving: Interleaving is the sub-class of Man-In-Middle attack and it is aimed for PKM v2. In this attack an adversary interleaves a communication session by maintaining connections with the Base Station and Subscriber Station. All the information on the route passes to the adversary node and an information leakage point built. The interleaving attack is the re-transmission of a set of messages from the same session.

C. Suppress Replay: Due to the loss of synchronization in the clocks of the entities the intruder can gain control on the authentication framework by capturing the messages and transmitting them with added delays, this will cause forward message delay.

D. Fabrication: Another active attack on authentication where an intruder pretends to be the source entity. Examples of fabrication attacks are Fake Emails and Spoofed packets. Man in the middle attacks is the example of fabrication.

III. SOLUTION METHDOLOGY

In this paper we developed an algorithm that is based on modified RSA cryptosystem based on 'n' prime numbers. This algorithm is useful to getting the high security. We endeavored to evolve 'n' prime numbers for security throws the networks. Because 'n' prime numbers are not easily decomposed and increased the efficiency throw the networks.

RSA algorithm:

- Select two different prime numbers p and q
  For security aim, the integer's p and q must be prime numbers.
- Calculate n=p*q
  n will be used as the module for public key and private key.
- Calculate f(n)=(q-1)(p-1), Where f is a function of Euler's
- Select an integer e such that
  1<e<f(n) and GCD (e, f(n))=1;
  e and f(n) are co prime.
- Determine d:
  d is multiplicative inverse of e mod (f(n))

(e * d) mod f (n) = 1 d is the private key

Encryption: A transfer the data m with the public key (e, n) to B receives the data m with the private key (d, n) Such that 0<m<n

$C=m^e \bmod n$

A will be used the public key and transfer the data plain text to cipher text.

Decryption: B will be gotten the data or message m throws the cipher text to plain text. B is used private key d.

$$m= c^d \bmod n$$

Example:

Below is given an example of RSA algorithm In which we will be used four prime numbers and get public key and private key.

Select four prime numbers.

P=2, q=3, r=5, s=17

1.Calculate n=p*q*r*s n=2*3*5*17

2.Calculate f(n)=(p-1)(q-1)(r-1)(s-1)

f(510) = (2-1) (3-1) (5-1)(17-1)

=128

f (n)=128

3.Select any number 1<e<128

F (n) must not be divisible by e

Let e=3

Select d, multiplicative of e(mod f(n))

d= 43

the public key is(n = 510,e = 3) private key is (n = 510,d = 43) Given message m = 11.

Encryption:

C = 311 mod 510 = 311

C=311

Decryption:

$M = 311^{43} \bmod 510 = 11$

B got the original message (11) which is sent by A.

IV. CONCLUSIONS

In this paper we used 'n' prime numbers which is provided the security over the networks. In which we endeavored to get the quality that make easier the cryptography to have a good use of 'n' prime numbers. The 'n' prime numbers act (play)very necessary role in RSA cryptosystem. To develop the RSA algorithm for 'n' prime numbers and also used four prime numbers.

REFERENCES

[1] Basic Theory of Wi-Fi .
[2] Wireless Fidelity.
[3] CISCO Spectrum Expert Wi-Fi Data Sheet.
[4] IEEE 802.16e Security Vulnerability Analysis and solution.
[5] RSA Algorithm.
[6] "Security Enhancement and Solution for Authentication framework in IEEE 802.16e
[7] Security Improvement of 802.11i (Wi-Fi Protected Access 2).

AUTHOR DETAILS:

T.Venkata Satya Vivek, completed his B.Tech (CSE) from Vishnu Institute Of Technology, Bhimavaram, India and M.Tech(Computer Networks & Security) from KL University, Vijayawada, India. Presently he is working as an Assistant Professor (CSE Department) in PACE Institute of Technology & Sciences. He has published a couple of Research Papers in various International Reputed journals and Conferences. His research interests include Data Hiding Techniques and Cryptography.

D.Anandam, completed his B.Tech(CSE) from VBIT Hyderabad, India and M.Tech from NIET Guntur, India. Presently he is working as an Assistant Professor (CSE Department) in PACE Institute of Technology & Sciences. He is having Five(5) Years of Teaching Experience in various colleges. He has published a couple of Research Papers in various International Reputed journals and Conferences. His research interests include Data Hiding Techniques, Image Processing, Networks, Cloud Computing.

Ganta Anil, Completed his B.Tech(IT) from Rao & Naidu Engineering College, Ongole, and M.Tech(IT) from SRKR Engineering College, Bhimavaram, India. Presently he is working as an Assistant Professor (CSE Department) in PACE Institute of Technology & Sciences. He has published a couple of Research Papers in various International Reputed journals and Conferences. His research interests include Data Hiding Techniques, Image Processing, Networks.

B.Sreenivasulu Completed his B.Tech(CSE) from VRS & YRN College of Engineering & Technology, Chirala and M.Tech(CSE) from St.Ann's College of Engineering And Technology, Chirala, India. Presently he is working as an Assistant Professor (CSE Department) in PACE Institute of Technology & Sciences. He is having Two(2) Years of Teaching Experience in various colleges. He has published a couple of Research Papers in various International Reputed journals and Conferences. His research interests include Data Hiding Techniques, Image Processing, Networks.

V.Lakshma Reddy, Completed his Master of Computer Applications from Sathyabhama Univesity,Chennai. Presently he is working as Assistant Professor(CSE Department) in PACE Institute of Technology & Sciences. He is having 4 years of Teaching Experience He has published a couple of Research Papers in various International Journals and Conferences. His research areas include Data Mining, Data Warehousing, Cloud Computing, Cryptography.

M Rao Batchnaboyina, Completed his B.Tech(CSIT) from Jawaharlal Nehru Technological University, Hyderabad and M.Tech(IT) from College of Engineering, GITAM University, Visakhapatnam, India. Presently he is pursuing his PH.D from Acharya Nagarjuna University, Guntur. He is having 8 years of teaching experience. He has published a couple of Research Papers in various International Reputed Journals and Conferences. His research interests include Information Security and Classification in Data Mining.