WI FI BASED SECURE WIRELESS COMMUNICATION USING RSA

Reena R.

Lecturer in Electronics,

MVGM Govt. Polytechnic College, Vennikulam, Pathanamthitta, Kerala.

ABSTRACT

A modified RSA cryptosystem based on 'n' prime is used to secure data or information. This is a novel method for ensuring maximum network data security. Encryption, decryption, and key generation are all involved. A prime number is used in a modified RSA cryptosystem to provide network security. In this technique, we used a 'n' prime number that is difficult to break. 'n' prime numbers are difficult to decompose. This technique increases network efficiency and reliability. We discussed security in Wi-Fi technology in this Research Paper. We also presented solutions to some of these security flaws. The solution is based on a random number generation process as well as a variety of encryption and decryption algorithms.

Keywords: *Wi-Fi, Random Number Generation, Key Generation, and the Modified RSA Algorithm.*

INTRODUCTION

Wi-Fi is an IEEE 802.11-based set of product compatibility Standards for Wireless Local Area Networks (WLAN). Wi-Fi was designed for mobile devices and LANs, but it is now commonly used for Internet access. When a person is in close proximity to an access point, he or she can connect to the Internet using a wireless-enabled computer or personal digital assistant. Wi Fi is a wireless networking protocol. It is also referred to as 802.11 networking and wireless networking. And we can use this technology to connect computers anywhere in an office or home without the use of wires. Computers connect to the network via radio signals and can be located up to 100 feet apart. It enables users to connect to the internet from virtually any location at speeds of up to 55 Mbps. This technology enables computers or handsets to send and receive data anywhere within the range of a base station using radio technologies based on the IEEE802.11 standard. Wi-Fi not only wirelessly connects computers, but it also connects people. [1-4]

We will be able to enter messages into the system after it has been started. The maximum message length is 32 characters. After that, the system prompts for a key, which can be either a number or an alphabet. Entering the key causes the encrypted message to be sent to the other system. The other system then requests that key view the message. If the user enters the correct key, the message is decrypted; otherwise, it displays a garbage value, securing wireless communication.

We developed an algorithm in this paper that is based on a modified RSA cryptosystem based on 'n' prime numbers. This algorithm is useful for achieving high security. We attempted to develop

'n' prime numbers for network security throws. Because 'n' prime numbers are difficult to decompose and increased network efficiency. [5]

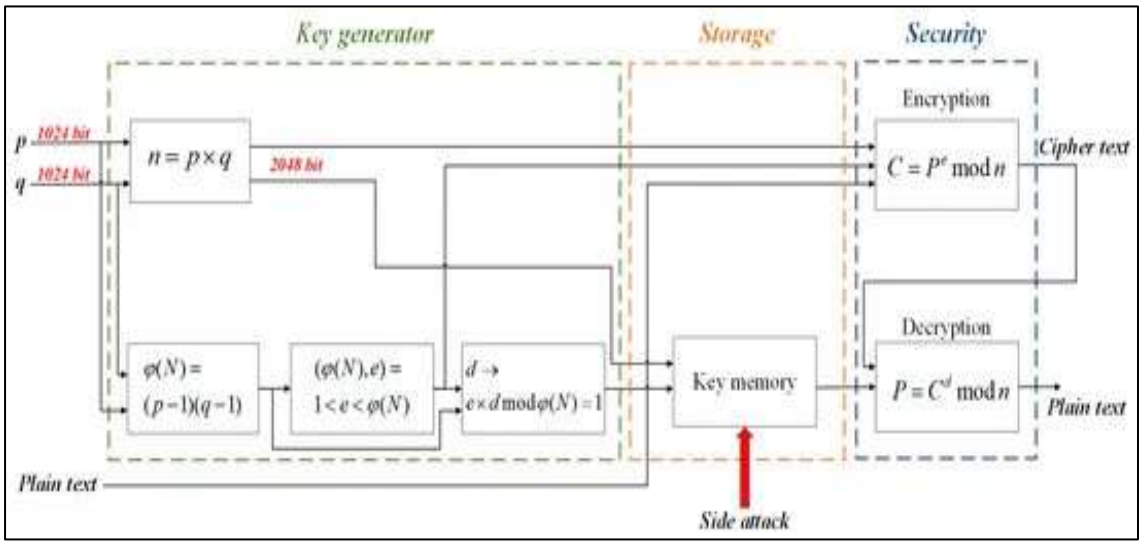


Figure 1: Conventional RSA block diagram

As illustrated in Figure 1, existing RSA encryption is divided into three processing modules. The key generator module first receives a 1024 bit pseudo-random number and generates a private and public key. The second storage module is a memory that stores a private key of 2048 bits. Because it constantly stores a 2048 bit key in memory, it is extremely vulnerable to side attacks. If the side attack is successful, the RSA encryption algorithm's security is compromised regardless of encryption key size. The security module then encrypts data with 2048-bit private and public keys. The algorithm for encrypting and decrypting using the 2048 bit key necessitates extremely large hardware that is nearly impossible to implement. Furthermore, exchanging 2048 bit private and public keys via wireless communication is difficult. [6]

RSA algorithm:

• Select two different prime numbers p and q For security aim, the integer's p and q must be prime numbers.

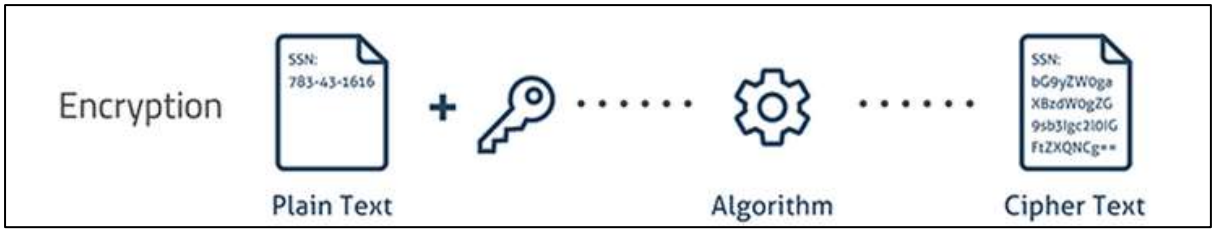
• Calculate n=p*qn will be used as the module for public key and private key.

• 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:

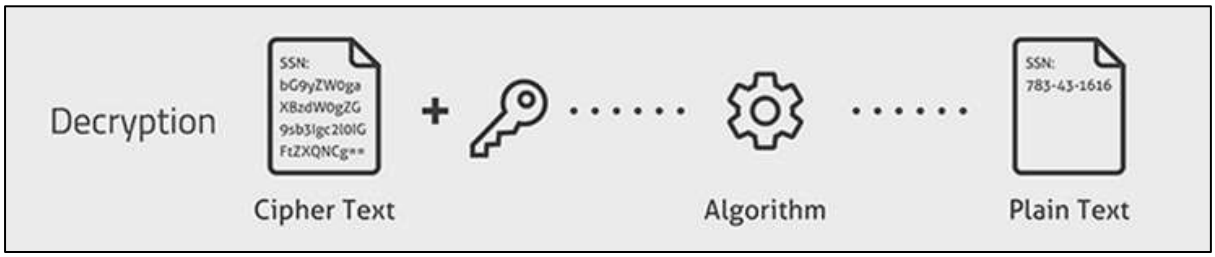


A transfer the data m with the public key (e, n) to B receives the data m with the private key (d, n) Such that 0<m<n

$$C=m^e \bmod n$$

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.

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

Objectives:

1. Wi-Fi-based secured wireless communication with RSA encryption enables us to communicate wirelessly while maintaining security.
2. Data transfer between two systems is encrypted using RSA encryption, which is highly secure.
3. Identifying security flaws in the Wi-Fi system.
4. Using a Random Number Generator, create a secure authentication process.
5. Make available a secure encryption and decryption algorithm.

REVIEW OF LITERATURE:

Lifeng Sang et al. proposed a shared secret free wireless network security infrastructure based on two physical primitives: cooperative jamming and spatial signal enforcement. Cooperative jamming is used for secure wireless communication, while spatial signal enforcement ensures message authenticity. Infrastructure that has been proposed. [7]

Arash Habibi Lashkari and colleagues presented an overview of wireless security protocols (WEP, WPA, and WPA2/802.11i). WEP protocol types, flaws and improvements, WPA protocol types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function, and rekeying mechanism are discussed. They also explained major issues with WPA that occurred on the PSK part of the algorithm. Finally, the paper described the third generation of wireless security protocols as WPA2/802.11i. [8]

Hyung-Woo Lee and colleagues discussed various issues and challenges in wireless sensor networks. The paper described two types of wireless security attacks: one against security mechanisms and the other against basic mechanisms such as routing mechanisms. Denial of service attacks, attacks on information in transit, sybil attacks, hello flood attacks, wormhole attacks, and blackhole/sinkhole attacks are all explained. The paper also discussed various wireless sensor network security schemes such as wormhole-based, statistical en-route filtering, random key, and tiny sec. In addition, a holistic view of security in wireless sensor networks is described. [9]

Gamal Selim and colleagues described various types of security attacks, including MIC modification, fabrication, interception, brute force, maintainability, and static placement. They examined the current security protocols, including WEP, WEP2, WPA, and WPA2. They also proposed a novel mechanism known as the multiple slot system (MSS). The key selector, slot selector, and MIC shuffle selector are all used by MSS. MSS employs one of four encryption algorithms, including RC4, RSA, Blowfish, and AES. [10]

Kirti Raj Bhatele et al. proposed a hybrid security protocol for improved security by combining symmetric and asymmetric cryptographic algorithms. The MD5 algorithm is used to calculate the hash value of the decrypted message using the AES algorithm. This hash value was encrypted with dual RSA and the encrypted message was also sent to the destination. At the receiving end, the hash value of the decrypted plaintext is calculated using MD5 and then compared to the hash value of the original plaintext calculated at the sending end to ensure its integrity. This allows us to determine whether or not the original text was altered during transmission through the communication medium. [11]

RESEARCH METHODOLOGY:

A study is being conducted for various popular secret key algorithms. They were put in place, and their performance was evaluated by encrypting real-time video streaming of varying contents.

Books, educational and development journals, government papers, and print and online reference resources were among the secondary sources we used to learn about the composition, use, and consequences of Wi-Fi Based Secure Wireless Communication Using RSA.

RESULT AND DISCUSSION:

The PROTEUS MODELING yielded the following results, which describe the encryption and decryption algorithms of our proposed system. The figure depicts the scanning of input texts in preparation for encryption. The condition of the switches is checked for inputs, and the encryption process is carried out. [12]

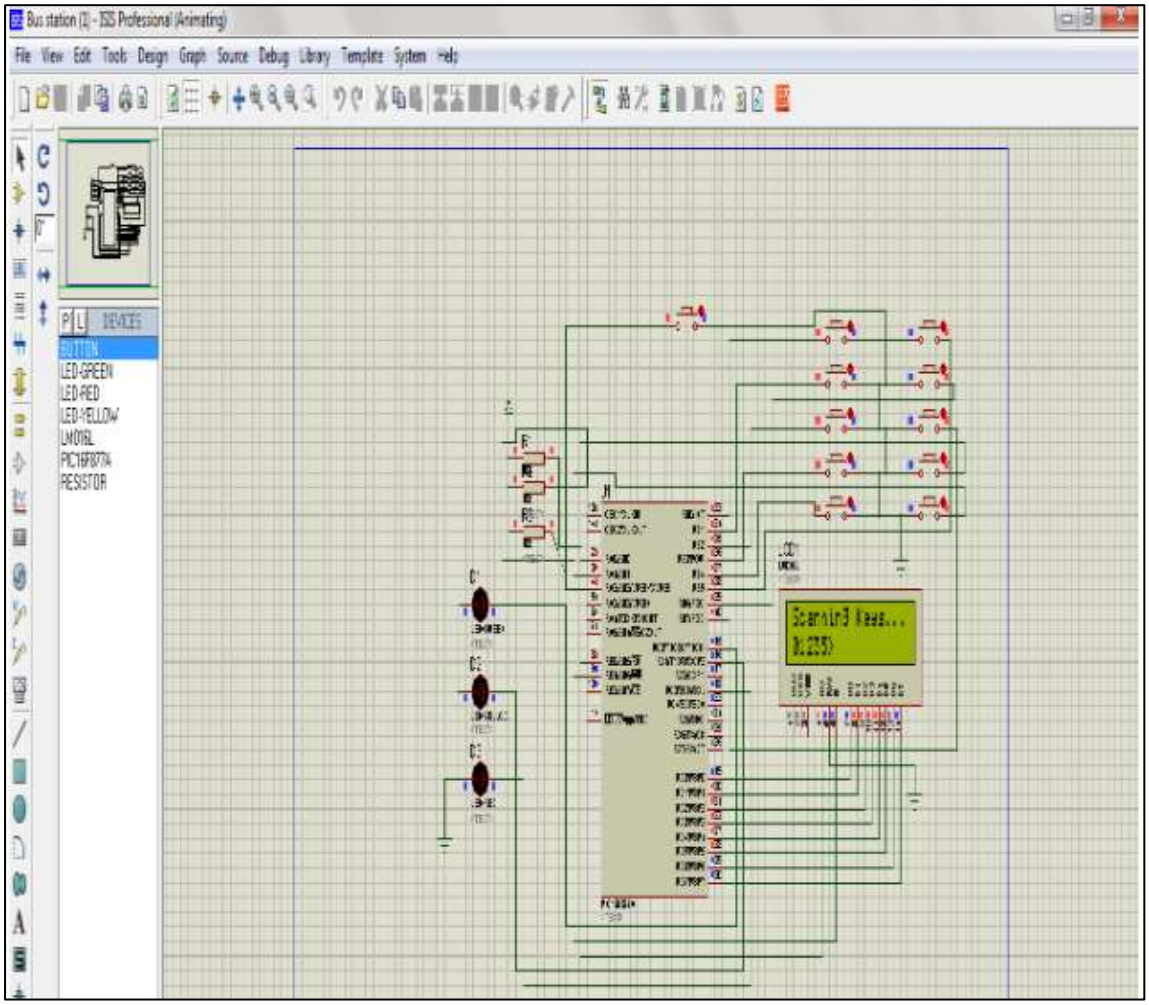


Figure : Simulation result showing the transmission of the input text

The simulation results in Figure show that the input text is transmitted to the receiver side. [13]

Figure depicts a hardware-implemented RSA encryption module. In the decryption module, the p, q values, and plain text are entered, and the keys (n, e, d) are generated using the RSA algorithm. According to the RSA encryption formula, the plain text value of 1542 is encrypted to the cypher text value of 8,135,351. [14-15].

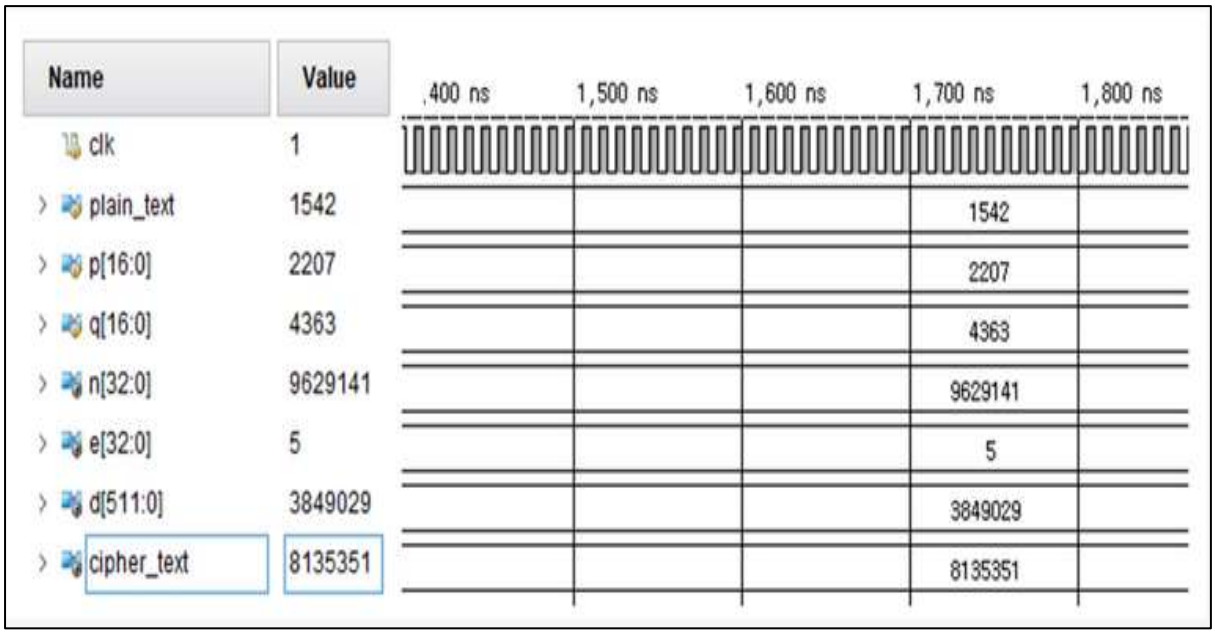


Figure: 7 Encryption simulation results

CONCLUSION:

Cryptography is the most secure method of data security. When compared to previous works, the proposed RSA performs better. It will take less time, and breaking the encryption algorithm without knowing the exact key value is impossible. This algorithm can be used to encrypt and decrypt data in any type of public application that sends confidential data.

REFERENCE:

1. A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.
2. Shams, R.; Khan, F.H.; Umair, M. Cryptosystem an Implementation of RSA Using Verilog. Int. J. Comput. Netw. Commun. Security 2013, 1, 102–109.
3. Silicon Labs Company, “Wireless protocol of Internet of Things,” Microcontrollers & Embedded Systems, no. 10, pp. 82-83, 2017.
4. Cisco Spectrum Expert Wi-Fi Data Sheet: http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html

5. "IEEE 802.16e Security Vulnerability: Analysis & Solution", A. K. M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST, October 2010, Volume 10, Issue 13, Version 1
6. Rivest, R.; Silverman, R. Are 'Strong' Primes Needed for RSA. In Cryptology ePrint Archive, Report 2001/007.
7. L. Sang and A. Arora, Editors, "A Shared Secret Free Security Infrastructure for Wireless Networks", ACM Transactions on Autonomous and Adaptive Systems (TAAS), (2012) July.
8. A. H. Lashkari and M. M. S. Danesh, Editors, "A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i", IEEE International Conference on Computer Science and Information Technology, (2009) August 8-11, Beijing.
9. H.-W. Lee, A.-S. K. Pathan and C. S. Hong, Editors, "Security in Wireless Sensor Networks: issues and challenges", International Conference on Advanced Communication Technology (ICACT), (2006) February 20-22, Phoenix Park.
10. G. Selim, H. M. E. Badawy and M. A. Salam, Editors, "New Protocol design for Wireless Networks security", IEEE International Conference on Computer Science and Information Technology (ICACT), (2006) Feb 20-22.
11. K. Bhatele, A. Sinhal and M. Pathak, Editors, "A Novel Approach to the Design of New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram.
12. Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, University of Mumbai. "Enhancing Data Security by using Hybrid Cryptographic algorithm", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013
13. D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks." IBM Journal of Research and Development,May 1994, pp. 243 -250
14. Shams, R.; Khan, F.H.; Umair, M. Cryptosystem an Implementation of RSA Using Verilog. Int. J. Comput. Netw. Commun. Security 2013, 1, 102–109.
15. Rahman, M.; Rokon, I.R.; Rahman, M. Efficient Hardware Implementation of RSA Cryptography. In Proceedings of the 3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication, Hong Kong, China, 20–22 August 2009; pp. 316–319.