A Novel Mutual Authentication Protocol for H(e)NB and Mobile Devices Using S8 S-box

By

Talha Naqash

Supervised By:

Eng.Umar Mujahid

DEPARTMENT OF COMPUTER SCIENCES

BAHRIA UNIVERSITY

ISLAMABAD

Session 2011-2013

Dated: ----------

Final Approval

This is to certify that we have read the thesis submitted by Talha Naqash, Enrollment # 01-244111-019, It is our judgment that this project is of standard to warrant its acceptance by the Bahria University, Islamabad, for the Degree of MS in Telecommunications and Networking.

Project Evaluation Committee

External Examiner: ----------

Internal Examiner: ----------

Supervisor: **Eng.Umar Mujahid**

This thesis is submitted in partial fulfillment of the requirements for

Master of Sciences (MS)

in

Telecommunication and Networking

PROJECT IN BRIEF

Project Title:	A Novel Mutual Authentication Protocol for H(e)NB and Mobile Devices Using S8 S-box
Submitted By:	Talha Naqash MS-(Telecommunication And Networking)
Supervised By:	Engr.Umar Mujahid
Start Date:	February 2012
Completion Date:	December 2013
Tools & Technologies:	-MATLAB 2012 -Ginger IT -Visio -Microsoft Office Excel 2007 -Microsoft Office Word 2007 -Paint
Operating System:	Windows 7
System Specifications:	Intel® Pentium® Core i 5 2.4 GHz 8GB RAM 700 GB HDD

ABSTRACT

In wireless communication, Femtocells are used to enhance the service coverage inside the office or home, particularly where access is narrow or engaged. Femtocells enhance the service quality that is attractive for the client and the mobile operator. Currently, security of core network from the unauthorized user in public environment is a big issue and there is no integrated solution to verify a rouge femtocell or unauthorized user equipment (UE). Forged equipment can launch any attack or hack the core network to act actively or passively. A femtocell is a feasible option to enhance the signal strength. Authentication of the legal user and legitimate femtocell is a serious issue. Many protocols have been proposed for mutual authentication but each has its own benefits and drawbacks. Hence, there is a need for a mutual authentication protocol, so communication equipments can verify each other during connection establishment and make a secure tunnel for communication.

In this thesis we proposed a solution which provides mutual authentication between the User Equipment (UE) and femtocell that will make the system more secure. The proposed algorithm is interoperable and use S8 S-box for AES to reduce the authentication time. S-box transformation is an important part of the AES algorithm as it is the only nonlinear component which introduces confusion in the algorithm. S8 S-box can be obtained by applying symmetric group S_8 on AES S-box, and 40320^{40320} new keys can be constructed. Every permutation of the elements of the S-box results in a new S-box which makes the communication more secure.

Moreover, novel scheme is also compatible with the current network architecture and resist various network attacks e.g., Sybil attack, MITM, DOS, Eavesdropping & Injecting attack and Packet Sniffing.

Contents

List of Figures

List of Tables

ACKNOWLEDGEMENTS

In the name of Allah Almighty, who is the most merciful and the most beneficent. He is the one who gave me the courage and determination to carry on when all seemed impossible.

It is my great fortune to have pursued my research under the guidance of my advisor, ***Umar Mujahid,*** who introduced me to the subject area, and guided me at every step of the way with his knowledge and experience. His prompt and detailed feedback greatly helped me throughout my research and inspired me to explore deeper. Our weekly meetings always kept me focused and helped me complete my work within the proposed timeline.

My special thanks go to ***Sir Dr Fazal e Hadi*** for arranging initial meetings with various other faculty members. I would also like to thank ***Dr. Imran Siddiqi***, from the Research cell, for his guidance regarding issues like time lines and other research requirements.

There come times when one feels discouraged by dead ends especially during my severe accident, but special thanks to my friends Amish Hasan and Kashif Shabir for guiding and supporting me to write this thesis

Finally I would like to extend my gratitude to Bahria University, Islamabad, for giving me this opportunity to conduct this research and to facilitate it by enabling access to valuable knowledge pool of IEEE archives.

DEDICATION

I dedicate this thesis to my family, my younger brothers and especially my Mom a centre of love for me for his support and inspiration, my parents for their endless prayers, and all my friends who helped me and encouraged me at every step of my life

RESEARCH PUBLICATIONS

- N. Talha, M. Umar, I. Najam et al; "Efficient Implementation of 1024-bit Symmetric Encryption and Decryption Algorithm for Real Time Communication Systems", Published in IEEE, Student Conference on Research and Development 2012 (SCORed) Malaysia

- N. Talha, M. Umar, I. Najam et al; "A Novel Mutual Authentication Protocol for H(e)NB and Mobile Devices Using S8 S-box"; Published in IEEE, International Conference on Open source System and technology 2012 (ICOSST 2012)

- N. Talha, M. Umar, I. Najam et al; "Mutual Authentication Protocol for LTE Based Mobile Networks"; Published in IEEE, International Conference on Open source System and technology 2012 (ICOSST 2012)

- N. Talha, H. Fazal, et al; "Protecting DNS from Cache Poisoning Attack by Using Secure Proxy"; Published in IEEE, 8th International Conference on Emerging Technologies 2012 (ICET 2012)

- N. Talha, H. Fazal; "Handover Mechanism for Mobile User and Femtocell for LTE Network" Submitted to IEEE, 10th International Bhurban Conference on Applied Sciences & Technology 2013 (IBCAST 2013)

- N. Talha, M. Umar, I. Najam et al "Secure DNS from amplification attack by using Modified Bloom Filters";Submitted to IEEE ,10th International Bhurban Conference on Applied Sciences & Technology 2013 (IBCAST 2013)

CHAPTER-1

INTRODUCTION OF LONG TERM EVOLUTION (LTE) & MUTUAL AUTHENTICATION

1. Introduction

Long term Evolution is also called next generation wireless communication. LTE can provide us digital technology and wide use of bandwidth with enhanced capabilities. LTE project was started in 2004. Basically it was developed to reduce the cost per bit, facilitate the users with better services, overcome the power consumption and establish a simplified, lower cost network. These initial goals motivate the inventors to add some special features in LTE like to reduce the latency for packets and HSPA, downlink three to four times and uplink two to three times. Customers already using the facilities of High Speed Packet Access (HSPA) for example DSL is replaced by the HSPA modems and with the help of 3G phones sending receiving videos and music files. The client experiences a great change with LTE technology. Further it provides better performance for the interactive TV, mobile video conversations, and advance online gaming setups or professional services. LTE provides many services a few of them are discussed below:

- Performance and Capacity: One of the features is to provide high downlink and uplink connection. LTE provides at least 100 Mbits/s for downlink. But this technology allows for speed over 200Mbit/s, Ericson demonstrated the idea of 150Mbit/s.
- Simplicity: LTE supports a flexible channel bandwidth (5Mhz to 20MHz). Frequency Division Duplex and Time Division Duplex are also supported by the LTE. LTE radio network products can easily build and manage the next generation network and provides facilities like plug and play, self configuration and self optimization of problem. These features can reduce the network building cost. It is based on simplified IP based core transport networks that are easier to build and maintain.

  According to a survey broadband subscription has reached 1.8 billion in September 2012. From these 1.8 million customers two third are using the mobile broadband. Mobile data traffic is expected to overtake voice traffic in 2010 which will place high requirements on mobile networks today and in future.

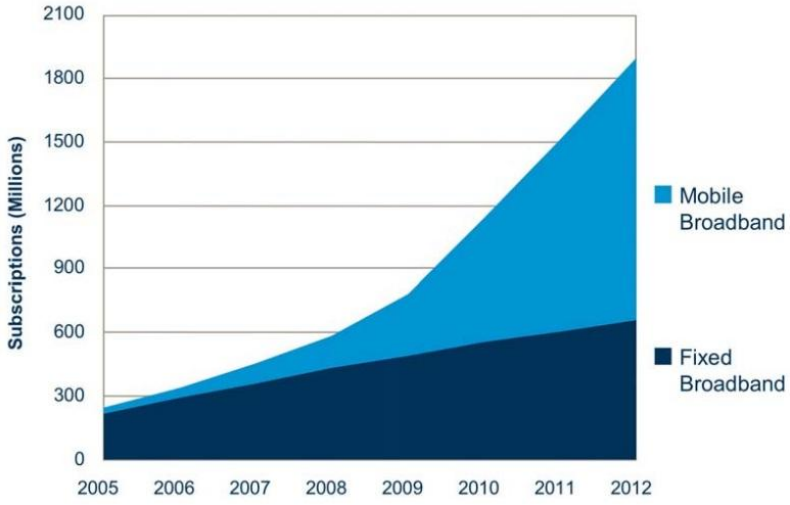


Figure 1.1 Fixed and Mobile Broadband Usage[6]

Authentication has a significant role in a secure communication. But in this era when communication is vulnerable by eavesdropper there is need of mutual authentication in which sender and receiver can check the authenticity of each other. Non vulnerable authentication in an insecure communication is impossible. In the past user authenticity was judged by checking user identification (ID) or password. The IP address of the user was also checked to assure the authenticity of the user. But all described methods fail when an eavesdropper gets access to physical system than all the communication will be at risk.

For the secure communication between mobile and femtocell there are different techniques are used but every technique has its own pros and cones. Encryption key has two types symmetric and A symmetric. In symmetric key cryptography transmitter and receiver both use the same key for encryption and decryption. But for secure communication two techniques of symmetric encryption DES and 3DES are changed with Advance Encryption Standard (AES) [1]. AES provides a secure communication tunnel. National Institute of Standard and Technology (NIST) approved the AES in 2001. AES can also be used for the wireless technology like Wi-Fi [2] and Wi-MAX [3] and many other technologies like femtocell authentication and smart card security [4].

Femtocells referred as Home Node B (HeNB) in 3GPP standard, are the access point base stations providing services, especially at the places where the signal strength is low or weak.

Femtocells are gaining much attention recently, as the services in Fourth Generation (4G) systems demands users to have a better connection at all times. The architecture of femtocell allows the users to have the best coverage at low cost, low power and compatible with the current mobile networks [5]. Femtocell is an inexpensive and a limited capacity base station that allows the operators to provide better and high bandwidth cellular coverage to residential users and small office environment.

Femtocells connect with broadband internet to provide 3G and 4G services to home users as shown in Fig 1.2 [8]. Service providers support femtocell technology because it provides RF environment, easy installation and can be managed remotely.

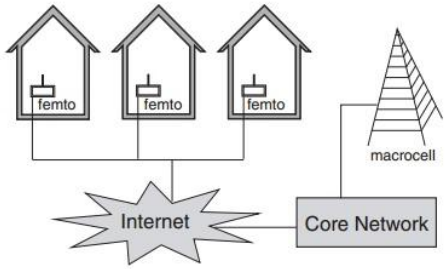


Figure 1.2 Typical femtocell and Macrocell scenario

Broadband service providers need femtocell deployment according to industry standards to give better and smooth voice and data services [6]. A femtocell has a range of 200 meters and it is wired to the core network, which is vulnerable. This conception is called backhaul [7].

1.1. Research Question

Femtocell Access Point (FAP) connects to core network through the femtocell Secure Gateway (FSG) in vulnerable environment as shown in figure 1.3. In such environment there is a need to authenticate a user before it connects to core network. Classical techniques allow User Equipment (UE) to connect with core network after an authentication phase on base stations. However, the idea of Femtocell has changed the classical way, now authentication phase is performed before UE connects with femtocell [8].

Femtocell attaches with xDSL to provide better Quality of Services (QoS). The communication between UE and femtocell can be compromised due to weak algorithms. Authentication data in femtocell is not secure, so the attacker can easily act actively and passively. On the other hand if

an eavesdropper establishes a replica credential and tries to connect with the core network, mutual authentication is the solution of such attacks. Legitimate and illegitimate user can also be categorized by using the Close Subscriber Group Identity (CSG_id) [5].

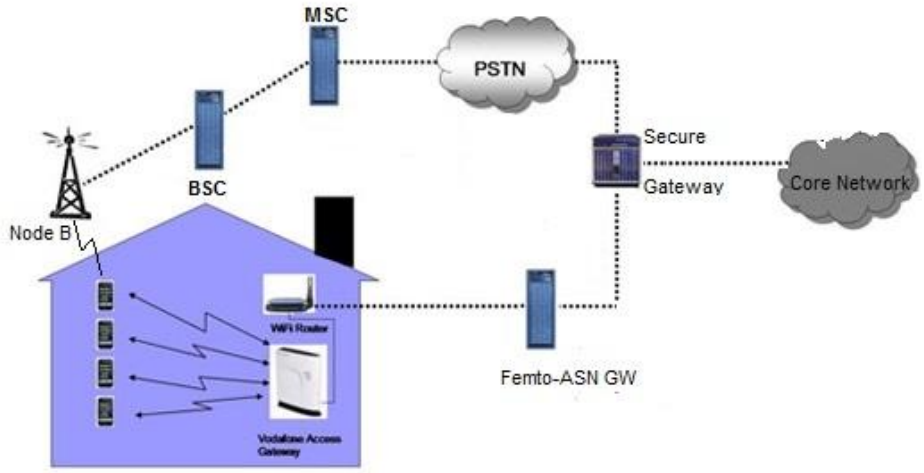


Figure 1.3 Femtocell Architecture

When a UE tries to connect with core network then its identity is checked in CSG list, only a legitimate user can access the core network. If the identity of the user is compromised then an eavesdropper can launch many attacks like Denial of Service (DOS), Sybil, and Man In The Middle (MITM) attack.

1.2. Research Scope

A number of femtocells are deployed in the year of 2012 as shown in the figure 1.4 [8]. Femtocell is used widely due to its following reasons:

- It enhances the signal strength where macro cell fails to provide the service.
- It minimizes the communication traffic over macro cell that helps micro cell to increase its performance.
- Isolation of the signal can also increase the performance of the service.
- Growing demand of the high data rate day by day can also be achieved by using femtocell. Because femtocell has a small coverage area with better signal strength.

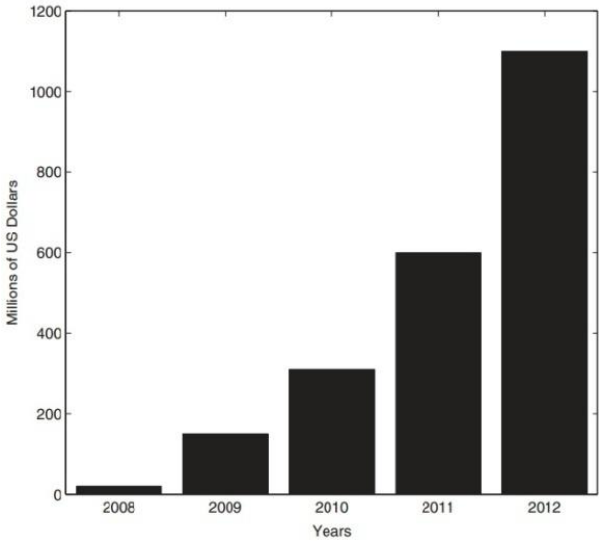


Figure 1.4. Usage of Femtocell in 2012

- Femtocell significantly save the power of the user equipment as femtocell is deployed inside the covered area so user equipment requires low transmitting power to transmit the signal. On the other hand battery life of the UE also increases.
- Femtocell also cost effective solution as femtocell is switched on when a user want to use it at home, office or any covered area.

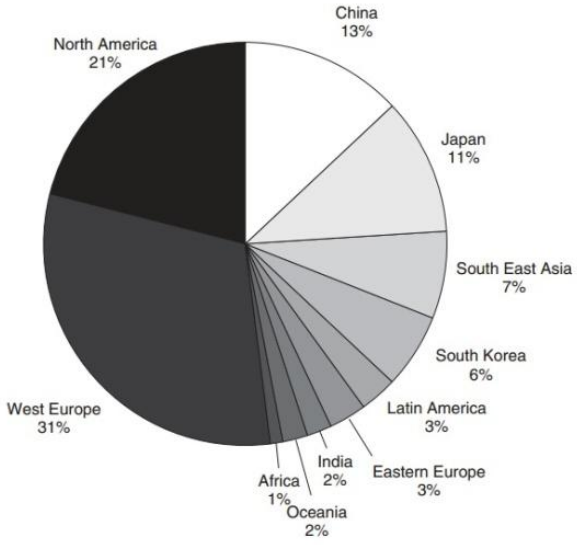


Figure 1.5 [8]. Country wise Deployment of Femtocell

1.3. Problem Statement

In a wireless communication all services require authentication but there is no way for mutual authentication that is non-vulnerable. Mutual authentication between the femtocell and user equipment is a delegated problem. The architecture of femtocell allows the users to have the best coverage at low cost, low power and compatible with the current mobile networks. Authentication of user on femtocell network is not secure, so the attacker can easily act actively and passively. On the other hand if an eavesdropper establishes a replica credential and tries to connect with the core network, mutual authentication is the solution of such attacks Many classical techniques have been described but there is a need of an algorithm for mutual authentication that must be secure, lightweight and time efficient.

1.4. Motivation and Objectives

Femtocell has three access modes, Open access mode, Close access mode and Hybrid access mode. In open access mode all UEs can use the services; there is no need to authenticate any user. In Close access mode only legitimate user can use the services after authentication. A white list is maintained by management to check the identity of legal UE identity. Hybrid access mode is the mixture of Open and Close access mode because all users are allowed to use the services in this access mode but under some restrictions [5]. These access modes have some limitations, in close access mode a guest clients can never access the services. However, it is hard to implement restrictions in Open and Hybrid access mode. Fake or rouge femtocells can be installed to spoof the identity of a legal UE.

To solve such troubles many solutions are proposed. The communication between Mobile Devices (MD) and femtocell is established on trust based relation, a password or any identification mark is given by the user for authentication [9]. Extensible Authentication Protocol (EAP) is widely used for the authentication in Wireless network. Various authentication techniques are recommended according to femtocell security gateway implementation. EAP-transport Layer Security (TLS) protocol is mostly implemented on femtocell. EAP-TSL protocol uses the Public key Infrastructure to produce and supervise the digital certificates. EAP-TSL is known as EAP-Secure Socket layer (SSL). UE generate the certificate and Public Key Infrastructure (PKI) handle the validity of certificate and encryption keys [10].

EAP-Subscriber Identity Module (EAP-SIM) authentication is used for GSM based technology; two parties can exchange information with each other by using a unique identity number [11]. Universal Mobile Telecommunication System (UMTS) uses a SIM card and Authentication Key Agreement (AKA) protocol [12]. Two symmetric keys are used to authenticate a legitimate user in AKA protocol. EAP-Internet Key Exchange version 2 (IKEv2) is the modified form of IKEv1. It's a flexible and secure authentication protocol because the public key is also encrypted in a certificate and only one unit knows the private key. IKEv2 use a password and symmetric keys for mutual authentication [13]. Mutual authentication is the need of Long Term Evolution (LTE) based mobile networks because an operator would like to authenticate only a legal user who can access the core network. On the other hand, a UE would like to connect with a legal or legitimate femtocell to get access to core network.

IP based networks generally use X.509 certificates. The serial number of the femtocell is hidden inside the trusted platform module; which is a hardware component designed by the manufacture. No one can change the information embedded in this hardware component. Only manufacture and operator know the serial number and when a client installs a femtocell to use then only public key and serial number are used together for communication [7]. SIM card can also be used by Femtocell Access Point (FAP) to authenticate a user. A SIM is bedded in the femtocell which contains the data (Identification code or Secret identity) [8]. Using a visual channel for communication is a safe and trustworthy way [9]. A programmable LCD is connected with the femtocell which displays Quick Response code (QR). This QR code contains the public keys used for mutual authentication between UE and the femtocell. User take a picture from the LCD attached with femtocell to get public keys and use them for Rapid Development Authentication Protocol (RDAP)[1]

So there is a need to design authentication protocol that mainly focus on four goals

1. An algorithm that is more secure than the classical technologies
2. The algorithm should be interoperable
3. The algorithm should be compatible with mobile architecture
4. The algorithm should be time efficient

1.5. My Contribution in Summary

AES has gained a lot of attention, as it is a highly secure symmetric key algorithm. S-box transformation is an important part of the AES algorithm as it is the only nonlinear component which introduces confusion in the algorithm [15].

S8 S-box can be obtained by applying symmetric group S_8 on AES S-box, and 40320^{40320} new keys can be constructed [16]. Every permutation of the elements of the S-box results in a new S-box which makes the communication more secure. Let $|S|$ be a set which contains all the SubBytes

$$S = \{\text{SubBytes}_1, \text{SubBytes}_2, \dots, \text{SubBytes}_n\}$$

and a set $|B|$ having all S8 S-boxes

$$B = \{S8\ S - boxes_i\}$$

we define a function f such that

$$f = S \to B$$

There can be n^{40320} functions between S and B so we can generate n^{40320} new S-boxes. S_8 symmetric group gives us 8! new keys to generate S-box. Hence, we can substitute n=40320 S-boxes into Sub-Byte operation of AES so total combinations will be 40320^{40320}. S8 S-boxes are bijective, nonlinear and have algebraic complexity needed for AES [14]. This motivates us to use S8 S-box in our proposed algorithm, as with the help of only 64 bits we can change the S-box, which makes the communication more secure against the attackers.

1.6 Thesis Outline

The rest of the thesis is organized as follows:

- In Chapter 2, primary techniques along with literature review are presented. The different techniques to authenticate the user or client and RDAP is discussed in detail
- In Chapter 3, Advance Encryption Standard is discussed in detail and proposed scheme to generate S_8 S-box
- In Chapter 4, Simulation results and time to complete each step of authentication protocol is discussed in detail.
- In Chapter 5, conclusions are made and a discussion of the Mutual authentication.
- References

CHAPTER-2

FOUNDATION OF MUTUAL AUTHENTICATION

2.1. Cryptography

Cryptography is the way of communication between two parties secretly in the presence of a third party. Communication can be encrypted in different ways according to requirement. The most common cryptographic ways are defined below.

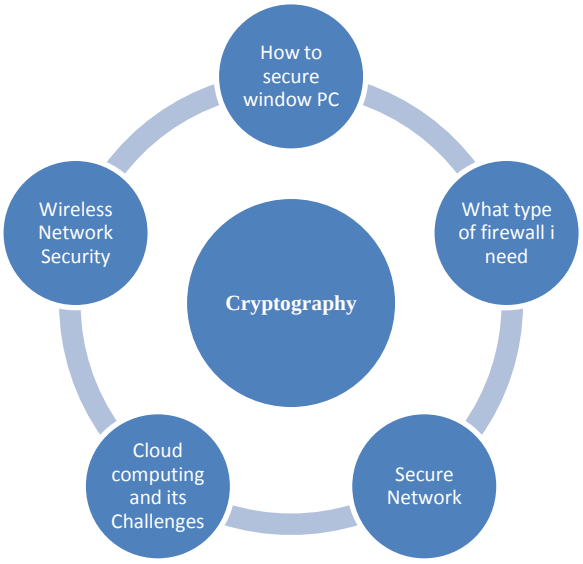


Figure 2.1 Cryptography

2.1.1. Classical Cryptography

In transposition cipher technique words are rearrange in the plain text. Normally position of a word in the text is changed and plain text become cipher text. It is hard for the third party to decrypt. For example as shown in the figure 2.2

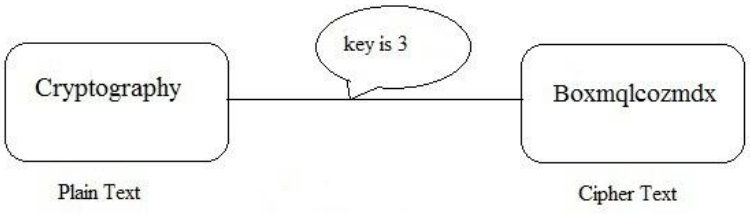


Figure 2.2 (a) Transposition Cipher

The next technique is Substitution Cipher in which a key is decided between sender and receiver than every text is encrypted with that key. A letter or group of letters is replaced according to key. It is a good encryption algorithm that produces out which seems arbitrary. But this is a breakable due frequent of the letter.

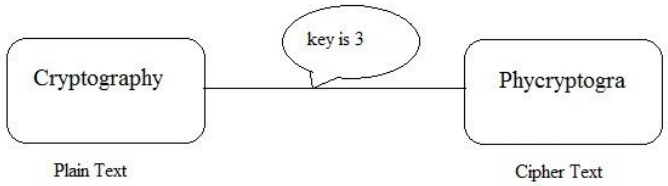


Figure 2.2 (b) Substitution Cipher

Another popular method is Blocking in which an algorithm is applied such that plaintext is divided into blocks and each block enciphered with a different key e.g JULIUSCAESAR becomes LWNKXVFDIWEV

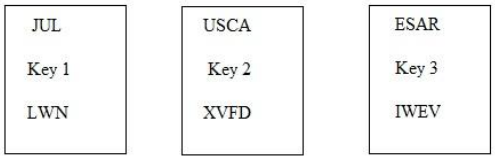


Figure 2.3 Blocking Cipher

2.2.1 Computer era and Cryptography

In computer era encryption and decryption system is handled by computer and normally use plaintext encryption technique (E), a key (k) to encrypt a message as (p), to form a cipher text (C). In mathematical form it can be written as

$$E(P, K) = C \qquad (1)$$

Similarly to decrypt a cipher text to plain text a decryption function (D) and key (K) is used as shown in the following equation [23].

$$D\ (C, K) = P \qquad (2)$$

In computer era cryptography techniques are Data Encryption Standard (DES), Ron Rivest, Adi Shamir and Leonard Adleman (RSA) and Advance Encryption Standard (AES) algorithms.

2.2.1.1 Data Encryption Standard (DES)

DES is an old technique and famous algorithm. On the demand of NSA, IBM invents an algorithm in 1970. DES algorithm has key size 8 bytes or 64 bits key. It basically encrypts 64-bit data blocks which pass through 16 cycles. Each cycle generates a different key [24]. As described before Cryptography has two main methods symmetric and asymmetric that are used today. Symmetric cryptography is also known as secret key cryptography and asymmetric is known as public key cryptography. Asymmetric cryptography is a great search in the field of cryptography. Till 1998 the standard for encrypting data was symmetric algorithm known as Data Encryption Standard (DES) later it was replaced by AES, which is described in chapter 3. DES is 64 bit block cipher that means it can encrypt the 64 bit data at a time. This standard was far better than the stream cipher which encrypt only one bit at a time. DES was invented by International Business machine (IBM) in 1960's.

The basic structure of the DES is based on the Feistel Block Cipher. This block scheme is also developed by the IBM's researcher Horst Feistel in 1970. This scheme has a specific number of rounds and each rounds has some specific steps, like bit shifting, nonlinear substitution and exclusive OR operation. In implementation step, plaintext and the key are provided to the DES. In DES encryption and decryption same key is used so it called symmetric DES. The key used is normally 64 bits or 8 bytes. The least significant bit of each byte is used for parity or set arbitrary. It is not to increase the security. All blocks are arranged from left to right which produces the 8 bits of the parity bits.

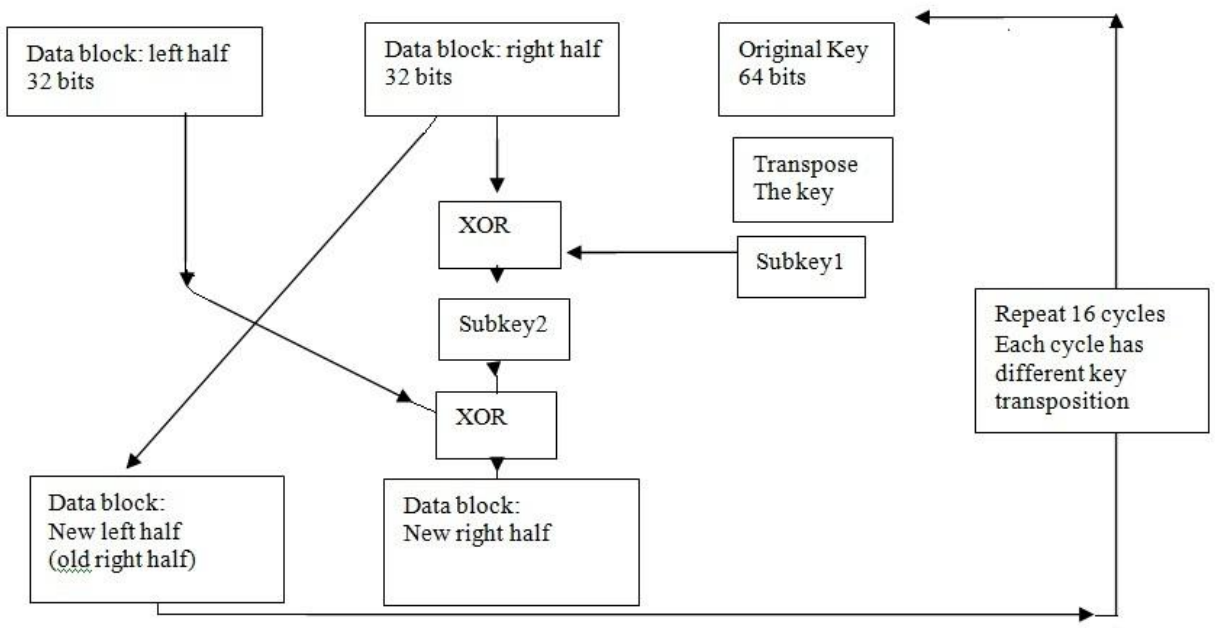


Figure 2.4 Data Encryption Standard (DES)

Automated Teller Machine (ATM) and Point of Sale (POS) security was the example of DES algorithm.

2.2.1.2 Ron Rivest, Adi Shamir and Leonard Adleman (RSA)

Three MIT students Ron Rivest, Adi Shamir and Leonard Adleman developed this algorithm which generates a public and a private key just by multiplying two large prime numbers but it is not easy to break this algorithm [26]. RSA executes a public key cryptosystem and the digital signature scheme. RSA was introduced in 1978 when electronic email was expected to release soon, RSA has two important features.

1. Public Key Encryption: with the help of this feature the need of courier to transfer key to another party before sending the actual encrypted data. RSA provides encryption key publically but decryption keys are not public, so only the person who has the correct encryption key can encrypt the data and decrypt the data. Every client can have its own encryption and decryption key. But this must be checked that public key cannot generate the private key.
2. Digital Signatures: the receiver and the sender could mutually authenticate each other this means the sender can check the legitimate receiver and receiver can check the

authenticity of the sender by checking the digital signature of each other. Also sender's decryption key and digital signature can be used to verify the sender. Signature cannot fake.

These features prove very helpful in electronic mail, bank transactions and message transmission for military communication. The security of the RSA is so much authenticate no known attempts to break it [26]. The algorithm follows following steps to generate public key for encryption and private key for decryption [25].

- Select two prime numbers, p=7 and q=17
- P*q=119
- Now calculate (p-1)*(q-1)=(7-1)*(17-1)=6*16=96
- Choose **e** : it's a prime number that is less than 96 and not a factor of 96 e.g. **5**
- Calculate **d** : it must fulfill these two conditions
    - **d** < 96
    - (**d***e)mod96=1
- So **d** =77

Now public key is 5, 119 and private key is 77,119

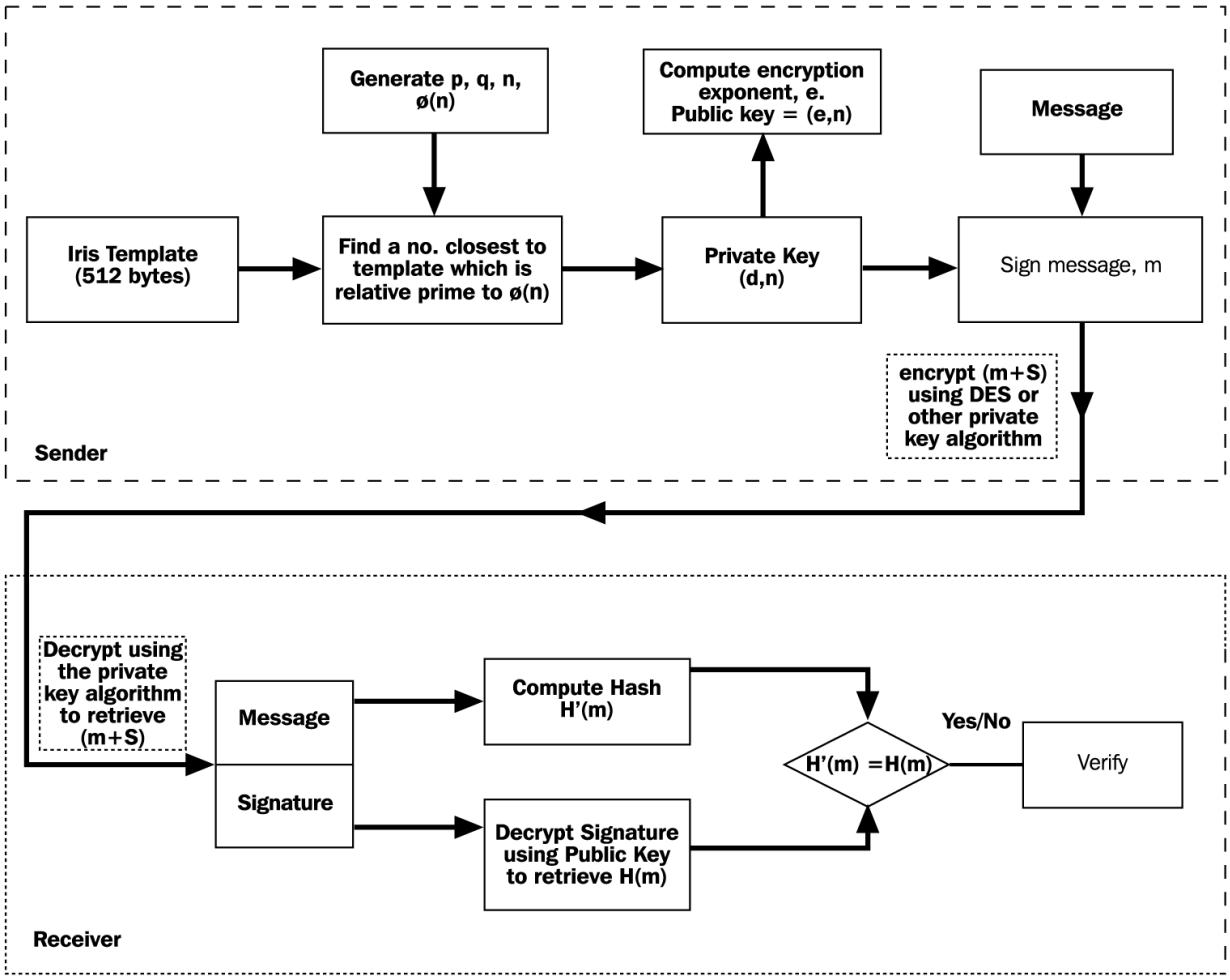


Figure 2.5 RSA Flow Diagram

2.2.1.3 Advance Encryption Standard (AES)

In 1997 NIST organize a completion to get a algorithm that will be more secure and non vulnerable. Two Belgium cryptographers Joan Daemen and Vicent Rijmen developed AES algorithem which was finally approved by NIST in 2001. AES is more provide more security than DES or Triple DES. Detail of AES is discussed in chapter 3. AES has the following steps ,

1. Key Expansion
2. First Round
    - Add round key
3. Rounds
    - Sub Byte
    - Shift Row
    - Mix Columns
    - Add round Key
4. Final Round (No mix colums)
    - Sub Byte
    - Shift row
    - Add round Key

The detail of these steps will be defined in Chapter 3. Strength of AES is depending on key size as key size can be 128 , 256 and 192 bits. 128 bit key is sufficient for encrypted communication but security agencies or defence related department need 256 or 192 bit key size for secure communication

2.2 Authentication

Authentication is method to confirm an entity is legitimate or not. There are many methods of authentication some methods are more secure than others. De-facto standard in authentication which based on the basic authentication method, for example getting a password from a user to check authenticity. Different methods described below. Each has different complexity.

2.2.1 Simple Authentication

In the past, simple user name and password was commonly used for the authentication, still this method is used but this technique is easy to break and old fashioned. But this technique is easy to implement. That's why this method is still popular. A user name and the password are provided by a user, then this information is verified by a database of user name password. This database is stored in that authorized system.

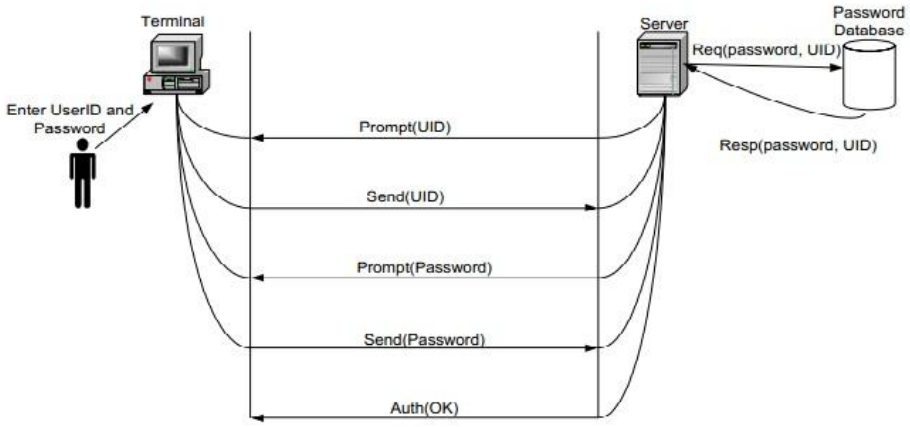


Figure 2.6 Simple Authentication

Mechanism of simple authentication is shown in the figure 2.6. When a user wants to use some service the server ask a user to identify code in the form of user name and password. The server verifies the identification code whether this code is in the database or not. If that code exists in the database , the user got rights to use the services.

In LINUX password can be set with this command /etc/password. Linux takes the username as plain text and password in the hash form (password, Salt). Salt is the random bytes attached with the real password then it calculate the hash of the password to store in the database. This technique makes it more secure against password guessing attack [27].

2.2.2 Digest Authentication

Digest authentication is like simple authentication but this technique is a little bit modified to remove a flaw in the simple authentication. In the simple authentication a password is sent by a user for authentication that is vulnerable but in digest authentication technique password's hash is calculated than hash of the password is sent for verification of the user [27]. Figure 2.7 describes the working of this modified new technique.

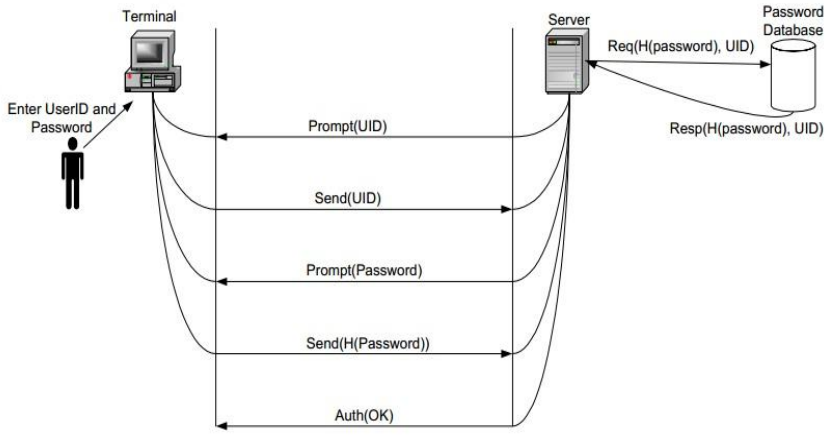


Figure 2.7 Digest Authentication

According to author of RFC 2617 digest authentication is more secure for communication than simple authentication also modified version is available with the key based method.

2.2.3 One Time Password authentication (OTP)

In this technique every time password change for authentication and all the old passwords will not be used again. The server's database store the all passwords list in a secure manner so when one password is used than next password will be valid for next time authentication. This method is more secure against the replay attack. In replay attack an attacker monitors the traffic and easily cracks the username password. A password generator in the OTP properly programmed so it never repeats the generated passwords [28].

2.2.4 Biometric authentication

In the Biometric authentication a biometric data is calculated through any biometric method like finger print scanning, Iris scanning, palm scanning, Pigment of voiceprint etc. The beauty of this technique is that even if an eavesdropper provides very similar biometric data for authentication even then this method does not allow the eavesdropper to sign in.

Biometrics is widely used by security agencies. Even laptops passwords, car security gate security can be operated with biometrics. According to a survey people like different techniques of measuring biometrics data.

Technique	Effectiveness of techniques	Acceptance of People
Palm Scan	1	6
Iris Scan	2	1
Retinal Scan	3	7
Fingerprint	4	5
Voice Id	5	3
Facial Recognition	6	4
Signature Dynamics	7	2

Table 2.1. Biometric Data measurement Techniques Survey

2.3 Symmetric Key Based Cryptographic Authentication

Joining different methods which are already defined joined to get a strong authentication method or for final authentication. A strong authentication protocol can be defined by using predefined symmetric cryptography keys. A lot of methods are defined in ISO/IEC for entity authentication. Two major classes of cryptography protocols are depended upon synchronization of time. It means when two parties want to communicate with each other there computer system must be

timely synchronized. This synchronization provides the required security for communication in few steps. This synchronization is obtained by generating a nonce. Nonce is a random numbers which is generated by the computer systems of the communicating parties. This feature makes it more secure against replay attack.

2.3.1 ISO/IEC 9798-2 Timestamp Based Unilateral Authentication

An authentication of a user can be obtained in few steps by synchronizing two communication nodes as shown in figure 2.8. First of all timestamp and key is exchanged between communicating parties. After exchanging this information both nodes will be synchronized. Node B can confirm the legality of the authenticator by confirming the timestamp that is identity of node B, with the help of these conditions Node B can verify the legality of the node A.

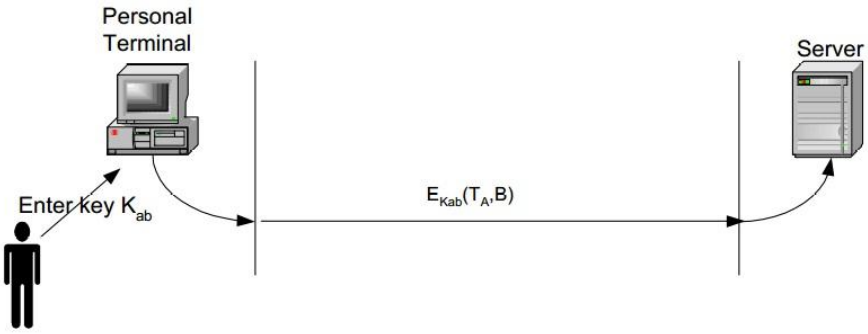


Figure 2.8 Timestamp Based Unilateral Authentication

2.3.2 ISO/IEC 9798-2 Nonce Based Mutual Authentication

Mutual authentication means both communicating parties can check the authenticity of each other. In the mutual authentication method of the ISO/IEC 9798-2 synchronization between the computers of the communicating parties is not necessary because a random number (Nonce) fulfils the requirements of mutual authentication.

According to figure 2.9 key is exchanged with each other by communicating parties, then node B can verify node A by checking N_B and node A can check the validity of node B by matching the received nonce N_A with sent nonce N_A [29].

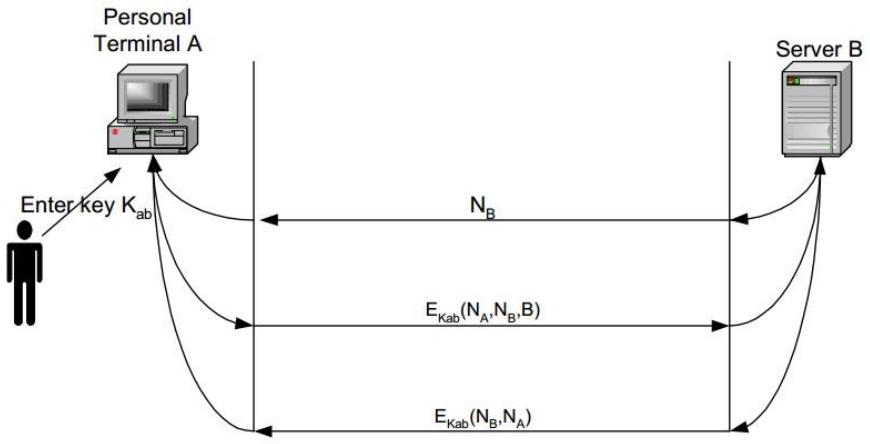


Figure 2.9 ISO/IEC 9798-2 Nonce Based Mutual Authentication

2.3.3 Rapid Development Authentication protocol

In this section Rapid Development Authentication protocol (RDAP) is discussed in detail. In this thesis chapter 3the proposed algorithm is defined to improve the efficiency of the protocols like RDAP and later on we compare the efficiency of RDAP with the proposed algorithm under section 3.5.4.

RDAP is a mutual authentication protocol that guarantees a secure connection to those devices which completely satisfy all the steps of RDAP. A session key is generated which prevents MITM and fake data injection attack. RDAP consist of three phases scanning, mutual authentication and secure connection establishment. The first phase is scanning. UE scan the QR code which is displayed by programmable LCD of the femtocell. 2D bar code contains secret keys (k*a*, k*e*) for encryption. k*a* and k*e* are unique for every device and their size is 128-bit secret key for encryption and 128-bit for authentication respectively [1]. Femtocell displays a second QR code on its LCD so every user has unique encoding keys. After scanning phase, mutual authentication phase starts. RDAP uses Diffie-Hellman (DH) as key exchange mechanism. Generally one component (base exponent) of DH is encrypted with the AES-CBC to avoid a MITM attack; also SHA-1 is used to avoid tempering attack. Femtocell and the UE exchange the following information for mutual authentication:

$$F \rightarrow M: \text{ request identity} \qquad (1)$$

Femtocell sends a request to Mobile for its ID that is used for Access Control List (ACL).

$$M \rightarrow F: \quad IDm, g, \beta, \{A\}_{ke}, nm,$$

$$hka\ (IDm, ||g||\beta\ \{A\}_{ke}\ ||nm \qquad (2)$$

Mobile Responded and generate 1024 bits random number "a" (a for DH) and "n*m*" (nonce is generated once as the unique number of that equipment). Mobile also generates "A". Mobile sends following information to femtocell: Id, g, β, n*m*, {A}k*e*, and Hash of all these with key "k*a*".

$$F \rightarrow M: B, \{nf||nm\}k, hka(B||\{nf||nm\}k) \qquad (3)$$

Femtocell checks the white list for mobile's id, if the id is present in it, protocol will continue otherwise it will stop and dismiss the connection. On the other hand femtocell generates "b" (b of DH) and nonce "n*f*". Femtocell also decrypt {A}k*e*, and generate encryption key "K". Femtocell send to mobile: B, {n*f* || n*m*} K, and Hash of all with key "K*a*".

$$M \rightarrow F: \{nf\}k, hka(\{nf\}k) \qquad (4)$$

The mobile sends to femtocell: $\{nf\}k$ and Hash of all with key "K*a*". Last phase of the RDAP is to secure connection establishment, after the mutual authentication the mobile device and femtocell establish a secure link which grants data protection and reliability.

Name	Description
M	Mobile Device
F	Femtocell
CSG	Close scriber group
n*m*,n*f*	Mobile Nonce, Femtocell ’s Nonce
K*e*	Mobile’s key for encryption
K*a*	Mobile’s secret key for SHA-1
Hk(m)	HMAC of message m with secret key K
||	Concatenation
g	Base exponent
β	Modulus
a	Mobile’s random number
b	Femtocell’s random number
A	A=g^a mod β
B	B=g^b mod β
{}k	K=g^(a+b) mod β

Table 2.2. Notation

2.3.3.1Quick Response (QR)

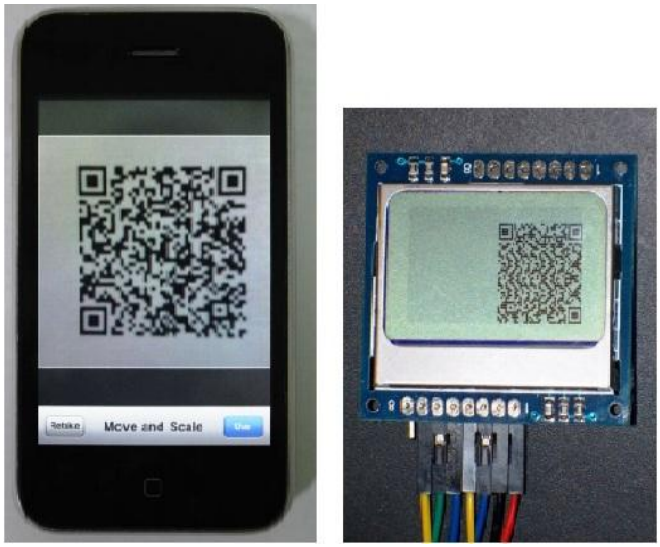
QR is a two dimensional bar code that is developed by Denso Wave. The QR codes are easier to decode due to their unique positioning pattern. QR carries information in vertical and horizontal direction at the same time. Maximum 20 characters are stored in the conventional bar codes, but QR code is capable to store much more data than the simple barcodes. The detailed information is given in table 3. QR Code contains 3 position detection patterns which are located at corners of the QR code. This feature makes it easy for device to decode the data because even if the user rotates the picture the QR codes can be decoded correctly. QR code has a unique feature, the information stored in it can be further divided into 16 more QR codes and they can be again combined to form a single QR code.

Numeric Only	7,089 Characters	0,1,2,3,4,5,6…
Alphanumeric	4,296 Characters	0-9, A-Z, Space,
Binary	2,953 Characters	8 Bit Bytes
Kanji/Kana	1,817 Characters	Japanese Language words

Table 2.3 QR Code Data Capacity

2.3.3.2 Visual Channel

The idea of visual channel is derived from the previous protocol that mutual authentication and a secure channel is planned for communication. In classical techniques password entry approach is used that is risky for security [9], [32]. Along with all such ideas visual channel is user friendly and protected channel to communicate with user equipment like mobile phones. LCD of femtocell displays the keys in encrypted form (2D barcode) that are read by the mobile camera as shown in figure 2.10 [5]. This advance approach of using visual channel for communication is used by many protocols [18], [33]. Encrypted data that should be publicly available for authorized user in treacherous environment can be provided by using visual channel.



(a) (b)

Figure.2.10: (a) QR code captured by the iPhone decoder (b) Barcode on LCD display

2.4 Literature Survey

H. Yao, and H. Li-Wei said that in [5] that femtocell has three access modes, Open access mode, Close access mode and Hybrid access mode. In open access mode all UEs can use the services; there is no need to authenticate any user. In Close access mode only legitimate user can use the services after authentication. A white list is maintained by management to check the identity of legal UE identity. Hybrid access mode is the mixture of Open and Close access mode because all users are allowed to use the services in this access mode but under some restrictions. These access modes have some limitations, in close access mode a guest clients can never access the services, however, it is hard to implement restrictions in Open and Hybrid access mode..Fake or rouge femtocells can be installed to spoof the identity of a legal UE.

S.F.Hassan said in [6] that femtocell is low power base station used for indoor coverage in small areas like offices, schools so femtocell can be called as Small-Office-Home-Office (SOHO). SOHO provides voice and broadband services. Femtocell Access Point (FAP) connects with the cellular network via an IP network to provide services. Femtocell can reduce the load of traffic on the base station and increase the signal strength even each end user can access the full signal strength without having to penetrate through urban structures like buildings.

R. Housley explained that IP based networks generally use X.509 certificates [7]. The serial number of the femtocell is hidden inside the trusted platform module; which is a hardware component designed by the manufacture. No one can change the information embedded in this hardware component. Only manufacture and operator know the serial number and when a client installs a femtocell to use then only public key and serial number are used together for communication. But if the serial number is compromised then it is easy to change the white list of the femtocell.

Z. Jie, and D. L. R. Guillaume stated that [8] SIM card can also be used by Femtocell Access Point (FAP) to authenticate a user. A SIM is bedded in the femtocell which contains the data (Identification code or Secret identity) but the spoof identity attack can easily launch on this methodology.

In [9] S. Laur, and K. Nyberg proposed a method by using a visual channel for communication is a safe and trustworthy way. A programmable LCD is connected with the femtocell which

displays Quick Response code (QR). This QR code contains the public keys used for mutual authentication between UE and the femtocell. User take a picture from the LCD attached with femtocell to get public keys, but in this scheme there is no record which key is assign to which user because LCD attached with femtocell change the code after every 5 second, so if identity of the user is compromised then public key can be scanned and various attacks can be launched

G. Koien and V. Oleshchuk [17] in all classical techniques a trust is established between the mobile devices and femtocells. A code or some password is typed by the user to exchange authentication information but every time typing the same password is a vulnerable, so this scheme is not so much secure.

According to J. M. McCune et.al [18] exchange the encryption keys through visual channel is user friendly and protected channel to communicate with user equipment like mobile phones. LCD of femtocell displays the keys in encrypted form (2D barcode) that are read by the mobile camera, but this scheme is hardware specific that means cell must be capable to decode the 2D barcodes.

B, Igros at al [19] stated that security and privacy for the mobile network is held solely by the core network . This is the beneficial beneficial as it ensure the trust relationship between the subscriber and the home network also the dynamic and the mobile devices controlled action that could be guaranteed a better protection. Main issues for the mobile devices are authentication and the location tracking by using femtocell technology, also by using contextual information such as node density, device speed and mobility pattern, mobile device triggered identity can reduce the risk of being tracked

In [20] Z. Liping and Z. Yujuan explained that trustee-boxes storing the private key are introduced to meet the roaming users accessing to the private key in the cross-regions; Making use of the characteristics of threshold technology, the divided private key slices are encrypted and stored into then trustee-boxes, and the whole private key is restructured as long as k trustee-boxes are effective. By cross-certificating with the strengthen servers a user is verified as a legal user when it accesses its own private key. The secure performance of storing and accessing private keys is improved in the scheme. At the same time, the legal users are authenticated by the system. But this protocol is time taking for low computation power equipments.

L. Choa, et al [21] stated that to overcome the man-in-the-middle attack can be handled by using the modified AKD protocol in which a number is set every time the packet is exchange the fix num is decreased n-1 ratio. So if the encryption key is compromised or attacker wants to launch any attack, attacker fails to compromise the current number because the attacker does not have any information about the number but two nodes accept or send packet according to n-1 number. "n" is initially set that is usually a large number. This algorithm is light weight but various attacks can be launched easily. The light weight algorithm is important but authentication of users is also important.

M. Abdalla et al [22] algebraic complexity of S8 AES S-box, is remains the same as AES S-box, by applying permutations on S-box which does not effect the algebraic complexity of S-box, so by modifying or making S8 S-box more complex can make AES more complex.

CHAPTER-3

DESCRIPTION OF AES

3.1 Advance Encryption Standard

In this chapter AES and entire standard of AES is briefly discussed. Block cipher is the standard of AES and this design principle called Substitution permutation network [30]. AES support 3 types of keys: 128 192 and 256 bits. Name of the AES changes with the key size as AES-128 AES-192 and AES-192. Normally the length of the keys is indicated with sign N_k . If we use a specific type of AES with key size N_k then the size of the results at every stage will be N_k. The block size is denoted with sign N_B and the number of AES rounds is represented by N_R . N_R can be calculated by measuring the key size of AES. Each type of AES has a specific number of rounds as AES-128 has 10 rounds AES-192 has 12 rounds and AES-256 has 14 rounds. The Table 3.1 shows the $N_{B,}$ N_K and N_R for the AES.

Type	Block size (N_B)	Key Length (N_K)	Number of Rounds (N_R)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

Table 3.1 AES types

The AES encryption process can also defines in form of flow chart as shown in figure 3.1. with help of cloud computing technology it is so easy to break the DES key in few seconds. But there need 149 thousand billion years are required to crack the 128-bit AES key. According to MIT University report as research is going on to increase the processing speed of cloud computing. However, the AES is still secure for next 109 years.

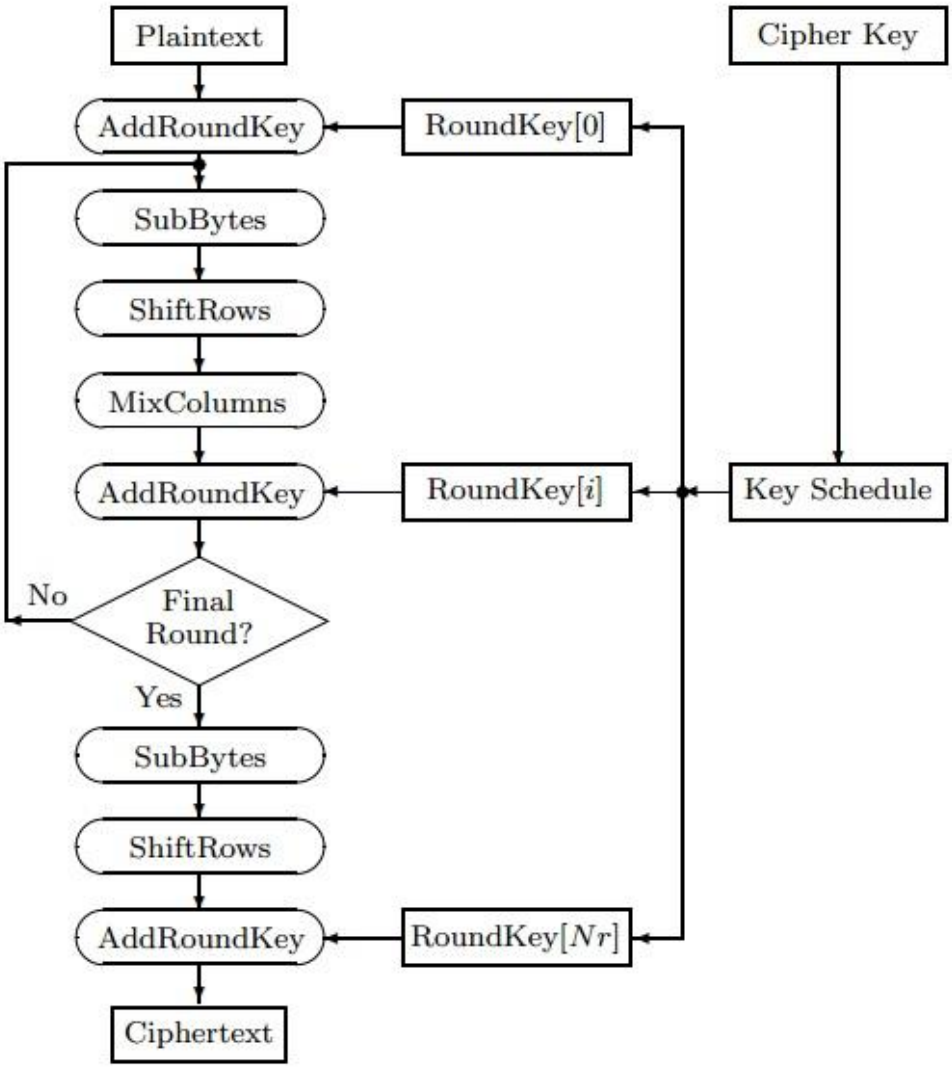


Figure 3.2 AES Flow Chart

Now further in this chapter Encoding Mechanism, Decoding mechanism and Attacks on the AES will be discussed.

3.2 Encoding

For encoding a plain text is provided as input a key is used to encrypt the data. The plain text is written in the form of 4 rows and 4 columns (4*4 matrix). The result at every stage is called a state. First N_R is implemented to the 4*4 matrix then that matrix puts in round step of AES. Every round has four transformations

1. Sub Byte Transformation (SB)
2. Shift Rows (SR)
3. Mix Columns (MC)
4. Add Round Key (ARK)

At the final round Mix Column transformation is not performed. The pseudo code of AES encoding is described below [31].

1. Byte s[4, N_B]
2. S=in
3. Add Round Key (s,w[0,N_B-1])
4. For round =1 to NR-1 do
    a. Sub Byte(s)
    b. Shift Rows(s)
    c. Mix column
    d. Add Round key(s,w[round*N_B(round+1)*N_B-1])
5. End for
    a. Sub Byte(s)
    b. Shift Rows(s)
    c. Add Round key(s ,w[round*N_B(round+1)*N_B-1])
6. Out = s

Now let's discuss every transformation in detail.

3.2.1 The Sub Byte Transformation

A non linear byte substitution result can be obtained by using S-box in Sub Byte transformation step. Block is substitute byte by byte in this step as shown in the figure 3.2 and S box is shown in figure 3.3

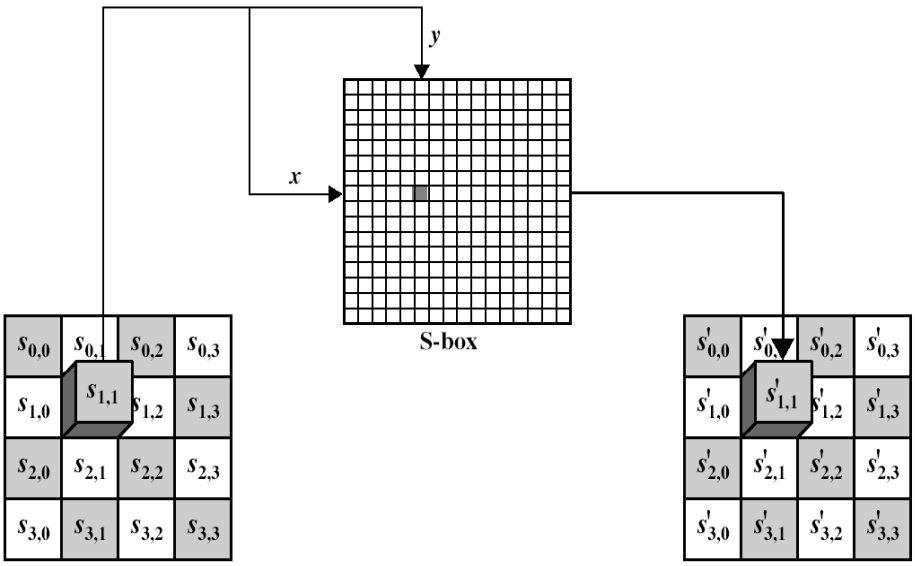


Figure 3.2 Sub Byte transformation step

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3.3 S-BOX

3.2.2 Shift Row Transformation

In this transformation the bytes of all rows except row are cyclically shifted over special numbers of bytes. The first row remains as it is. The number of shifts depends on the numbers of rows as in figure 3.4 there are four rows so there will 3 shifts the first row has1 shift , 2nd row has 2 shifts and finally the 3rd has three shifts.

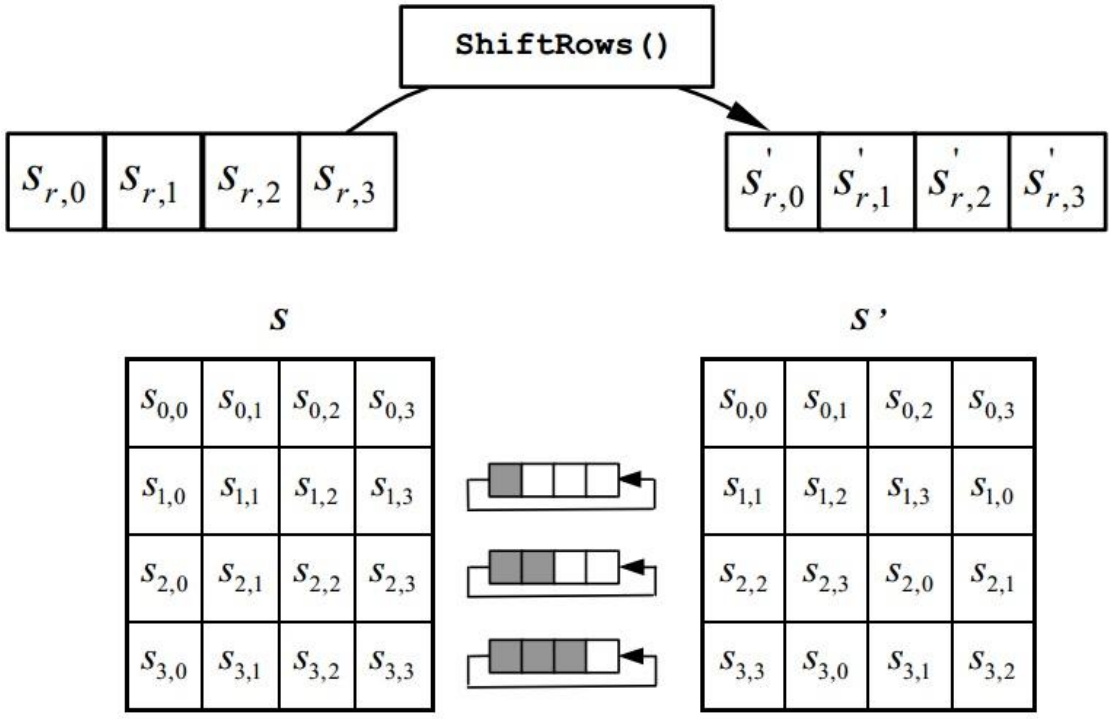


Figure 3.4 Shift Row Transformation

In this step actually the Bytes moves towards the lower position in the row. Rows shift in left side as if "n" numbers of row then left shifts will be "n-1". For the AES-256 2nd, 3rd and 4th rows will be shifted left. And 1st row remains unchanged. This scheme is only used for the Rijndael cipher AES-256. This type of design has optimal diffusion and additional diffusion results. Optimal diffusion is necessary to block attacks like linear and differential cryptanalysis.

3.2.3 The Mix Column Transformation

A linear transformation is applied to the state in Mix Column transformation and it effects column by column. For AES-128 matrix "A" is used that is shown in figure 3.5. This multiplication can be explained as multiplication with one means byte as it is. Multiply by two means left shift and multiply by three means left shift than XOR it with initial state values. If the result greater than 0*FF then again XOR it with 0*11B but it's a conditional step.

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix}$$

Figure 3.5 For AES-128

Generally each column is multiply and results are stored on another column to form the new state for the add round key as described below in figure 3.6

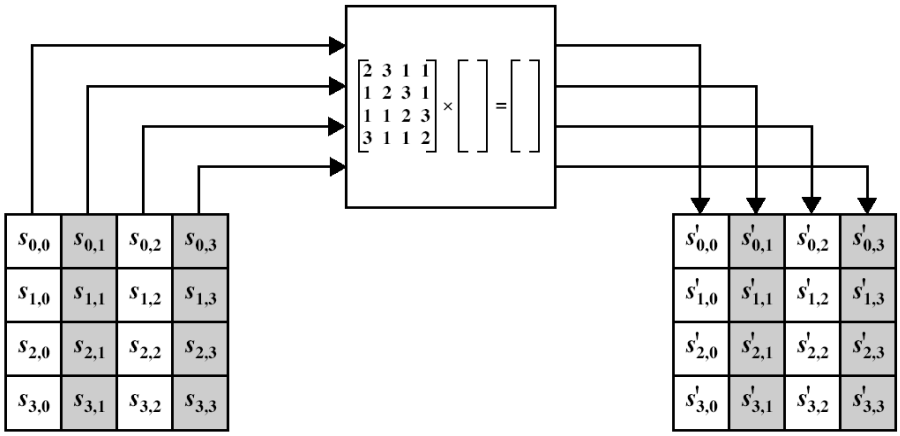


Figure 3.6 Shift Column Transformation

3.2.4 Add Round Key Transformation

A bitwise XOR operation is performed in add key transformation. A key schedule scheme is used to generate a key which is used in this state. The key schedule produces same size key as the state. The key schedule scheme will be described later in this chapter. The key schedule can be understood easily with this example that is shown in the figure 3.7. Let's assume that figure 3.7 (a) is stated after the Mix Column transformation step and figure 3.7 (b) is the key for this round. Each column will be bit wise XOR with the key schedule. As shown in the figure 3.8.

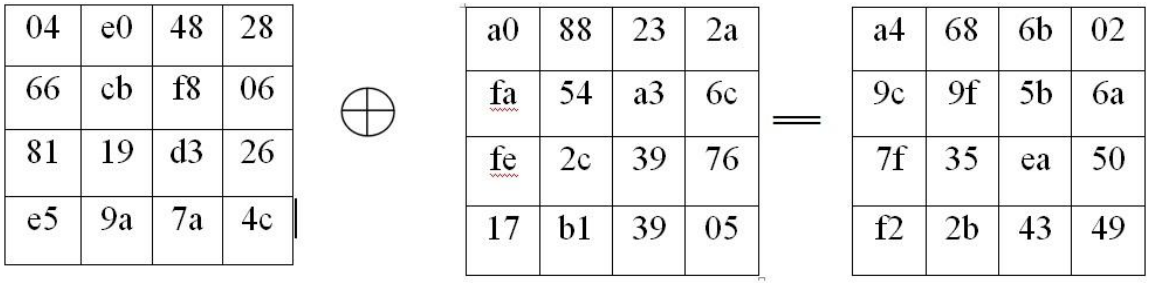


Figure 3.7 Add Round Key Transformation

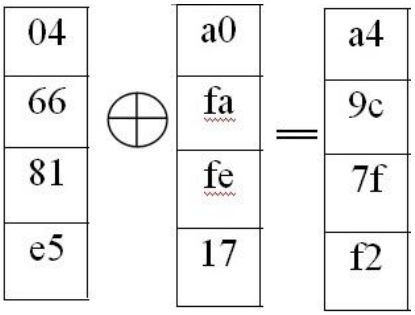


Figure 3.8 Bitwise Operation

Figure 3.8 shows the effect of add round key on the state. In the same way all the columns are XOR to prepare the Mix column transformation state.

3.3 DECODING

In decoding process, an encoded text and the key used as input and the out is plain text as a result. The four steps Sub Bytes, Shift Rows, Mix Columns and Add Round Key, all used in a reverse arrangement to get results. All the steps used in the encryption process are called Inv Sub

Byte, Inv Shift Rows and Inv Mix columns. The pseudo code of the AES decryption process is described below. All the parameters are as described before in section 3.2

1. Bye s[4,N_B]
2. S = in
3. Add Round Key
4. Inv Shift Rows
5. Inv Sub Byte
6. For round = N_R – 1 to 1 do
    a. Inv Shift Rows
    b. Inv Sub Bytes
    c. Add Round key (s, w [round*N_B(round+1)*N_B - 1])
    d. Inv Mix Columns
7. End for
8. Add Round Key(s, w [0,N_B - 1])
9. Out = s

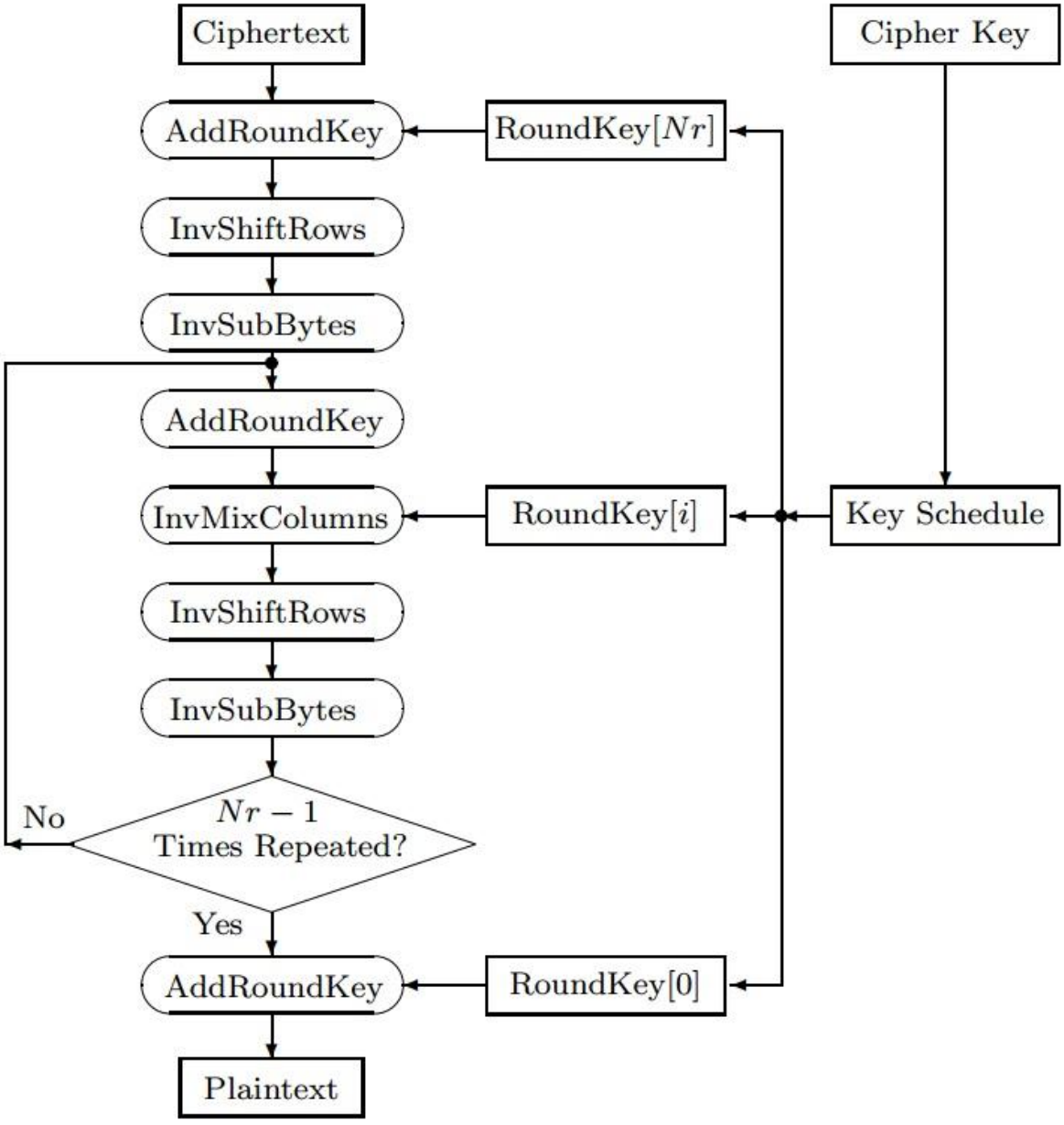


Figure 3.9 AES Decoding Process

3.3.1 Generation of Inverse S-Box

Just by using again the S-box formula inverse of S-box can be generated or simply by inverting the value of S-box as shown in the figure 3.10 and inverse S box can be generated with it.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3.10 S- box highlighted values for Inverse S-box

Now at the value of “52” in s-box will be in “00” in inverse S-box

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 3.11 Inverse S-Box

3.3.2 Key Scheduling for AES

To expand AES-128 short key for in many split round keys. This scheme is called Rijnjael key Schedule. RCON is a fixed value table used to expand the key.

01	02	04	08	10	20	8D	1b	36	6C
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Table 3.2 RCON

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Figure 3.12 Key for AES round 1

Last column of the AES key is called Root column we take that column and shift it top to bottom.

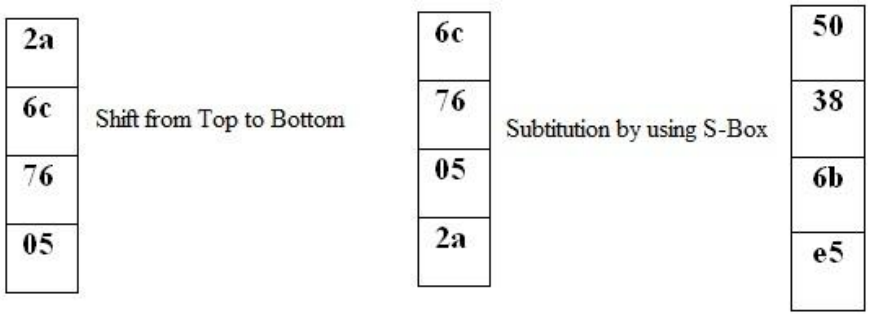


Figure 3.13 key Scheduling Step 1

Now substitute every element of new shifted column by using S-Box. Than XOR substitute column, first column of the key and the first column of the RCON table.

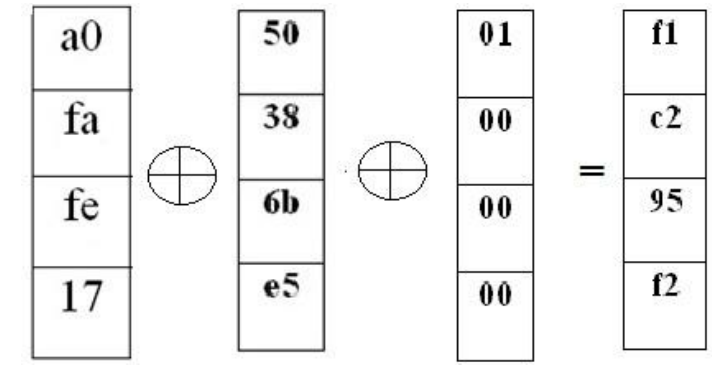


Figure 3.14 First column of new key scheduling

Figure 3.14 (d) will be the first column of the key for 2nd round.

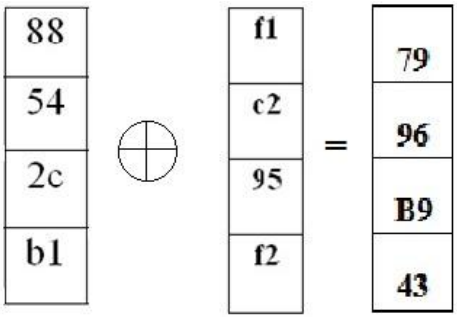


Figure 3.15 2nd column of key for AES Round 2

Now using the same method key for each round of AES can be generated.

3.4 Proposed Algorithm for Mutual Authentication Using S_8-S box

In this section a proposed algorithm is described for the mutual authentication of mobile and the femtocell using S8-Sbox.

3.4.1 Generation of modified S_8-Sbox

In this proposed method a symmetric group S_8 is applied on AES standard S-box then by using that new S-box 40320^{40320} keys can be constructed for the AES [31]. This feature makes this proposed algorithm very strong against many attacks.

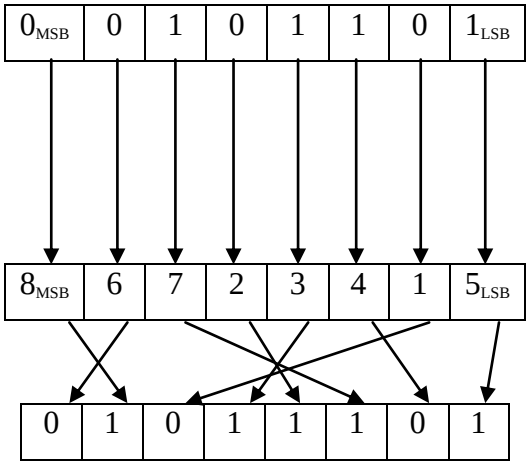
Every element in the S-box is permutated to generated new box. Let's take an example of permutation of a single element of s-box. A key (Ks) of size 64 bits is chosen for the permutation. Let's assume that the key for S-box (K_s) is

8_{MSB}	6	7	2	3	4	1	5_{LSB}

If the first element of the S-box is "45" then binary of it will be

0_{MSB}	0	1	0	1	1	0	1_{LSB}

Now for the first element of the new S_8 S-box every bit shifted as the K_S



Now the new combination of binary's decimal is "93". So the first element of the new S_8 S-box will be "93". Similarly all the elements are permutated and new S-box is created for the AES.

3.4.2 Novel Mutual Authentication Protocol

In this section, we present a novel algorithm to provide mutual authentication between the femtocell and the mobile device. The proposed algorithm guarantees secure communication with the authenticated femtocell and defend against all of the well known attacks like DOS, Masquerade, Backhaul and Sybil attack. The proposed algorithm facilitates multiple mobile devices at a time. Table 3.3 contains all the notations and each step of our algorithm is summarized in table 3.4.

The proposed algorithm is divided into two phases. First phase is the Key Exchange phase, then the mobile device and the femtocell undergo the mutual authentication phase and finally, in the last phase safe link is established. In this proposed algorithm we have the assumption that each mobile device has the necessary software to execute our algorithm. We have assumed that each user has the specific S8 S-box of authenticated femtocell stored in it before authentication so that there will be no extra overhead. Each step of our proposed algorithm is described as follows

Name	Description
M	Mobile Device
F	Femtocell
CSG	Close scriber group
r_a	Random number to identify keys
n_m	Mobile's random number
n_f	Femtocell's random number
k_e	Mobile's key for encryption
k_s	Mobile's key for S8 S-box generation

Table 3.3. Notations

3.4.2.1 Exchange key Phase

The proposed algorithm begins with every mobile device by generating "a" for Deffie Helman, than send it to femtocell

$$A = g\hat{}a \; Mod \; \beta \qquad (1)$$

Then Femtocell generates "b" and produce B as

$$B = g\hat{}b \; Mod \; \beta \qquad (2)$$

This step generates "K" that is used to encrypt the keys for S_8 S-box and for AES.

$$K = g\hat{}(a * b) \; Mod \; \beta \qquad (3)$$

3.4.2.2 Mutual Authentication Phase

Mobile device after obtaining the secret keys and the random number generates a S-box and connects with the femtocell. In this thesis the details of this connected is not discussed. The steps of mutual authentication phase are described as follows

$$\mathrm{F} \rightarrow \mathrm{M}: \text{ request identity and } \mathrm{r_a} \qquad (1)$$

F will ask the M to send its identity and the random number $\mathrm{r_a}$.

$$\mathrm{M} \rightarrow \mathrm{F}: \quad \mathrm{r_a}, (\mathrm{ID_m}, \mathrm{n_m})_{\mathrm{k_e},\mathrm{k_s}} \qquad (2)$$

M will send the random number $\mathrm{r_a}$ and encrypt its identity and a random number $\mathrm{n_m}$ generated by the mobile for mutual authentication and to avoid man in the middle attack. F after receiving the message from M, use the random number $\mathrm{r_a}$ to look for the keys against it in its list and after generating the S8 S-box and its inverse using $\mathrm{k_s}$ and then decrypts the identity of M. This identity is matched with the CSG maintained in the femtocell, if the result is negative then that mobile device is not given access and the connection is disconnected immediately.

$$\mathrm{F} \rightarrow \mathrm{M}: \quad (\mathrm{n_m}, \mathrm{n_f}, \mathrm{k_{s'}})_{\mathrm{k_e},\mathrm{k_s}} \qquad (3)$$

Mobile devices whose identities match with the CSG will send random numbers nm, $\mathrm{n_f}$ and a 64 bit key $k_{s'}$ for mutual authentication and to generate a new S-box. M after receiving this message decrypts it and match $\mathrm{n_m}$ with the random number it has generated earlier. If these two numbers

match then M is sure that it connected with the authenticated femtocell otherwise it will not communicate.

$$M \rightarrow F: \quad (n_f)_{k_e, k_{s'}} \qquad (4)$$

M will generate a new S-box using $k_{s'}$ and send back F the random number n_f encrypted with k_e to complete the authentication process.

3.4.2.3 Safe Link Establishment Phase

Femtocell receiving the random number n_f to match it with the number stored in it, if they match F will establish a safe link with M.

Key Exchange Phase	
M	:generate a, then
	:A = g^a Mod β
M→F	:A, g , β, h(A)
F→M	:check received message
	: generate b than calculate
	: K= g^(a*b) Mod β
	By using B = g^b Mod β A = g^a Mod β
F→M	: B, ($k_e \| k_s \| r_a$)K
Mutual Authentication Phase	
F → M	:request ID_m
M → F	:r_a, (ID_m, n_m)$_{k_e,k_s}$

F	:Verify the received message;
	if verified ,carry on
	if (IDm is not in CSG)
	protocol suspended
	(discard M)
	else
	"n_f" is generated by F

F → M	:(n_m, n_f, $k_{s'}$)$_{k_e,k_s}$
M	: Verify n_m if success, continues: Generate new S8 S-box
M → F	: (n_f)$_{k_e,k_{s'}}$
F	: Verify n_f if success:
"Authentication successful"	
	else QUIT

Table 3.4 Mutual Authentication Protocol Using S8-Sbox

3.5 Security Analysis of proposed Algorithm and RDAP and Critical Analysis of RDAP

Femtocell users are very concerned about communication security and privacy. In this section we will discuss the security threats and how the proposed protocol behaves when an attacker tries to attack the femtocell network. Femtocells are normally used in open access mode, any UE can use the services and access the core network, so a secure and non vulnerable environment is necessary to ensure the privacy of every UE and avoid an attacker to act passively. A rouge femtocell can be installed by the eavesdropper to get the identity of legitimate users. Femtocell sends the user data over the internet so it can be attacked actively or passively.

3.5.1 Man in the Middle Attack (MITM)

The proposed algorithm is secure against MITM attack because 'ID_m' is encrypted and the intruder does not know the secret keys. Guessing the secret keys is almost impossible because, first, the proposed algorithm uses two secret keys of length 128 and 64 bits, secondly, for a particular random number there is a specific pair of secret keys. In this novel scheme all data is encrypted with k_e and $k_{s'}$. $k_{s'}$ is used to permutate S-box and k_e is used in AES to encrypt data. It is impossible to guess the right keys for an attacker because there are 40320^{40320} key combination to generate S8 S-box, and 2^{128} combinations for encryption

3.5.2 DoS and Sybil attack

The vulnerability under Sybil and DoS attacks comes from the fact that ME sends (ID_m, g, β, n_m) without encryption and femtocell has no database of keys it is generated in the form of 2D bar codes. To remove this weakness (ID_m, n_m) are send encrypted along with the femtocell keep track of the keys it is generating by assigning a random number r_a to these keys. If a malicious subscriber uses Dos attack on the femtocell it will be detected at step 1 of our proposed protocol as they do not have the right keys against the specific random number. Sybil attack will be detected at step1, as the identity of the ME is encrypted and only users who get their keys by Deffie Helman method.

3.5.3 Masquerade Attack

Attacker installs a fake femtocell near the legal one. Fake femtocell then starts working as the legal femtocell. When a legitimate user connects with fake femtocell, its identity and personal information are compromised. In this protocol only legal UE has the specific S-box of legitimate femtocell, it is impossible for the fake femtocell to get the identity as it is encrypted by S-box. A random number of femtocell n_f is send to UE for mutual authentication so Masquerade attack is not possible.

3.5.4 Critical Analysis of RDAP

In this section, RDAP architecture and its behaviour against various attacks are critically analysed. RDAP is relying on physical contact between UE and femtocell to star mutual authentication. Physical channel is more secure and reliable to issue encryption keys. In classical protocol 160-bit HMAC-SHA1 key is used with every packet to make communication more secure. DH cryptography is used so 1024-bit "a" and "b" is generated by UE and femtocell respectively. The entire encryption bits overload the equipment and the session key that is generated by 1024-bit DH also decrease the performance on a common UE [9]. "g" is *.pem file format, so it's hard to be device specific to use a protocol, because practically RDAP is tested on the iPhone platform, so there is need to develop a protocol that more secure and interoperable.

3.5.4.1 Sybil & DOS Attack:

Malicious attacker sends so many fake identity packets to femtocell to make it busy or for DOS attack. Disorder communication or complete denial of services to legal client is called DOS attack. The attacker does not act actively in such attacks. RDAP suggest CSG_id and HMAC-SHA-1 techniques to handle these attacks, but if visual code is compromised than encryption keys will be decrypted by the eavesdropper and femtocell will fail to identify the legitimate user because IDm is sniffed. There is no way to check the attacker after authentication phase.

3.5.4.2 Eavesdropping & Injecting Attack

In this attack the attacker acts actively. All the information or some part of the information is altered by the eavesdropper [8]. RDAP provide mutual authentication but when a user connected with femtocell it authenticates it by matching nf. If a fake femtocell is installed near the legal one then all the communication will be started from that rouge femtocell. The attacker can easily get the IDm of that mobile and can launch any attack.

3.5.4.3 Man in the Middle Attack

Attacker acts actively in this attack, all the communication between the UE and femtocell can be disrupted and fake information can be injected, as described above the attacker can easily get the IDm during the communication of user with legal femtocell then the attacker can launch a MITM attack, so this protocol fails to handle this attack. Security of RDAP stands upon ke, if the attacker guesses the correct ke then MITM attack will be successful.

3.5.4.4 Password guessing Attack

According to RDAP the attacker tries to guess ke to generate session Key K, but ke is publically available because visual channel barcodes provides ka and ke. There is no way to confirm which keys are generated against which barcode, so if IDm is sniffed then any keys will start the authentication phase and femtocell consider that UE legitimate.

3.5.4.5 Tracing Attack

In tracing attack attacker can construct the next generated key for the encryption and securing the previous communication data [13] but the keys are publically available and CSG_id just checks IDm for authentication. IDm, β, nm can easily sniffed by using data sniffing tools. “g” is 2 and this value is fixed in RDAP [1], so mutual authentication is at risk by using classical RDAP.

CHAPTER-4

SIMULATION AND RESULT DISCUSION

In this chapter all the simulation is step by step is discussed. A result of every step is compared with the Rapid Development protocol [5]. The authentication of the femtocell and mobile device is key feature that plays an impotent role to create a secure communication channel. As shown in the figure 4.1 the femtocell is deployed inside a covered area where signals may or may not be strong. To full fill signals deficiency femtocell is the demand of the hour.

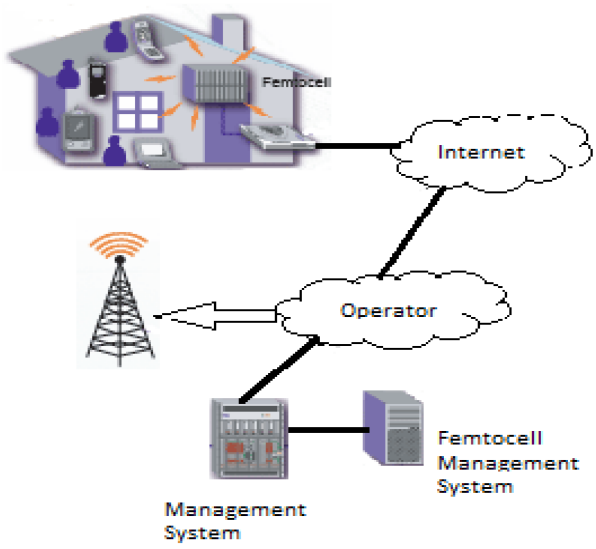


Figure 4.1 Femtocell Deployment Structure

4.1Key Exchange Phase

The proposed solution is discussed in detail in the chapter 3. It basically has a key exchange phase and the authentication phase. As shown in the flow diagram of the key exchange phase mobile and the femtocell use the Deffie Helman‘s key exchange method.

Each steps flow diagram and the simulation results are defined in this chapter. The first step is defined in figure 4.2(a)and 4.2(b).

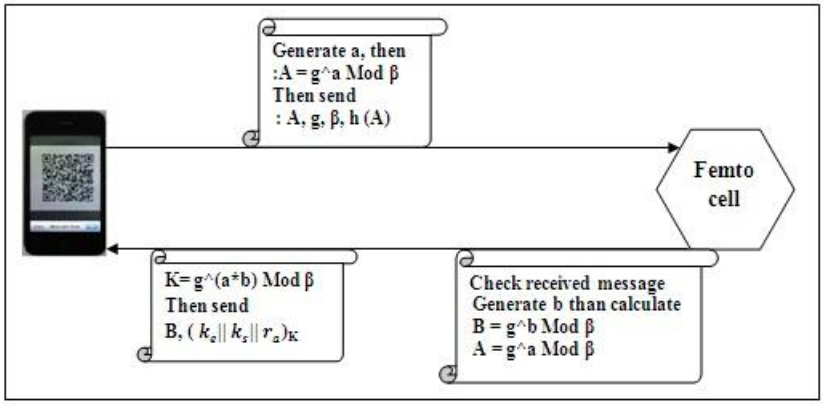


Figure 4.2 (a) Key exchange Phase Model Diagram

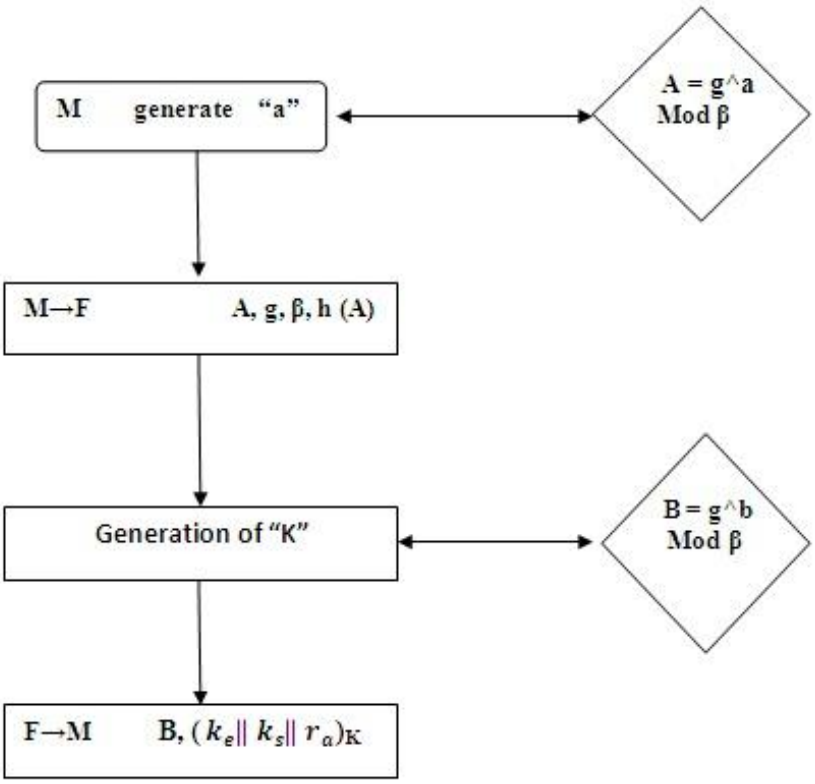


Figure 4.2 (b) Key exchange Phase Model Diagram

4.1.1 Step 1

In this step Deffie Helman key exchange method is used. Mobile device sends a request, and send "β", "g" and "A" which is calculated by a formula shown in table 3.3. A random number (n_m) is generated by mobile but not send to femtocell.

Figure 4.3 (a) Key Exchange Phase output

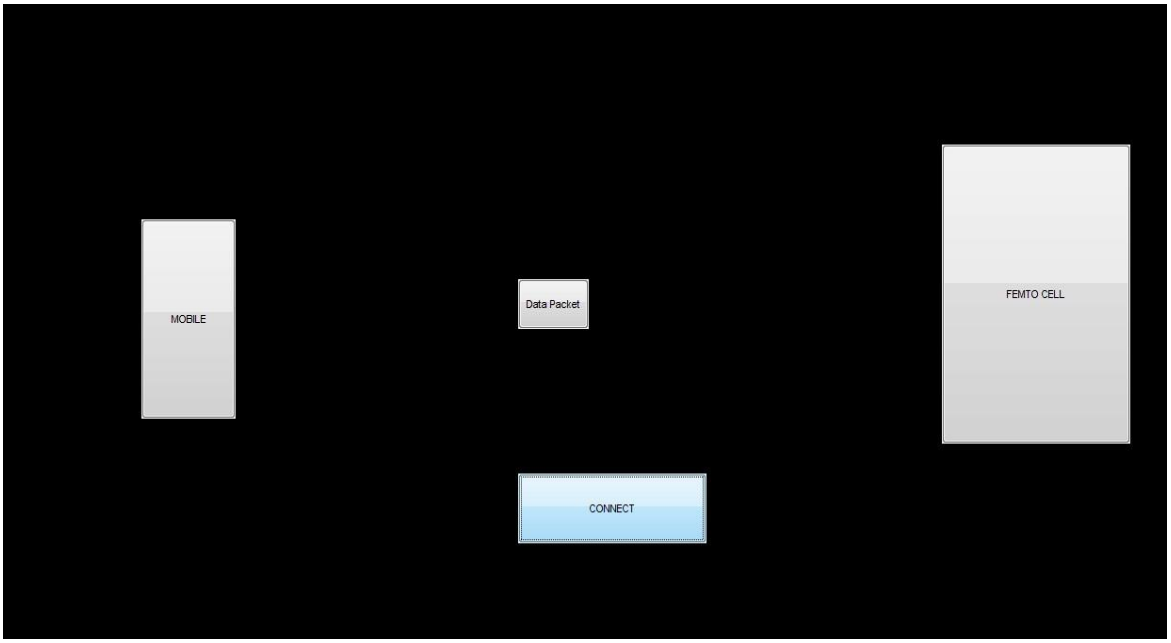


Figure 4.4 Key Exchange Phase GUI

4.2 Mutual Authentication Phase

In the authentication phase femtocell and the mobile both has exchanged the encryption keys now both devices will mutually authenticate each other the flow diagram of this phase elaborating this phase.

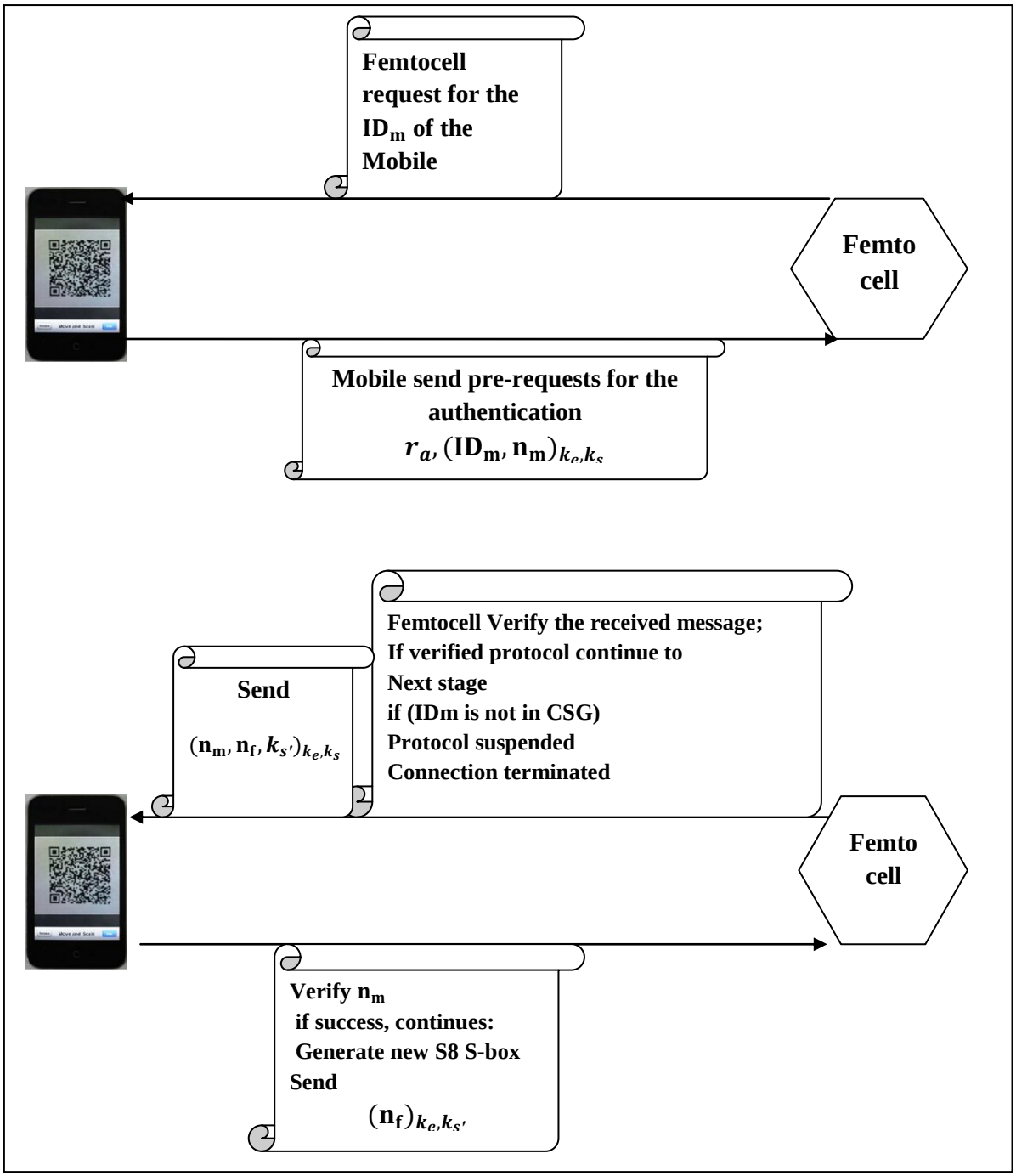


Figure 4.5 (a) Mutual Authentication phase

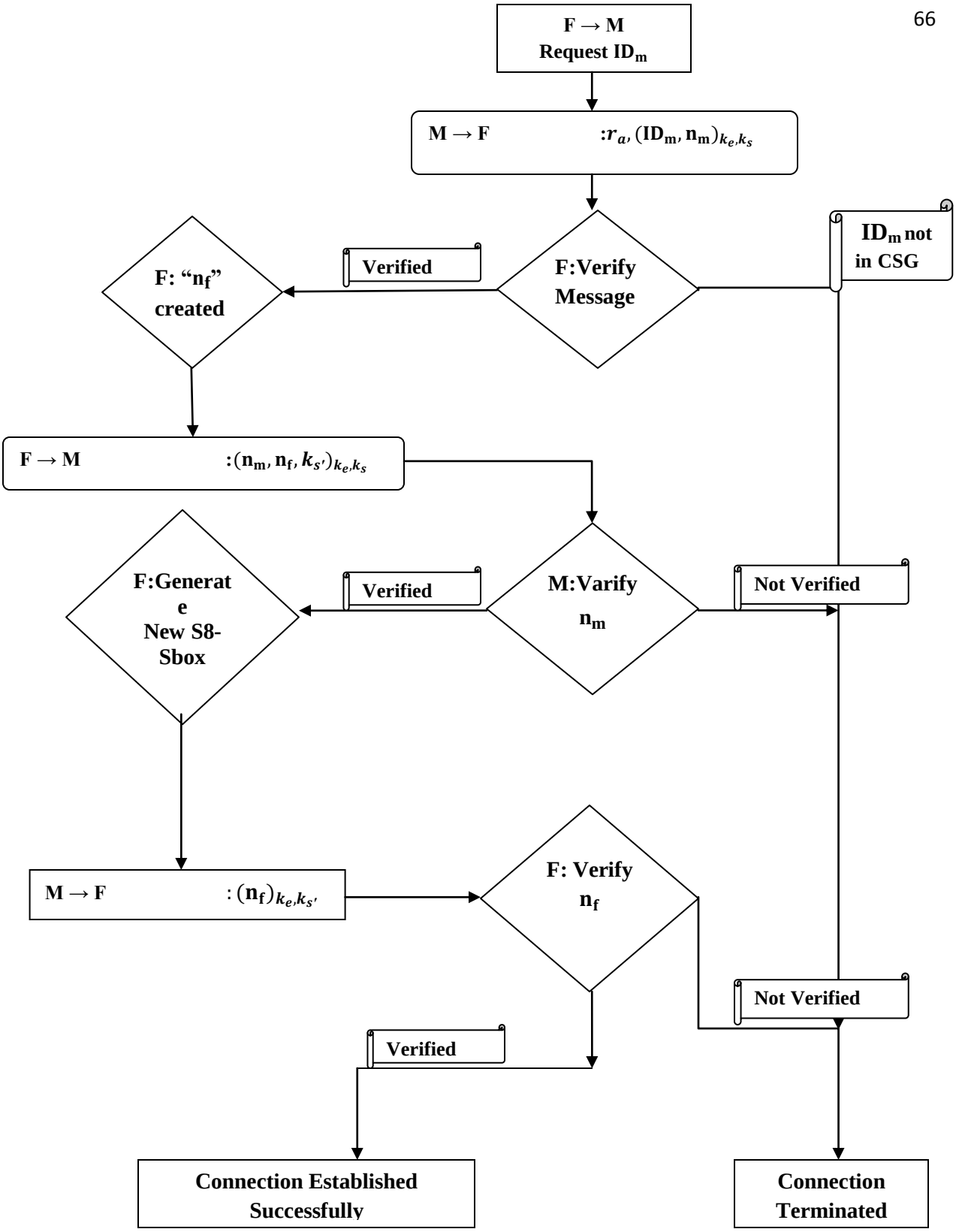


Figure 4.5 (b) Mutual Authentication and Connection Establishments Phase Flow Diagram

4.2.1 Step 2

In second step femtocell generate the "B" For Deffie Helman extract the key and generate the ciphered text and send it to the Mobile and request for the $ID_{m.}$ as ID_m is 11 digits if user provide more or less than eleven digit a window pop up wrong entry and if user provide wrong ID_m connection will be terminated after 10 second.

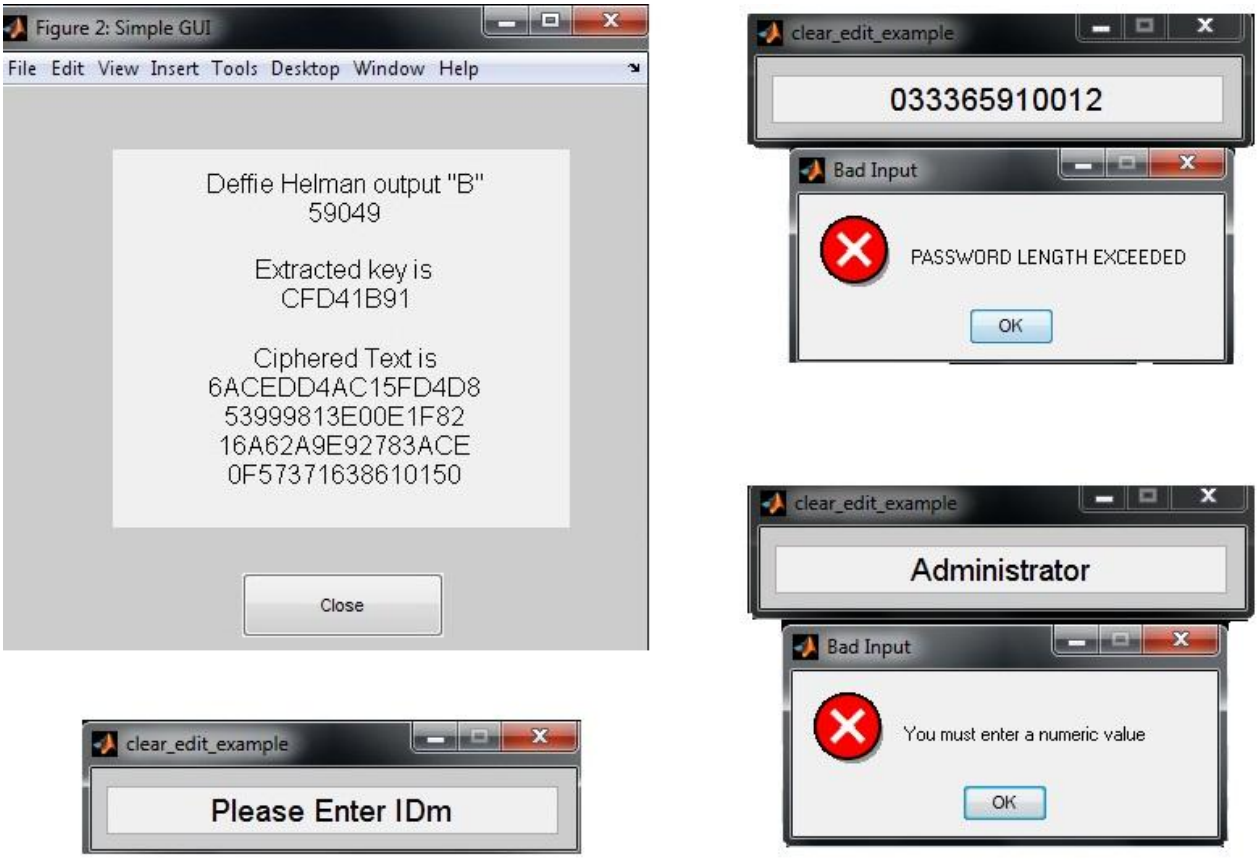


Figure 4.6 Mutual Authentication Phase step 2

4.2.2 Step 3

In 3rd step random number "r_a" and mobile nounce "n_m" with ID_m sent as cipher text from mobile to femtocell. This number will help to identify the mobile. As a unique nounce is assign to the mobile if the ID_m or n_m is forged then this nounce will help to discard the illegal user.

Figure 4.7 Mutual Authentication Phase step 3

4.2.3 Step 4

Femtocell sends mobile a ciphered text which contains "n_m", "N_f" and "K_S`" to generate new S-box for AES.

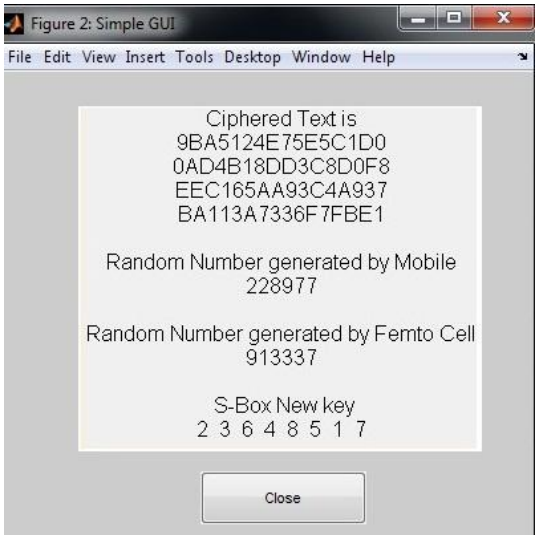


Figure 4.8 Mutual Authentication Phase step 4

4.2.4 Step 5

Mobile send "n_f" as cipher for mutual authentication

Figure 4.9 Mutual Authentication Phase step 5

4.3 Safe Link Establishment Phase

when both devices mutually authenticate each other then femtocell send a message the safe link is established as shown in the flow diagram

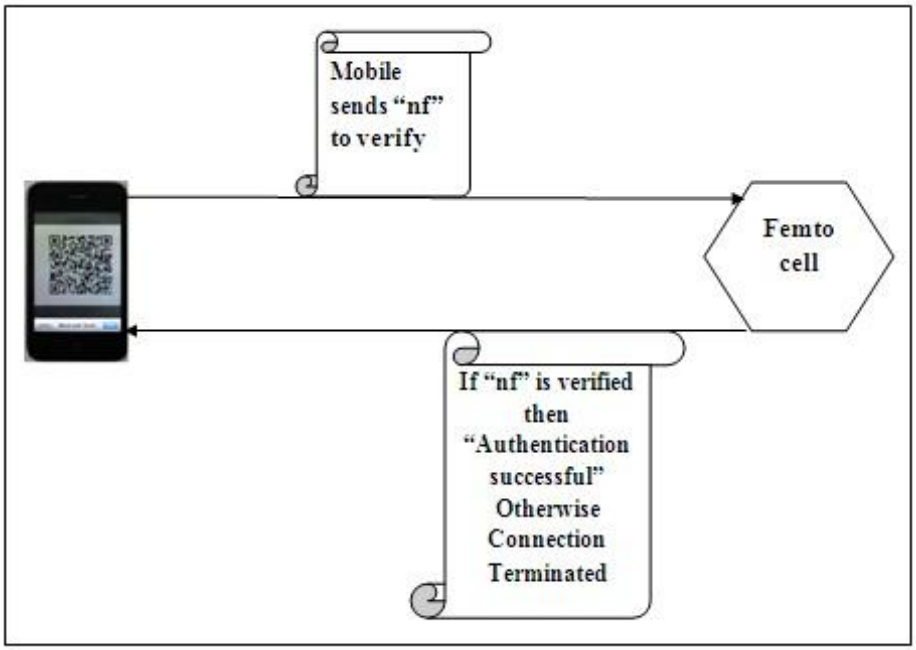


Figure 4.10 Safe link Establishment

4.3.1 Final Step

Send and received "n_f" are matched by femtocell and if they are same connection establish otherwise connection will be terminated

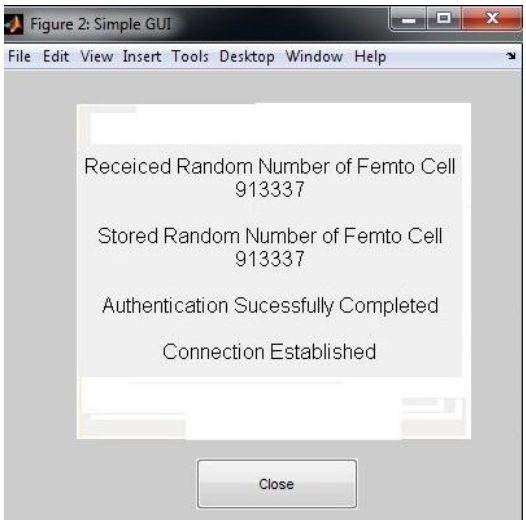


Figure 4.11 Connection Establishment Step

4.4 Time to Establish Connection

Time of every step is calculated total time for authentication is 0.82 seconds. In this short time it is hard to calculate 40320^{40320} and chose the correct key to establish a connection. As compared to RDAP [5] the authentication time of this proposed protocol is much less and trustworthy for the secure communication.

Figure 4.12 Time Of Each Step

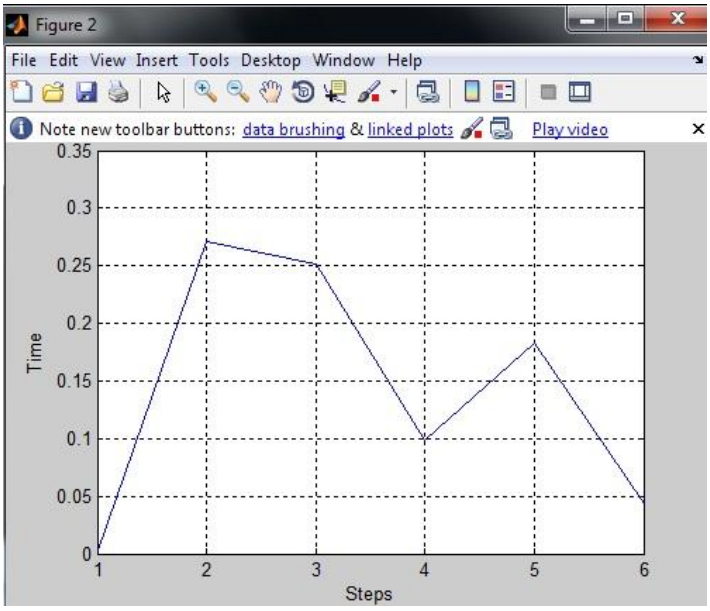


Figure 4.13 Graphical Results of Each Step

4.5 Summary

In this chapter proposed mutual authentication protocol described by taking sender and a receiver. Let's take mobile devices and the femtocells which need mutual authentication to communicate. Generation of S8 S-box with permutation method enhance the complexity of the algorithm and then make it invulnerable to various attacks. A secure tunnel is created before authentication phase to securely exchange the key. AES with S8 S-box reduces the resource usage and provide the secure tunnel for communication.

CHAPTER-5

CONCLUSIONS AND FUTURE WORK

5.1 Evaluation of Results

After studying the different techniques of authentication like simple authentication, Digest authentication, One Time Password Authentication (OTP), Biometric Authentication, ISO/IEC 9798-2 Timestamp Based Unilateral Authentication, ISO/IEC 9798-2 Nonce Based Mutual Authentication and Rapid Development Authentication protocol which is very close to the proposed protocol. But every method has some pros and cones, so for the secure communication environment for mobile device and HeNB there is need of a protocol which provides a secure communication atmosphere; protocol should be compatible with sending and receiving devices, time efficient and most important protocol should be non vulnerable against authentication attacks like MITM, Sybil attack, Masquerade Attack etc.

By using proposed method of S_8 S-box for AES we successfully achieved a protocol which full fill all the basic necessities of mutual authentication protocol. This protocol is time efficient and more secure than the Rapid Development Authentication Protocol.

5.2 Future Work

In the future there is need to develop a mutual authentication protocol that establish a connection less than the time taken by AES S_8 S-box for mutual authentication. Later there is need to make this proposed solution more efficient and to implement it on RFID and RFID reader at Bus toll plaza, because many people shows fake RFID to the reader. But the S_8 S-box solution cannot be implemented on the RFID tag due to its low manipulation power.

REFRENCES

[1] National Institute of Standards and Technologies, “Announcing the Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication,no. 197, Nov. 2001.

[2] Wi-Fi, http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[3] WiMAX, http://standards.ieee.org/getieee802/download/802.16e-2005.pdf

[4] S. Trimberger, “Security in SRAM FPGAs,” IEEE Design and Test of Computers,vol. 24, no. 6, pp. 581, Nov. 2007.

[5] H. Yao, and H.Li-Wei, "RDAP: Rapid Development authentication protocol between Mobile devices and Femtocell", TENCON,2010

[6] S. F.Hasan.,N.. H. Siddique, et. al.,“Femtocell versus WiFi A Survey and Comparison of Architecture and Performance”.In Wireless VITAE' Oct. 2009

[7] R. Housley, W. Polk, W. Ford, and D. Solo, “Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile,” 2002

[8] Z. Jie, and D. L. R. Guillaume,.“Femtocells Technologies and Deployment,” John Wiley and Sons, Ltd., Publication, pp. 305-306, 2010

[9] S. Laur, and K. Nyberg, “Efficient mutual data authentication using manually authenticated strings,” in Cryptology and Network Security (CANS), pp. 90–107. 2006

[10] B. Aboba and D. Simon, ‘RFC2716: PPP EAP TLS Authentication Protocol,’ IETF, Tech. Rep., Oct.1999.

[11] H. Haverinen and J. Salowey, ‘RFC4186: Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM),’ IETF, Tech. Rep., Jan.2006

[12] J. Arkko and H. Haverinen, ‘RFC4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),’ IETF, Tech. Rep., Jan.2006

[13] H. Haverinen and J. Salowey, ‘The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method,’ IETF, Tech. Rep., Feb.2008.

[14] J. Daemen and V. Rijmen, “AES proposal: Rijndael AES algorithm submission,” 1999.

[15] C. E. Shanon, "Communication theory of secrecy systems," In Bell System Technical Journal, volume 28(4), pp. 656-- 715, 1949.

[16] I. Hussain, T. Shah, and H. Mahmood, "A New Algorithm to Construct Secure Keys for AES," Int. J. Contemp. Math. Sciences, vol. 5, no. 26, pp.1263-1270, 2010.

[17] G. Koien and V. Oleshchuk, "Location Privacy for Cellular Systems;Analysis and Solution," Lecture Notes in Computer Science, vol. 3856, pp. 40, 2006

[18] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing Is Believing: Using Camera Phones for Human Verifiable Authentication," in Proceedings of the IEEE Symposium on Security and Privacy, May 2005

[19] B.Igror.,J. Murtaza and H.P. Jean. "Securrity issues in Next generation Mobile Networks:LTE and Femtocells", IEEE computer network in Future, 2011

[20] Z. Liping and Z.Yujuan, "Research on Managing Private Key of PKI Users" International Conference on Mechatronic Science, Electric Engineering and Computer, Jilin, China, 2011

[21] L. Choa, M. Maode, L.Hui, M. Jianfeng "A Security Enhanced Authentication and Key Distribution Protocol for wireless networks" IEEE Globecom 2010 work shop on Web and Pervasive Security.2010

[22] M. Abdalla, P.-A. Fouque, D. Pointcheval. Password-Based Authenticated Key Exchange in the Three-Party Setting. In Public Key Cryptography'05, Les Diablerets, Switzerland, Lecture Notes in Computer Science 3386, pp. 65–84, Springer-Verlag, 2005

[23] S. Bruce, Applied Cryptography, John Wiley & Sons, US, 1996

[24] Data Encryption Standard Federal Information Processing Standards Publication 46-3, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[25] R. Rajaram and M. P. Amutha. "An Efficient Password Authentication Scheme for Smart Card", International Journal of Network Security, Vol.14, No.3, PP. 180-186, May 2012

[26] M. Savari, "Comparison of ECC and RSA algorithm in multipurpose smart card application", International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), june 2012

[27] J. Franks, P. B Hallam, et al, "RFC2617: HTTP Authentication: Basic and Digest Access Authentication", IETF, June 1999

[28] N. Haller, C., Metz, P. Nesser, M. Straw, "RFC2289: A One-Time Password System", IETF, February 1998

[29] Ashley, P., Vandenwauver, M., Practical Intranet Security : Overview of the State of the Art and Available Technologies, Netherlands: Kluwer Academic Publishers, 1999. ISBN 0-7923-8354-0.

[30] D. Joan and R. Vincent ; "AES proposal"; the first AES candidates conference, Ventura, CA, USA. AUG 20-22 1998

[31] I. Hussain, T. Shah, and H. Mahmood, "A New Algorithm to Construct Secure Keys for AES," Int. J. Contemp. Math. Sciences, vol. 5, no. 26, pp.1263-1270, 2010.

[32] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-baseddefense mechanisms countering the DoS and DDoS problems," (CSUR), vol. 39, no. 1,pp.3-4, 2007

[33] Y. H. Lin, A. Studer, H. C. Hsiao, et al "SPATE: Small-group PKI-less authenticated trust establishment," in Proceedings of the 7th Annual International Conference on Mobile Systems, Applications and Services, Jun. 2009.