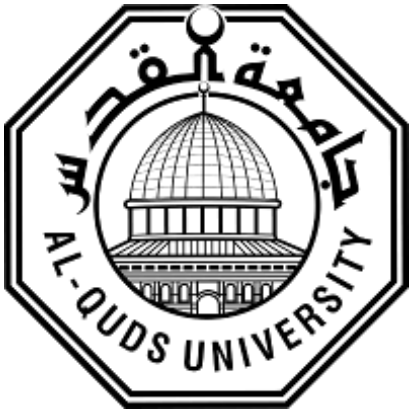
**Deanship of Graduate Studies**

**Al-Quds University**




# Extending AES with DH Key-Exchange to Enhance VoIP Encryption in Mobile Networks

**Prepared By:**

**NoorAldeen Kamal Mahmoud Jabali**

**M.Sc. Thesis**

**Jerusalem-Palestine**

**2017/2018**

**1439/1438**

# Extending AES with DH Key-Exchange to Enhance VoIP Encryption in Mobile Networks

**Prepared By:**

**NoorAldeen Kamal Mahmoud Jabali**

**M.Sc.: Computer Science, Al-Quds University-Palestine**

**Supervisor: Dr. Raid Zaghal**


جامعة القدس
Al-Quds University

**A thesis Submitted in Partial fulfillment of requirements for the degree of Master of Computer Science / Department of Computer Science / Faculty of Graduate Studies – Al-Quds University**.

**2017/2018**

**Al-Quds University**

**Deanship of Graduate Studies**

**Computer Science Department**

# Thesis Approval

# Extending AES with DH Key-Exchange to Enhance VoIP Encryption in Mobile Networks

**Prepared By: Noor Aldeen Kamal Mahmoud Jabali**

**Registration No.:1411873**

**Supervisor: Dr. Raid Zaghal**

Master thesis submitted and accepted. Date: / /2018

The names and signatures of the examining committee members are as follows:

1- Head of Committee: Dr. Raid ZaghalSignature: ……..…….

2- Internal Examiner: Dr. RushdiHamamrehSignature: ……..…….

3- External Examiner: Dr. Mousa FarajallahSignature: ……..…….

Jerusalem – Palestine

**2017/2018**

# Declaration

I dedicate this thesis to: My Family,My Sisters,MyColleagues,and My favorite friends.

Finally, I would like to thank all members for sending me abundant love, encouragement and support from all their hearts. I dedicate all my success to each one of them.

Signed……...

Noor Aldeen Kamal Mahmoud Jabali

Date: / /2018

# Acknowledgements

I would like to express my warm thanks and gratitude to my supervisor Dr. Raid Zaghal who provided me with his full support, encouragement and guidance to get this Thesis in its present form.Without his help and support, this work would not see the light. He was available any time I needed him. I would therefore like to convey my sincere gratitude to him.

I highly appreciate the excellent guidanceof the defense committee; Dr. Mousa Farajallah and Dr. RushdiHamamreh for their valuable comments and feedback, and also the faculty members of the Master program at Al-Quds University; especially,Dr. Saeed Salah, Dr. Badie'Sartwai, Dr.Rashid Jayousi, Dr. Wael Hasouneh, Dr. Jihad Najjar and Dr. NidalKafri.

## Abstract

Recently,the evolution and progress have become significant in the field of information technology and mobile technology, especially inSmartphone applications that are currently widely spreading. Due to the huge developments in mobile and smartphone technologies in recent years, more attention is given to voice data transmission such as VoIP (Voice over IP) technologies– e.g. (WhatsApp, Skype, and Face Book Messenger). When using VoIP services over smartphones, there are always security and privacy concerns like the eavesdropping of calls between the communicating parties. Therefore, there is a pressing need to address these risks by enhancing the security level and encryption methods. In this work, we use scheme to encrypt VoIP channels using (128, 192 & 256-bit) enhanced encryption based on the Advanced Encryption Standard (AES) algorithm, by extending it with the well-known Diffie-Hellman (DH) key exchange method. We have performed a series of real tests on the enhanced (AES-DH) algorithm and compared its performance with the generic AES algorithm. The results have shown that we can get a significant increase in the encryption strength at a very small overhead between 4% and 7% of execution timebetween AES and AEScombine withDH for all scenario which was incurred by added time of encryption and decryption.

Our approach uses high security and speed and reduces the voice delay.In dealing with sound transfer process via the internet, we use the SIP server to authenticate the communication process between the two parties. The implementation is done on a mobile device (Which is operated by (Android) system) because it has recently been widely used among different people around the world.

**الملخص:**

اصبحت الثورة والتطور كبيرة حديثاً في حقول تكنولوجيا الاتصالات والهواتف النقالة، وخصوصا في تطبيقات الهواتف الذكية التي تنتشر حاليا بشكل واسع. وتم اعطاء المزيد من الاهتمام لنقل البيانات الصوتية مثل تكنولوجيا الاتصال عبر بروتكول الانترنت، على سبيل المثال: (الواتساب، السكايب، الفيس بوك، والماسنجر). ويعزى ذلك للتطور الكبير في تكنولوجيا الهواتف النقالة والذكية في السنوات الاخيرة.

عند استخدام خدمات الاتصال عبر بروتكول الانترنت VoIP، هناك مخاوف دائمة حول الحماية والخصوصية كالتجسس على المكالمات بين جهات الاتصال. ولذلك هنالك حاجة ماسة لمعالجة هذه المخاطر عن طريق تحسين مستوى الحماية وطرق التشفير.

في هذا العمل، نستخدم/ نجمع بين اثنتين من الخوارزميات لتشفير قنوات الاتصال عبر بروتوكول الانترنت (128، 192، و 256 بت) عبر خوارزمية AESوتمديدها عبر طريقة تبادل ديفي هيلمان الرئيسية المعروفة. وقمنا باداء العديد من التجارب الحقيقية على AES–DH ، وقمنا بمقارنة ادائها مع اداء خوارزمية معيار التشفير المتقدم العامة.

اظهرت النتائج انه بامكاننا الحصول على زيادة كبيرة في قوة التشفير بنسبة صغيرة جدا بين 4% و7% من وقت التنفيذ بين AESو AES/DH لجميع السيناريو والتي تم تكبدها من قبل الوقت المضاف للتشفير وفك التشفير.

يستخدم نهجنا درجة عالية من الحماية والسرعة ويقلل من تأخير الصوت، ونستخدم في التعامل مع عملية نقل الصوت عبر الانترنت SIP Serverلتوثيق عملية الاتصال بين الجهتين.

وتم التنفيذ على هاتف نقال يعمل على نظام اندرويد؛ لانه استخدم بشكل واسع مؤخرا بين مختلف الناس حول العالم.

## Table of Contents

## List of Tables



**List of Figures**

# Chapter One: Introduction

## 1.1 Introduction

Nowadays, the mobile has become an integral part of our everyday life around the world. The huge developmentsin mobile applicationshave madeour lives easier,yet, more sophisticated and more challenging (e.g. due to security concerns). It is not just a phone with aSIM card for receiving incoming / outgoing calls; it has more uses in different ways due todevelopments in hardware and software. Mobile phones use has expanded to include sending messages, checking emails, shopping, banking services, storing contacts, selecting maps, storing important dates, camera services, and other uses. Part of the most usefulapplications in mobile phones is mobile Wireless Fidelity (Wi-Fi) that led to the development of new services in domain transfer of media including voice transfer known as Voice over Internet Protocol (VoIP)[1].

VoIP is very demanding as it is cost ineffective technology and entails semi-free voice calls through internet; it draws the attention of many internet users. However,VOIP deals with small size packets compared with other video or web packets, and the redundant header size of a VoIP packet is larger than the size of the payload including voice information[15]. Therefore, the problem here is that it can be easily eavesdropped by hackers and the dataon public and private cryptosystemscan be monitored.

VoIPtechnology is vulnerable to different types of attacks, such as eavesdropping,packet capturing, and others. To protect our communication channel from these attacks, we need to employ certain protective measures such as authentication,confidentiality (via encryption),and integrity with replay protection to the media stream[2].

The most important protective measure here is confidentiality of the data which means that the encrypted data is indistinguishable by anyone who does not have the key. Message authentication implies that if a secondparty user agent (server) receives a packet sent by a first party user agent (client), then it was indeed sent by the first party. Data integrity implies that any modification of the data during transmission will be detected by the recipient[3].

## 1.2 VoIP Service

In this section we will know about VoIP service that helpsunderstand how VOIP works and explain some concepts related to the different types of VoIP service for calling.

### 1.2.1 Types of VoIP service

There are different types of VoIP services based on the infrastructures of these VoIP[3] .

#### 1.2.1.1 Phone to Phone (IP phone)

The most important service in this thesis is phone to phone service. They are different type s of application in phones but this service is known as a hardware-based service that allows the caller and receiver to talk to each other using the internet receiver depending on IP protocol. This service is separate and differs from a company to anotherespecially those that use this type of service to handle long distance calls. To handle this type, we must convert a voice to the packets and transfer it over the IP without Public Switched Telephone Network (PSTN) for beginning and terminating calls in the emergency situation as shown in Figure 1.1.

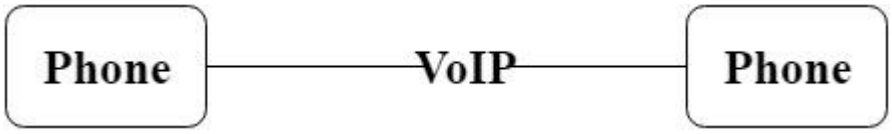



Figure 1.1: Phone to Phone Service

### 1.2.1.2 Computer to Phone and Vice Verse

This is a software-based and hardware-based service. Softphone's software is used to route the call an Internet Protocol (IP) and hand off to a conventional telephone network. To use the service, one needs to subscribe and be charged at a low rate. Examples include Skype,Google Talk and MSN that provide the service to enable their customers to call landline from their computers[3].

Computer to phone requirements are internet-enabled phone and a computer,VoIP service subscription,a modem and an analog terminal adapter to convert the call signal to digital signal and also to analog signal again. Computer to phone service does not allow emergency calls and the computer needs to have a computer connected to the internet, as shown in Figure 1.2.

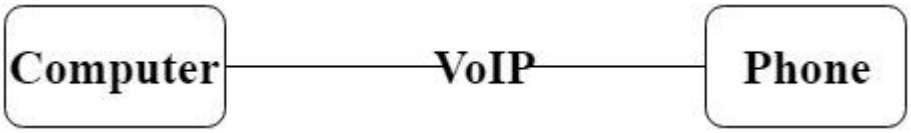



Figure 1.2: Computer to Phone Service

### 1.2.1.3 Computer to Computer

Computer to Computer service provides internet telephony freely using the same softphone software such as Skype, Instant Messaging, AOL etc. This type provides voice transfer from caller to receiver by internet protocol, and both parties must be using their computers in order to conduct calls. The following requirements must be met to use computer to computer VoIP service: softphone software, a sound card and good internet service, and the caller with receiver should be online[4], as shown in Figure 1.3.

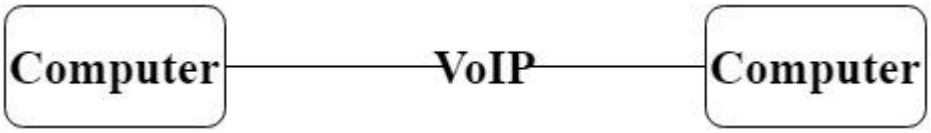



Figure 1.3: Computer to Computer

### 1.2.2 VoIP Security Threats

In this part there are different key elements of VoIP threat. According to[5] the possible threats for VoIP security include the following:

**1.2.2.1 Eavesdropping, Interception, and Modification Threats**: Here an outsider can intrude the call/session and listen to the signaling (call setup) or the content of a VoIP session, and he/she can possibly modify aspects of that session indirectly without being detected.In our module we will address this threat.

**1.2.2.2 Social Threats:** This type is targeted directly against humans. Such asmisconfigurations, bugs or bad protocol interactions in VoIP systems may enable or facilitate attacks that misrepresent the identity of malicious parties to users.

**1.2.2.3 Service Abuse Threats:** this type is covering the improper use of VoIP services, especially in situations where such services are offered in a commercial settingsuch as threats that include toll fraud and billing avoidance.

**1.2.2.4 Denial of Service Threats**: this type denies the user from accessing the VoIP services. This may be particularly problematic in the case of emergencies, or when a DoS attack affects all of user's or organization communication capabilities. It may be caused by VoIP protocol. They may also involve attacks through computing or other infrastructures (e.g., shutting down power).

#### 1.2.2.5 Physical Access Threat:

this type is referring to inappropriate/unauthorized access.

## 1.3 VoIP Components

There are different elements/components of VoIP; they include the following:

### 1.3.1 End-user Equipment

The end-user equipment is used to access the VoIP system to communicate with another end point. In the system of VOIP there are two users: the first-point user/ sender user and the endpoint user called the receiver to communicate with each other to exchange data (voice data) by connecting to the network either physically via cables or through wireless[7]

.

### 1.3.2 VoIP Protocol

There are different types of VoIP protocols used in VoIP network; the most commonly used ones are SIP and H.323 over UDP and TCP.The most important protocol here in this thesis is SIP for many reasons.

#### 1.3.2.1 Session Initiation Protocol (SIP)

SIP is used in this module to control protocol known in standardized Internet Engineering Task Force (IETF); it manages interactive user sessions, including instant messaging, voice, video, and other multimedia sessions. SIP is a major signaling protocol used in Voice over IP (VoIP), and it can support both IP and conventional telephone communication[6].

SIP is used to setup IP based multimedia services such as audio and video streaming, instant messaging, and other real-time communication across commonly used packet

networks. This protocol is becoming widely used; it is also more popular than the H.323 family, because of its simpler nature and flexible design [6], as shown in Figure 1.4.

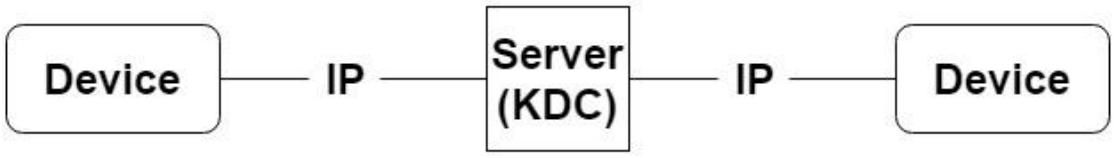



Figure 1.4: SIP Protocol

The SIP is mediator between two parties and it transfers data between two clients; the SIP server receives the data from a sender in a packet form like Hypertext Transfer Protocol (HTTP); it opens many opportunities for several attacks such as registration hijacking, impersonating a proxy and Denial of Services (DoS). SIP is a signaling protocol, and during the signaling phase several parameters are exchanged between the end users. These parameters contain sensitive information like the user name and the location.

Security concept of SIP are becoming a main problem due to the adoption of the SIP based VoIP system. when callsbetween two parties are established, the conversation should be protected and the information should not be revealed to an outsider by applying different security parameters. These parameters,according to [6], include:

- Availability

SIP needs availability of secured voice resources on ability to access desired data or required services;this means when a user requires or requests any service, a system should ensure the user can access the required service without any problem.

But sometimes this parameter is not possible due to various attacks such as Denial of Service (DoS) attacks or Distributed Denial of Service (DDoS) attacks.

These parameters offer suitable environment to threats.A SIP system is vulnerable to common IP and VoIP threats. Those threats are representedbyan intruder who may provide data by eavesdropping when he knows the IP between user and SIP server[3].

In order to find the SIP security mechanism, different numbers of security protocols or schemes should be integrated with the SIP protocol or used together with the SIP to improve the security, but most of them have originated from communications communities.

- Confidentiality

SIP can use confidentiality to prevent malicious users from call monitoring which contains significant information such as caller presence status, buddy list and contact address. The system would be vulnerable to many attacks like message tampering, and eavesdropping.

To provide confidentiality in SIP server, there are different encryption techniques which provide user authentication such as symmetric encryption and asymmetric encryption.

Integrity service is used to protect the source of data and provide the authentication service; consequently, without integrity control the system is non-trusted and an intruder has the ability to modify the different content without being noticed.

- Authentication

The users should know what kind of information is used in transfer through the communication, and it should be encrypted to successfully reach the other party.

These concepts present many threats to the applications such as message tampering, and eavesdropping; therefore, a set of secure interfaces, which provide authentication, authorization and integrity,is to be implemented by users.

### 1.3.2.2Comparison between SIP and H.323

After explaining all the commonly used protocols,it is time for choosing the SIP server between the SIP and H.323. The SIP server has a more flexible design to make secure activity [7], as shown in Table 1.1:

Table 1.1: Comparison between SIP and H.323

| **Type** | **SIP** | **H.323** |
|---|---|---|
| **Media Transport** | RTP/RTCP, SRTP | RTP/RTCP, SRTP |
| **Encryption** | Yes, via SSL, PGP, S/MIME, or various other means. | Yes, via H.235 (including use of SRTP, TLS, IPSec, etc.). |
| **Transport** | EitherTCP, UDP or both, The UDP protocol is mostly used for signaling. | Either TCP or UDP (mostly TCP for signaling). |
| **Security** | Registration: uses agent to register with proxy server.<br>Authentication: user agent authentication uses HTTP digest or basic authentication.<br>Encryption: SIP defines three methods of encryption for data privacy | Registration: endpoints register and request admission with gatekeeper.<br>Authentication and encryption: H.323 provides recommendations for authentication and encryption in H.323 system |

| | | |
|---|---|---|
| **Capability Exchange** | Uses Session Description Protocol (SDP) for ensure arrival data to the other party. | Uses H.245 for call control. |
| **Quality of service** | SIP relies on other protocols like RSVP, COPS and OPS to implement QoS. | Bandwidth management and mission control managed by H.323 gatekeeper |
| **Data** | Text, voice or video. | Multimedia only. |

### 1.3.3 Security Methods of VoIP

There are two algorithm use for VoIP encryptionAES and DH algorithm.

#### 1.3.3.1 Advanced Encryption Standard (AES) Algorithm

The AES is used to provide security for sensitive data, and it is based on Substitution and Transposition methods. The AES is used in many password-protected documents and wireless communications such as wireless sensor networks, and in top secret government filesfor which it was first built[8].

This algorithm takes the input data block of size 128 bit and a variable key size of 128, 192 or 256 bits for 10, 12 or 14 rounds respectively. Each round consists of several processing steps, including the encryption step itself. Similarly,a set of reverse rounds are performed to transform ciphertext back into plaintext, the pictorial representation of the AES encryption process to encrypt 128-bit in plaintext to 128-bit in cipher text. When the plaintext size is more than 128-bits,

it will be divided into blocks of 128-bit plaintext [8], as shown in Figure 1.5.

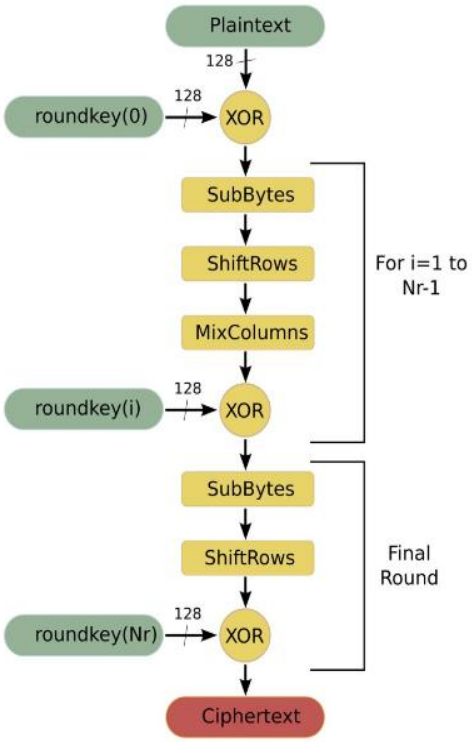



Figure 1.5: AES encryption process [10]

In such a situation, AES encryption will be done for each block separately. So, the weak part of the algorithm is the secret key;therefore, it should be motivated to do some processing to give more security to this key [8],as shown in Figure 1.6.

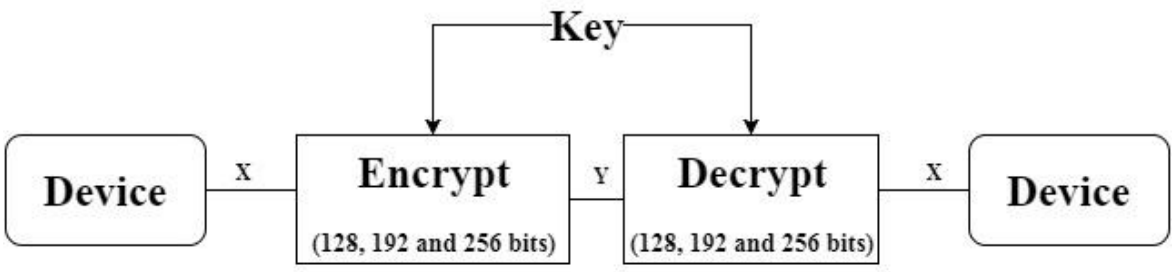



Figure 1.6: AES key Algorithm

### 1.3.3.2 Diffie-Hellman key exchange (DH) Algorithm

In cryptography,The DH algorithm is one of the most popular public-key encryption and it is a kind of asymmetric encryption method. Senders and receivers can utilize those keys to exchange encrypted message. The importance of this algorithmis to ensure secret communication for exchanging information over a public channeland DH is usually utilized when you encrypt data on the Web utilizing either SSL (Secure Socket Layer) or TLS (Transport Layer Security). The Secure Shell (SSH) protocol also uses DH. Obviously, the DH is a piece of the key exchange mechanism for IPSec, anyVPN based on that technology that uses DH [12]as well as any firewall and network security products currently available.

Furthermore,VoIP networks are growing very fast, so a larger volume of VoIP traffic is expected and this will significantly increase the cost of supporting DH computations.

Depending on the DH algorithm in the future means increasing the corresponding keys sizes in order to cope with the improvement of processors' speeds that the attackers might use to attack this algorithm. Unfortunately, increasing the keys sizes will worsen the performance,as shown in Figure 1.7.

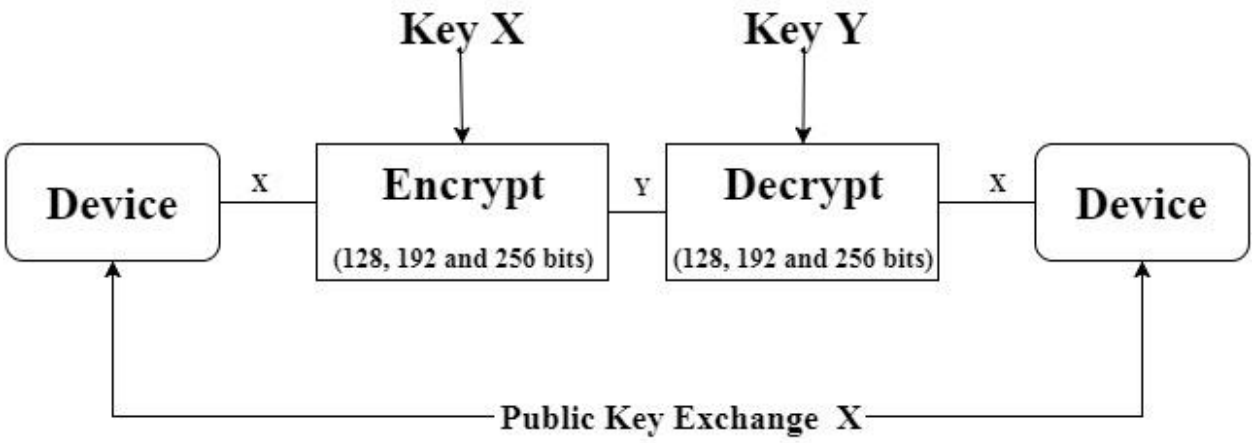



Figure 1.7: DH key exchange

In this case, the proposed modulesuggests using the DH and AES to reduce the intruder attacks and problems of getting data during the process of transportation, as discussed earlier, the private computations between users as follows:

$$\text{DeviceA} = g^{a} \bmod p$$

$$\text{Device B} = g^{b} \bmod p$$

## 1.4 Contribution

Even though the AES algorithm provides strong encryptionbecause is largely considered impervious to all attacks, with the exception of brute forceand it is vulnerable to different kinds of attacks using different hacking techniques; Intrudersknow that AES uses a (symmetric key), and thus they can use the same cipher key for all encrypted packets ofthe VOIP encryption, and they have better chance of success in eavesdropping and compromising the voice call. In the AES system, the intruders need $2^{67}$ seconds to find key for a 128-bit AES key[7], but with the asymmetric key nature of the DH algorithm, it will take $2^{80.5}$seconds[9]to guess the key, and thus it becomes almost impossible for the intruders to hackthe voice channel.

The main contribution of this thesis i.e., presenting a suitable solution for reducing problems of voice transmission through SIP server, and these contributions are summarized as follows:

1. To identify the quality of service which represents process speed of the voice transmission for delivering the voice to the second partydepending on the service provider.
2. To measure the quality of service when parties call each other to make sure the performance is good when use two algorithms together (AES and DH).

3. To ensure data confidentiality from any type of intruders while eavesdropping or monitoring on the voice by DH and AES encryption algorithms.

## 1.5 Statement of Problem

TheVoIP service has spread around the world since 1995 and has been used a lot bycompanies and peoples. In February 2005 the NIST warned the users that VOIP can be exposed in the form of the packet data become weaker in terms of security; consequently, higher possibilities for eavesdropping and attacks have emerged compared with the existing telephone servicesthat are safer and more secured.

The VOIP uses different ways to protect data, such as different algorithm to encrypt data packets in VOIP like AES, DES, RC2, Blowfish(BF), Triple DES. But recently with the introduction a new method of decryption these algorithms start to have problems in data protection in VoIP. For example, the AES algorithm uses VOIP to encrypt, but this algorithm has a problem with the level of security by using weak key exchange; There are many cryptanalysis systemsthat were designed to attack this algorithm using the same key to decrypt the packet or attack block ciphers with a reduced number of rounds[8]. In our algorithm we enhance the level security by using asymmetric key exchange and make it almost impossible to hack by different intruders or against any kind of attacks such as differential, brute-force and liner attacks.However, in this thesis,the encryption is applied on the voice to produce the cipher voice and the decryption is also applied to retrieve the original voice by using AES algorithm and Diffie-Hellman key exchange (DH) for high security and speed.

## 1.6 Research Questions

This study is meant to address the following questions and seek answers for them:

1. Can we use Advanced Encryption Standard (AES) algorithm combined with Diffie-Hellman (DH) exchange key algorithm to improve security, quality of service and speed through SIP server across local connection links?
2. Can we improve packet delivery without loss and reduce delay?
3. Canwe perform a real test of the module and collect data?

## 1.6 Thesis Outline

This thesis includes five chapters including the introduction. The following is a summary for the chapters:

- Chapter two includesthe related work and gives the main problem discussed in this research, and summary of the most important related works.
- Chapter threedescribes the theoretical design that has been used; it also introduces a description of a proposed solution of the problem explained by flowcharts and algorithms.
- Chapter fourpresents the experiments and the results.
- Chapter five introduces conclusions and future works for this research.

# Chapter Two: Related Work

## 2.1 Introduction

During the last decades, the technology development has occurred in the information technology field generally, and the communication field,specifically,in the field of mobile technology. The biggest technology development was achieved, especially, in transferring information and data through the internet.

The development caused many problems and the main was how to avoid the intruder.As well as the following:

1. The intruder can discover the important information or data through reading the text or eavesdropping on the voice.
2. The delayed time occurred through the transferring process.
3. To ensure that interruption problemswouldn’t occurred between the two parties.

The transmission process from sender to receiver should protect data through a specific secure method because data is very important.

In this thesis, we will choose one type of the data transmission techniques, and that is the voice transmission. Because it is threatened by the intruder, so it should transfer the data between two parties with high protection and suitable speed. We will try to achieve this by designing a module to secure data before sending it to the other party, as shown in Figure 2.1.

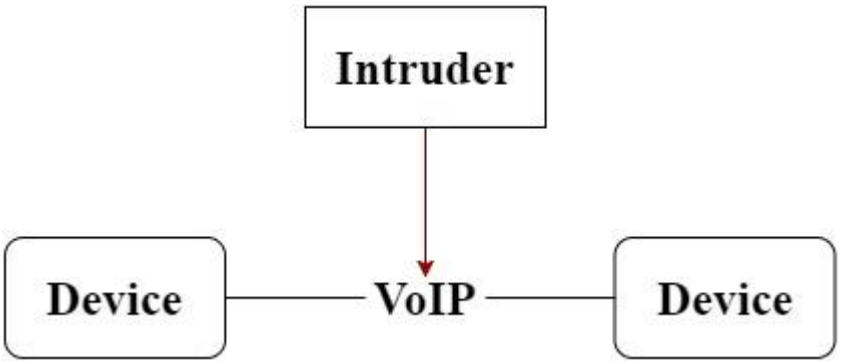



Figure 2.1: VoIP Threats

## 2.2 Literature Review

**Prashant Kumbharkar and TrimbakSontakke[4]:** The authors presented a media application P2Pknown as SALMON to secure all media such as VIDEO-STREAMING that utilizesSIP to safe applications as layer in the system. This paper shows anapplication that was built against meddlers between pairs that use some media to exchange data, such as the voice known as VOIP or the VIDEO-STREAMING which is known as video conference.The application is used by elliptic-curve Diffie-Hellman (EDH) key trade on SIP flagging and AES encryption. SALMON show quality ofControl messages,Disruption count andService latencies.The result in P2P VIDEO-STREAMINGshows that the average transfer speed and life time are associated, not just have a finer execution in overhead of control messages.

**YacineRebahi et al [13]:** The authors presented a SIP standard for managing IP multimedia sessions in the internet. Identity management in SIP is a crucial security field that deals with identifying users in SIP networks and controlling their access to the corresponding resources. RFC 4474 describes a mechanism, based on certificates, for dealing with the SIP users identities. The RFC recommends use the DH algorithm because it is currently the most popular public key cryptography system. The proliferation of small and simple

devices as well as the need to increase the capacity of the SIP servers to handle the increasing VoIP traffic will make continuous reliance on DH more challenging over time. The implementation is described by the current RFC 4474.

This paper discusses the integration of Elliptic Curve Cryptography (ECC) into SIP identity management schemes. In fact, RFC 4474 that describes a certificate-based mechanism for dealing with SIP users identities is implemented using DH as well as Elliptic Curve Digital Signature Algorithm (ECDSA). The experiment is shown the superiority of ECDSA over DH in terms of performance. Due to its computational efficiency, ECDSA can be used in constrained environments where traditional public key mechanisms are impractical. Moreover, the paper also analyzes the security issues related to the identity management mechanism. Although this mechanism is helpful to authenticate the SIP identities, the performance of it poses security threats to SIP services. Thus, it is necessary to optimize the performance of this mechanism from different aspects,which can be considered as a first step for use of elliptic curves in the identity management for SIP.

**R. Vargic, et al [14]:** The authors proposed a solution for two issues in current communications. Firstly, that IP Multimedia Subsystem (IMS) suffers from lack of clients. Secondly, the mobile operators want to give the subscriber a possibility to access their VoIP network and efficiently cover special densely populated areas like airports. To address these problems, they developed a novel service architecture, which allows second Generation (2G) subscriber access a SIP based VoIP network via Wi-Fi complying security standards,such an approach can be used especially in highly-populated areas, such as airports and business centers.

The user authentication and authorization are based on an algorithm that uses the Extensible Authentication Protocol and proves the user identity by owning a Subscriber

Identity Module.This algorithm is called EAP-SIM algorithm. The integrity and confidentiality are provided by Internet Protocol Security (IPSec) connection established using parameters derived from authentication triplets.

They tested secured and not secured SIP sessions. The latter ones were tested for non-IPSec enabled clients,and verified the proposed architecture with a mobile phone and have proven the correctness of their approach. The main drawback that remains is the difficulty of IPSec implementation that can be passed by a special application. The lack of IMS clients and special requirements of the mobile operators have forced researchers and industry to develop new service architectures.

**Byounghee Son et al [5]:**The authors present the VoIP encryption module was designed to prevent eavesdropping on internet telephones communications and involved encoding/decoding the output data at the transmitter and receiver of the internet telephone. The VoIP encryption proposed a module for securing privacy. In encoding communication using the proposed module,the AES that should be used is the one which resulted in the overall verification of the system performance and delayed times through experiments. In the experiments, a high speed symmetric 128 bit AES method was used to reduce the voice delay of the VoIP telephone. In the beginning, the call process using a mutual key exchange in the encryption system, an asymmetric encoding method RSA algorithm was used to improve security. The speech quality demonstrated good performance with a Mean Opinion Score (MOS)of 4.18~4.20 (Good Voice Quality range from 1 (Impossible to communicate) to 5 (Good)) and an R-factor of 91.25~93.00 (Good quality of a test voice signal range from 1 (worst) to 100 (best)).

**H.HakanKilinc and TugrulYanik[16]:** The authors presented a survey of authentication and key agreement protocols that are critical security services to implement a secure SIP protocol which is a common part of the VoIP architecture. Performance and security of the

authentication and key agreement schemes are two critical factors that affect the VoIP applications with large number of users. Therefore, the performance of the authentication and key agreement protocols is of great importance.

In this survey, they are identified, categorized and evaluated various SIP authentication and key agreement protocols according to their performance and security evaluation. They are examined schemes according to four different categories which can be denoted as Password Authenticated Key Exchange (PAKE) based, Hash based, Public Key Cryptography (PKC) based and ID based.

On the other hand, most SIP implementations today still employ the Hypertext Transfer Protocol (HTTP) Digest Authentication. The simplicity of implementation and the lower performance overhead seem to be the major reasons. But with the increasing number of security breaches in VoIP systems this choice might change in the near future. Although the performance is inversely proportional to the security features provided in general, they observed that there are successful schemes from both the performance and security viewpoint.

The discussed schemes are mostly designed for client/server architectures. Most of the proposed schemes do not consider delays introduced by network and database access. When designing authentication and key agreement protocols it would be appropriate to consider the delays in a distributed environment. For Peer-to-Peer (P2P) and Next Generation Networks (NGN) architectures, new authentication and key agreement protocols that consider the various overheads introduced by the distributed network structure are necessary.

**HarjitPal Singh et al. [17]:** In this paper, the authors presented and discussed many issues that the Internet has revolutionized the telecommunication systems by supporting new

applications and services. Voice over Internet Protocol (VoIP) is one of the most prominent telecommunication services based on the Internet Protocol (IP). The signal quality of the VoIP system depends on several factors such as networking conditions, coding processes, speech content and error correction schemes. From the very beginning of transferring the voice data over packet switched networks, the journey of the packet based communications to modern VoIP and advancements to improve the service of the VoIP system. The VoIP system has been established as the best alternative to the traditional Public Switched Telephone Network (PSTN) telecommunication system for providing the voice services to the users.

The author summarized the advantage/disadvantage, compression schemes and measurement schemes for the VoIP system. Moreover, the progress in improving the signal quality of the VoIP system in the last four decades had been reviewed. The possibility of the VoIP communication over satellite link, security issues and the role of digital filters to improve signal quality had been highlighted.

## 2.3 Summary

Recently, there have been many researches that present suitable transfer method in the VoIP fieldwhich is representing the protocol for transmitting voice data using the internet.
Several techniques and algorithms have been proposed to improve the quality of VoIP transmission, but these techniques have focused on one side of the transmission aspects, such as security, quality or speed.
This researchattempts to handle all the important aspects of the VoIPfield through focusing on two important points:

- **The first point:**use SIP serverfor the VoIPtransmission which works as a monitoring on the communication sessions between the sender andreceiver.

- **The second point:**How to improve the quality of VoIP transmission with high security and high speed depending on the characteristics of two algorithms (AES and Diffie-Hellman Exchange key).

# Chapter Three:Methodologyand Approach

## 3.1 Introduction

The process of voice transfer may contain important and personal information, or data that is related to both sender and receiver. So the information or data must be secured and known only by authorized parties.

To encryptVOIPwe must use algorithms to encrypt data or information as known as voice between pairs that pass in mobile application; the algorithms are; 256 bit_ AES, and (128, 192 and 256 bits) DH algorithm. Data collection for this study come from two users as voice and transmitted by SIP protocol in the internet.However,the data is passedto analgorithm to encrypt it by AES and DH algorithm so as to transfer it from a sender to a destination to obtain more scientific results that could be used to represent the highest level of security and speed[15].

This thesis focuses on two main points:

- The module proposes and generates a method to reduce eavesdropping threats during transfer operation. This module should be secured and without drawing any attention to the intruders.
- This proposal uses the advantages of AES speed with DH security to produce a unified algorithm calledAES-DH (AES-DH Speed and Security).

Themoduleuses tool to measure the efficiency of thetwoalgorithms together as a different way to improve the high security and speed compared with the different sizes of key 128,192,256 bit in DH algorithm.

The experiment will show different parameters to test the module as follows:

1. Delay time value shows samples T for 256_bit AES with DH algorithm in different key size as shown in Table 3.1 as follow.

Table 3.1: Delay time for AES and DH algorithm.

| Algorithm | AES | DH |
|---|---|---|
| Delay time $T_1$ | 256_bit | 128_bit |
| Delay time $T_2$ | 256_bit | 192_bit |
| Delay time $T_3$ | 256_bit | 256_bit |

Figure 3.1 explain the steps for connection two users together by proxy server and show the delay time in the conversation.

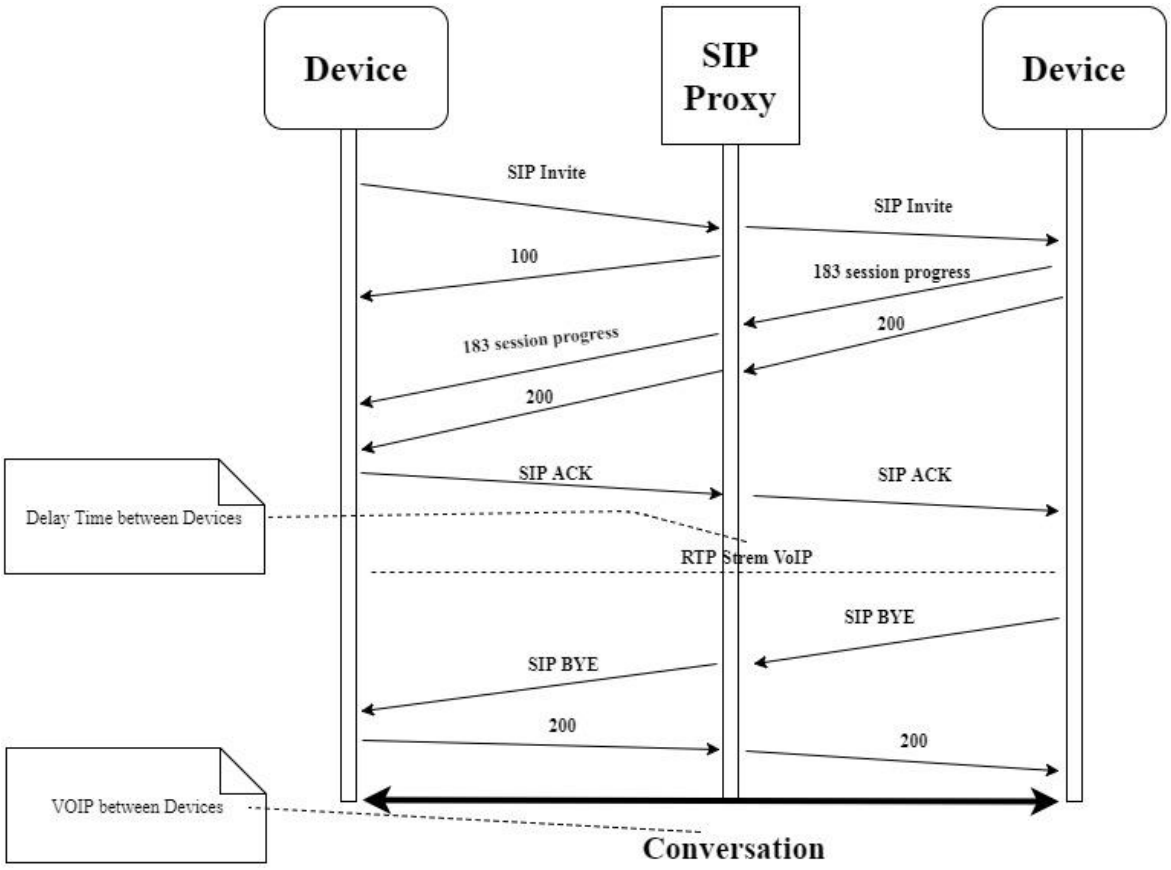



Figure 3.1: Delay time connection

2. Execution time shows sample T for encryption and decryption of different key sizes.
3. The voice quality such as (Packet Loss,and Effect of Security on VoIP Performance).

4. The proposed module includes three procedures that work together and the charts below illustrate working of every step: -

    1. SIP Server procedure: this procedure's function is to make a connection between two parties; it elaborates when receiving extension request and checks if it is available or not, then it opens asession depending on the availability ofa sender and a receiver.
    2. Sender procedure: this procedure's function is to encrypt the audio in the sender side, and then sends it to the receiver which is working after the extension is available.
    3. Receiver procedure: this procedure's function is to receive the encrypted audio from the sender, and then decrypts it in the receiver side which elaborates after the SIP server is opening session.

Figure 3.2 explains the three procedures and the main steps in each procedure

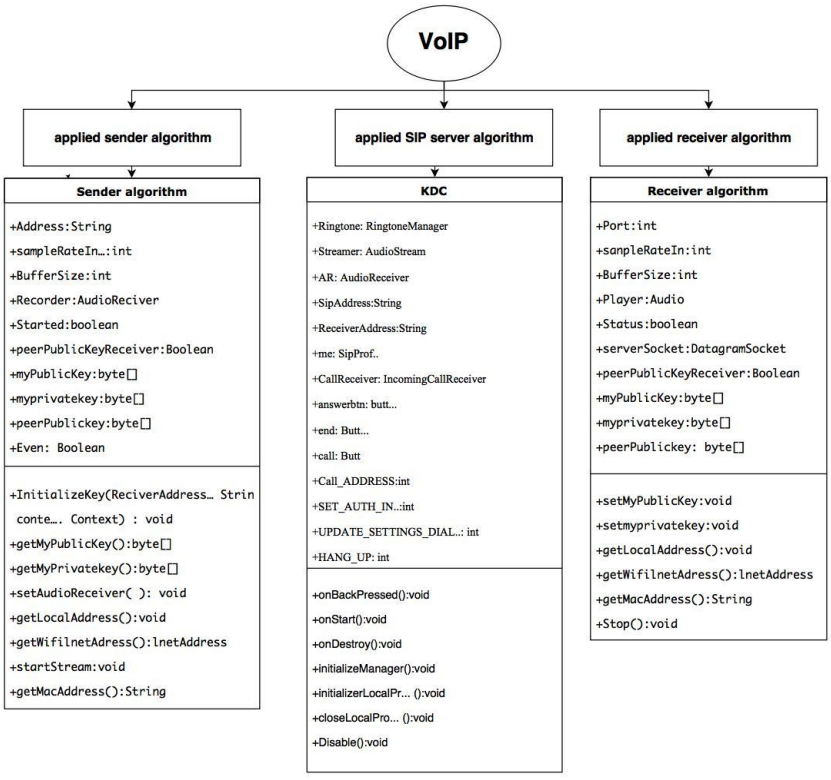



Figure 3.2: The Proposed Module

## 3.2 Test-bed

### 3.2.1 Android platform development (android studio)

Android platform development is the Official IDE for Android; Android studio is used for developing android mobile phone application which the researcher will use to build a module App for VOIP encryptionusing the two algorithms together (AES and DH) in order to access/registerSIPserverto encrypt/decryptvoice from sender to receiver and test the App in real devices with SIP server (3CX) tools.

### 3.2.2 SIP Server (3CX)

3CX Phone system is a SIP server used for windows that works with popularVoIP Gateways;SIP phones allow you to setup a complete IP. SIP servers are responsible for setting up the calls between SIP devices and usually combine several functions of the SIP server includingSIP proxy and SIP register into one piece of software.

### 3.2.3 Wireshark capture filter

Wireshark is a network protocol analyzer that shows capture and interactively browses the traffic running on a computer network. It is afree softwarethat includeshundreds of supported protocols and media such as read real data from 802.11 wireless LAN, Ethernet, Token-Ring, FDDI, ATM connections.

## 3.3 Used Algorithms

There are two algorithms used in this thesis for providing suitable security in transmission voice; these algorithms are divided into three procedures and each procedure includes many steps to execute a specific function.

### 3.3.1 Main Flowchart

This part is used to transmit an audio between a sender and receiver in addition to a third-party in safe form as shown in the Figure 3.3.

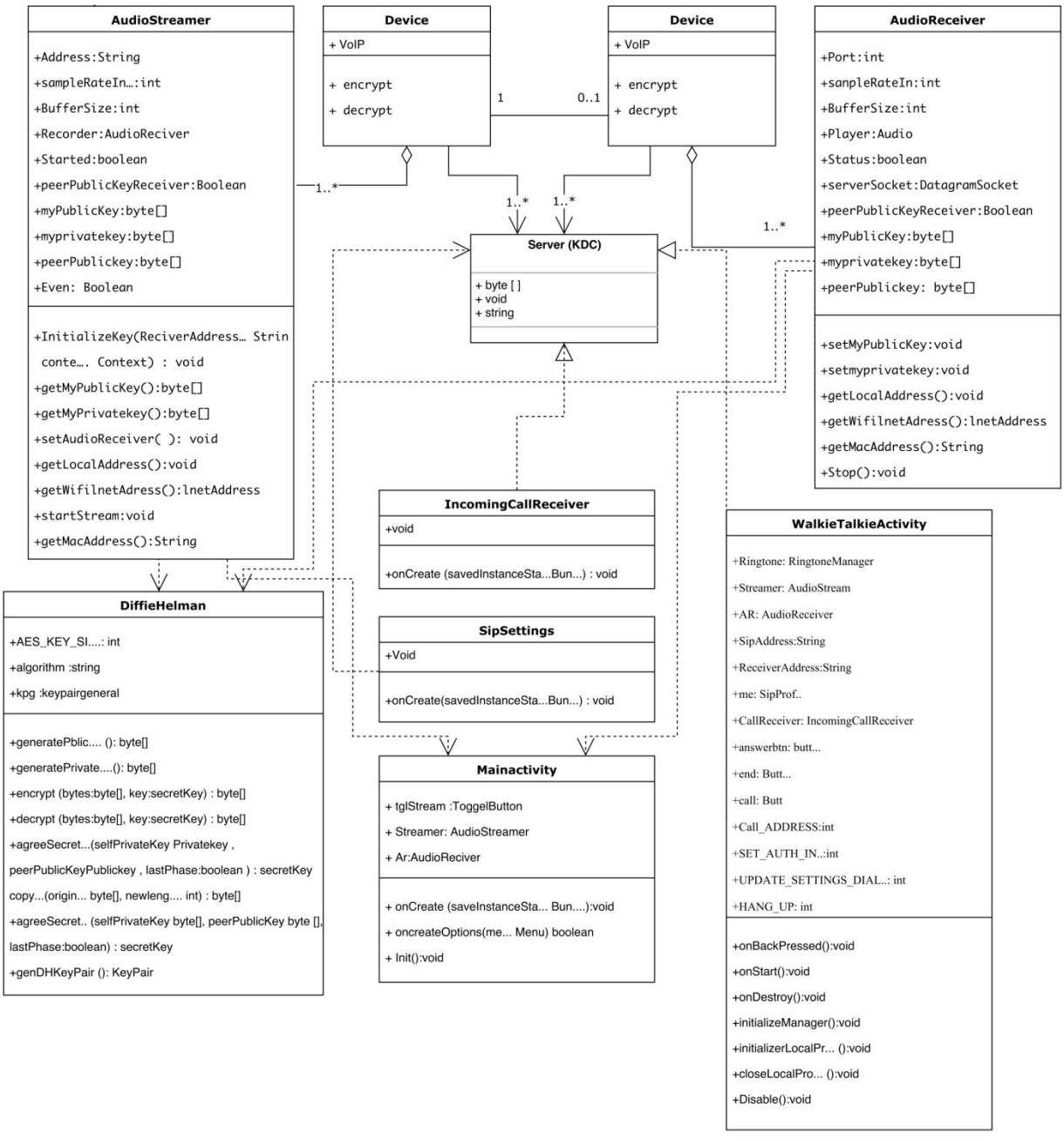



Figure 3.3: Major Flowchart

In Figure 3.3, audio streamerone of these endpoints in the main module. This audio streamer process registersto the SIP server by getting Id and IP address to use it for open session andcommunity with endpoint to allow for start call with generate public key and shared it with endpoint that managed by SIP server and generate the privet key to can be encrypt/decrypt the audio secretly by AES/DH.

### 3.3.2 SIP-Server Flowchart

The SIP Server is used to receive the required extension from the sender, then make sure this extension is available or not. Based on the case, the server decides to open the session or not. SeeFigure 3.4.

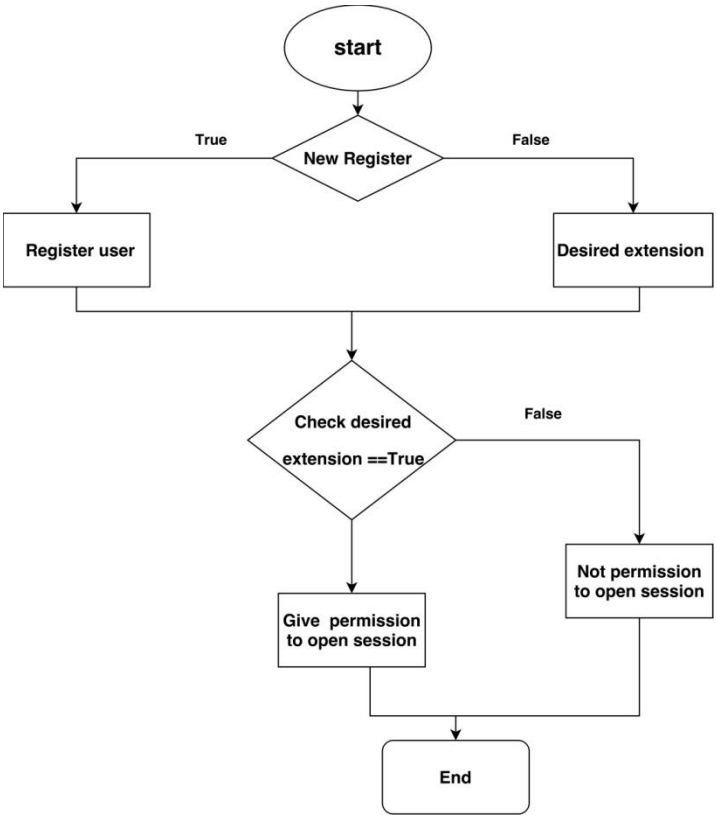



Figure 3.4: SIP-Server Flowchart

### 3.3.3 AES-DH Encryption Flowchart

The AES-DH algorithm will be used due to their two characteristic features of the AES algorithm (e.g., high speed and reasonable security) and the DH algorithm (e.g., strong Security and reasonable speed). **AES-DH** is using the advantages of AES speed with DH security.Thispart is used to open the session with the SIP server; it also makes sure the second party is existing or not. After that, the sender is encrypting the audio then sending it to the recipient as shown in Figure 3.5.

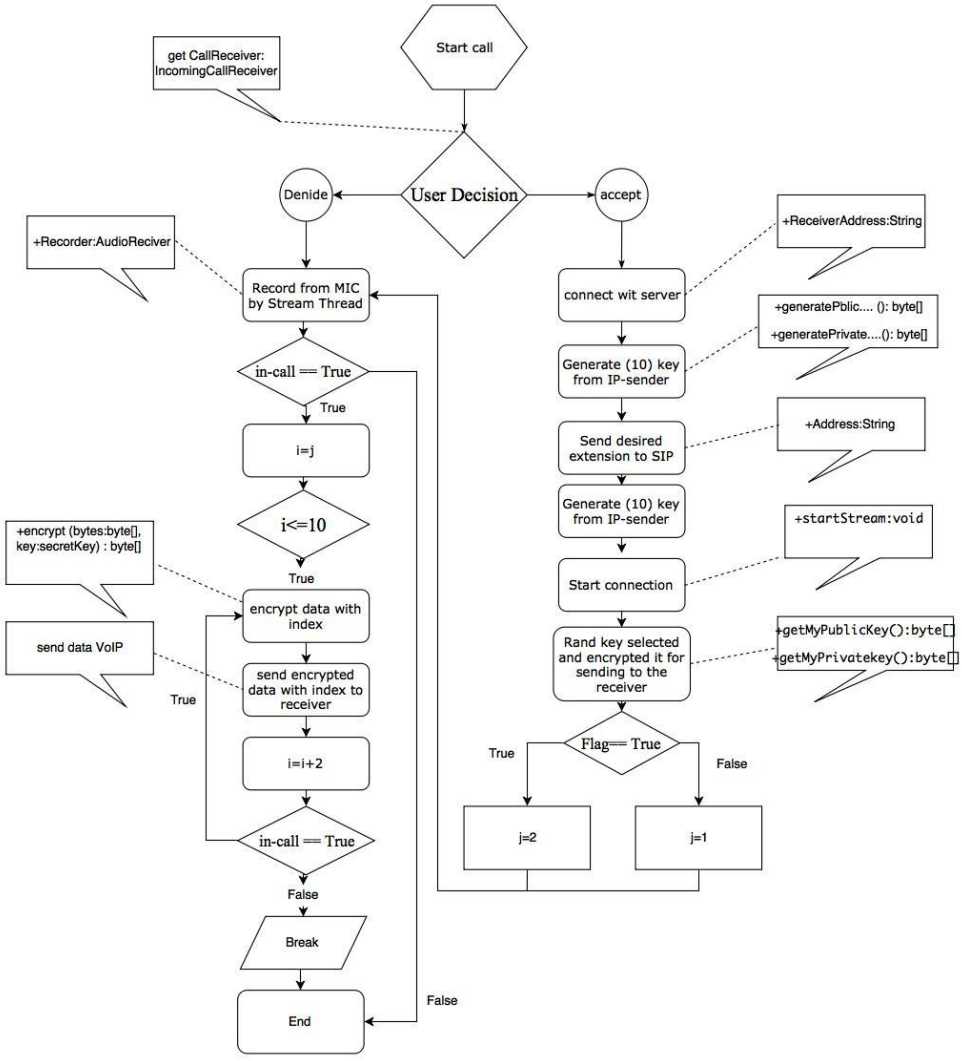



Figure 3.5: Enc. Algorithm

### 3.3.4 AES-DH Decrypt Flowchart

This part is used to receive encrypted data from the sender, then decrypt this data and combine it; look at Figure 3.6.

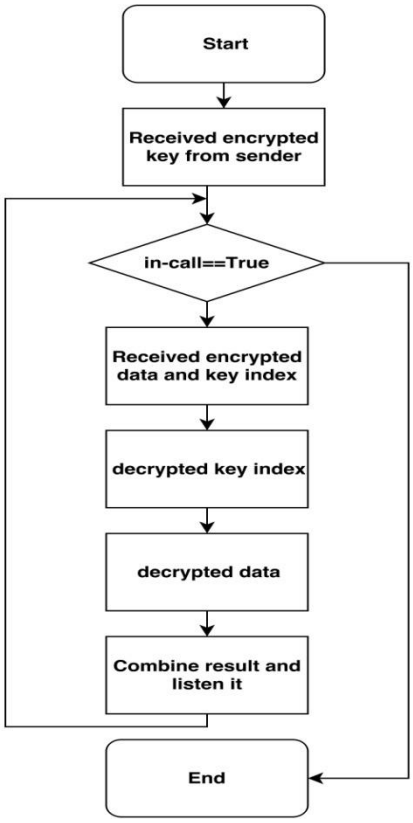



Figure 3.6: Dec.Algorithm

Figure 3.7 show the steps for encryption and decryption use AES with DH algorithm for plain text "hello my friend" to output.

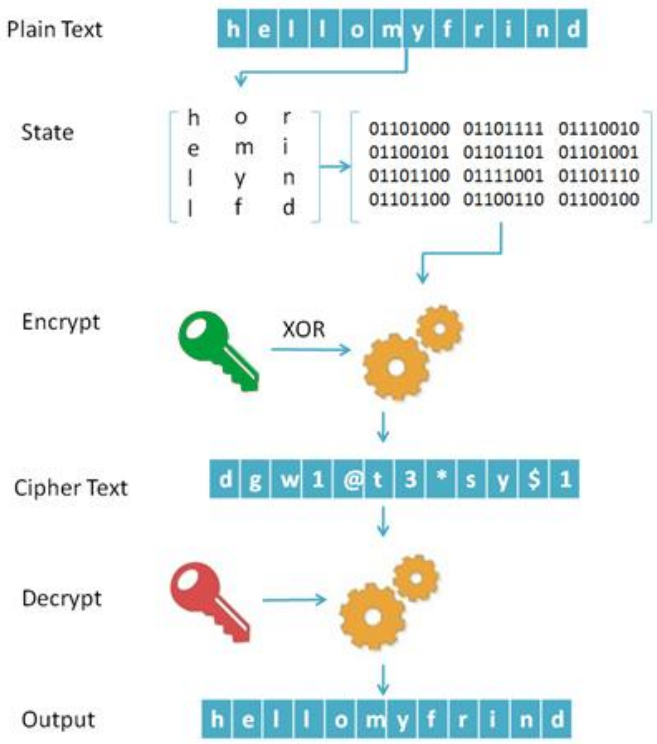



Figure 3.7: Hello example

## 3.4 Summary

Chapter threepresented the suitable method for the suggested problem, and declares the proposed module through algorithms and flowcharts. Each of the algorithms explains one of the parts in the module. Also this chapter focuses on the module that aims for accepting achieved results. The module aims to:

1- Ensure encryption process by AES algorithm, which handles delay voice transfer quickly to the receiver.

2- Ensure encryption packet using a DH algorithm to prevent anti-eavesdropping on clients.

# Chapter Four:Experimental Work

## 4.1 Introduction

Communication has beenan important issue recently. So,voice data is the most important type of data communication that needs to be protected.VoIP is the protocol for transmitting voice data using the internet. ButVoIPcan be targeted by various types of attacksusing easy wayscalledeavesdropping communications,capturing packets, etc.

The weakness point in VOIP is how to manageit;usingVoIP technologies by two parties (sender and receiver) is likely to be risky without controlling sensitive data that can be eavesdropped by intruders. For that purpose, the sender and receiver should share a session key by the server before any communication. Therefore, this key is exchanged over the network to be used based on providing a secured channel.

IP telephony is an emerging technology that enables a range of new service possibilities. Although it uses various protocols such as (UDP and TCP), this technology is added to the SIP server which seems to be the standard applications that are widely adopted by different VoIP communities. The services that the VoIP providers offer their customers whatever they need to reach a certain secure maturity level.

The module, i.e. AES-DH, is implemented by additional new interface between the two parties. It is built outside the SIP server. The sender part uses the AES-DH algorithm for encrypting voice before transmitting it to the other party by SIP server, and the receiver will use the same algorithm in reverse to decrypt the voice, as shown in Figure 4.1:

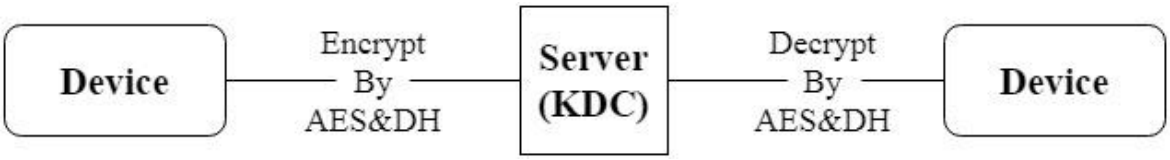



Figure 4.1: Framework

## 4.2 Interfaces Execution

The execution of application throughout the experiment is divided into four procedures:

### 4.2.1 Admin Procedure

The main interface shown in SIP server is the admin interface. It includes (Language, User name and Password).After pressing the log-in button, the next interface will include all the registered users in SIP server. The green point is for online or active user; the red point for offline user.When the user chooses the extensions option, the next interface appears for adding new extensions to the SIP server by filling the required information in this interface.After the admin clicks the apply button, another interface will appear.

The admin can edit any extension in the SIP server by choosing the user who wants to edit the information after that interface will appear and the admin can edit the information.When one of party decided to call another party.Through calling process between two parties, e.g. from 12 extensions to 10 extensions.

### 4.2.2 Register Procedure:

During installation of the application in a mobile, the main interface will appear showing a message which states that the user is not registered.

When the user clicks the ok button, another interface which includes (Enter Username, Enter Domain and Enter Password). the user enters the username using numbers or

characters and enters the SIP name through the IP of the SIP server last one the user enters the password.

### 4.2.3 Call Procedure

At the end of the registration process, the call procedure will begin. The message shows a ready notification to the user and he is now ready to make the call between the parties.

The application can initiate thecalling process either by IP domain of the receiver or add by name receiver.When the calling process begins the address of the destination will appear.

### 4.2.4 Fail Procedure

If the SIP server is turned off or the registration process fails, the application displays a message to the user for editing information in settings.

## 4.3 Environment Parameter

This part will explain the results obtained through the implementation of the program on PC (CPU 1.70 GHz, RAM 8 GB) with Samsung mobile device. This type is (galaxy s5) whose CPU is 1GHz and RAM 8 GB; the router used is 108 megabytes per second the speed of transmitting data.

## 4.4Experiment scenarios

We have done the experiment in six scenarios with different Parameterwhich are clarified as the table 4.1below:

Table 4.1:The experiment scenarios

| Scenario N0. | Parameter | | |
|---|---|---|---|
| | Key Size (bit) | Message Size (KB) | Router (MB/s) |
| 1 | 128 | 20 | 108 |
| 2 | 192 | 20 | |
| 3 | 256 | 20 | |
| 4 | 256 | 10 | |
| 5 | 256 | 40 | |
| 6 | 256 | 10 | 54 |

1. **Scenario with key size 128 (bit), message size 20 (KB) and with router 108 (MB/S):**

A key size of 128 bit is used with a messagesize for the sender is 20016 bytes, including 16 byte for key. It will be receiving 20 KB. Table 4.2 shows the estimated time to make the encryption, decryption, delay and number of packet loss. Each scenario includes 20 different acts of contact between the sender and the receiver to calculate the average time for the scenario which, by turn, guarantees readings and results. It is time consuming to display the results of each scenario, therefore, the researcher suffices with showing one example and then displays the average time for the same algorithm in Figure 4.2 below.

Table 4.2:The first experiment part 1.

| AES and DH algorithm 128 bit | | | | |
|---|---|---|---|---|
| **Process No.** | **Encryption Time (ms)** | **Decryption Time (ms)** | **delay time (ms)** | **packet loss** |
| **1** | 5 | 7 | 2 | 2 |
| **2** | 3 | 5 | 2 | 1 |

| | | | | |
|---|---|---|---|---|
| **3** | 4 | 9 | 4 | 3 |
| **4** | 7 | 10 | 3 | 2 |
| **5** | 3 | 6 | 3 | 0 |
| **6** | 9 | 14 | 5 | 4 |
| **7** | 5 | 8 | 3 | 2 |
| **8** | 6 | 10 | 4 | 3 |
| **9** | 4 | 8 | 4 | 1 |
| **10** | 4 | 7 | 4 | 0 |
| **11** | 4 | 9 | 3 | 2 |
| **12** | 5 | 7 | 2 | 4 |
| **13** | 7 | 11 | 4 | 5 |
| **14** | 4 | 7 | 4 | 3 |
| **15** | 5 | 7 | 2 | 2 |
| **16** | 4 | 6 | 5 | 1 |
| **17** | 6 | 9 | 3 | 2 |
| **18** | 5 | 9 | 4 | 0 |
| **19** | 6 | 8 | 2 | 2 |
| **20** | 7 | 13 | 6 | 2 |
| **Totalrange time** | **103** | **170** | **69** | **41** |
| **Average Time** | **5.15** | **8.5** | **3.45** | **2.05** |

Table 4.3:The first experiment part 2.

| **AES algorithm 128 bit** | | | | |
|---|---|---|---|---|
| **Process No.** | **Encryption Time (ms)** | **Decryption Time (ms)** | **delay time (ms)** | **packet loss** |
| **1** | 2 | 2 | 2 | 1 |
| **2** | 3 | 4 | 1 | 1 |
| **3** | 3 | 3 | 0 | 2 |
| **4** | 4 | 5 | 1 | 2 |
| **5** | 2 | 4 | 3 | 0 |

| | | | | |
|---|---|---|---|---|
| **6** | 5 | 6 | 5 | 2 |
| **7** | 5 | 8 | 3 | 2 |
| **8** | 3 | 5 | 2 | 3 |
| **9** | 2 | 5 | 3 | 2 |
| **10** | 1 | 3 | 4 | 0 |
| **11** | 2 | 4 | 2 | 2 |
| **12** | 3 | 5 | 2 | 3 |
| **13** | 4 | 4 | 2 | 2 |
| **14** | 4 | 4 | 1 | 1 |
| **15** | 5 | 6 | 4 | 0 |
| **16** | 3 | 4 | 1 | 1 |
| **17** | 5 | 6 | 1 | 0 |
| **18** | 3 | 4 | 3 | 0 |
| **19** | 3 | 5 | 2 | 1 |
| **20** | 2 | 3 | 2 | 3 |
| **Totalrange time** | **64** | **90** | **44** | **28** |
| **Average Time** | **3.2** | **4.5** | **2.2** | **1.4** |

Table 4.4:The first experiment part 3.

| **Silent** | | | | |
|---|---|---|---|---|
| **Process No.** | **Encryption Time (ms)** | **Decryption Time (ms)** | **delay time (ms)** | **packet loss** |
| **1** | 0 | 0 | 0 | 1 |
| **2** | 0 | 0 | 1 | 0 |
| **3** | 0 | 0 | 0 | 1 |
| **4** | 0 | 0 | 1 | 2 |
| **5** | 0 | 0 | 1 | 1 |
| **6** | 0 | 0 | 0 | 1 |
| **7** | 0 | 0 | 0 | 0 |
| **8** | 0 | 0 | 0 | 1 |

| | | | | |
|---|---|---|---|---|
| **9** | 0 | 0 | 1 | 0 |
| **10** | 0 | 0 | 1 | 0 |
| **11** | 0 | 0 | 1 | 0 |
| **12** | 0 | 0 | 1 | 2 |
| **13** | 0 | 0 | 1 | 1 |
| **14** | 0 | 0 | 1 | 1 |
| **15** | 0 | 0 | 0 | 0 |
| **16** | 0 | 0 | 0 | 0 |
| **17** | 0 | 0 | 1 | 1 |
| **18** | 0 | 0 | 1 | 0 |
| **19** | 0 | 0 | 0 | 1 |
| **20** | 0 | 0 | 0 | 1 |
| **Totalrange time** | 0 | 0 | **11** | **14** |
| **Average Time** | 0 | 0 | **0.55** | **0.7** |

The results show the average time for (AES-DH) and (AES only) algorithm and normal way (silent). we captured three parameters while running the sessions: execution time for both encryption and decryption processes, propagation delay, and number of lost packets. shown in the three tables above. This scenario uses messageSize (20KB) and key size (128 bit)as shown in Figure 4.2.

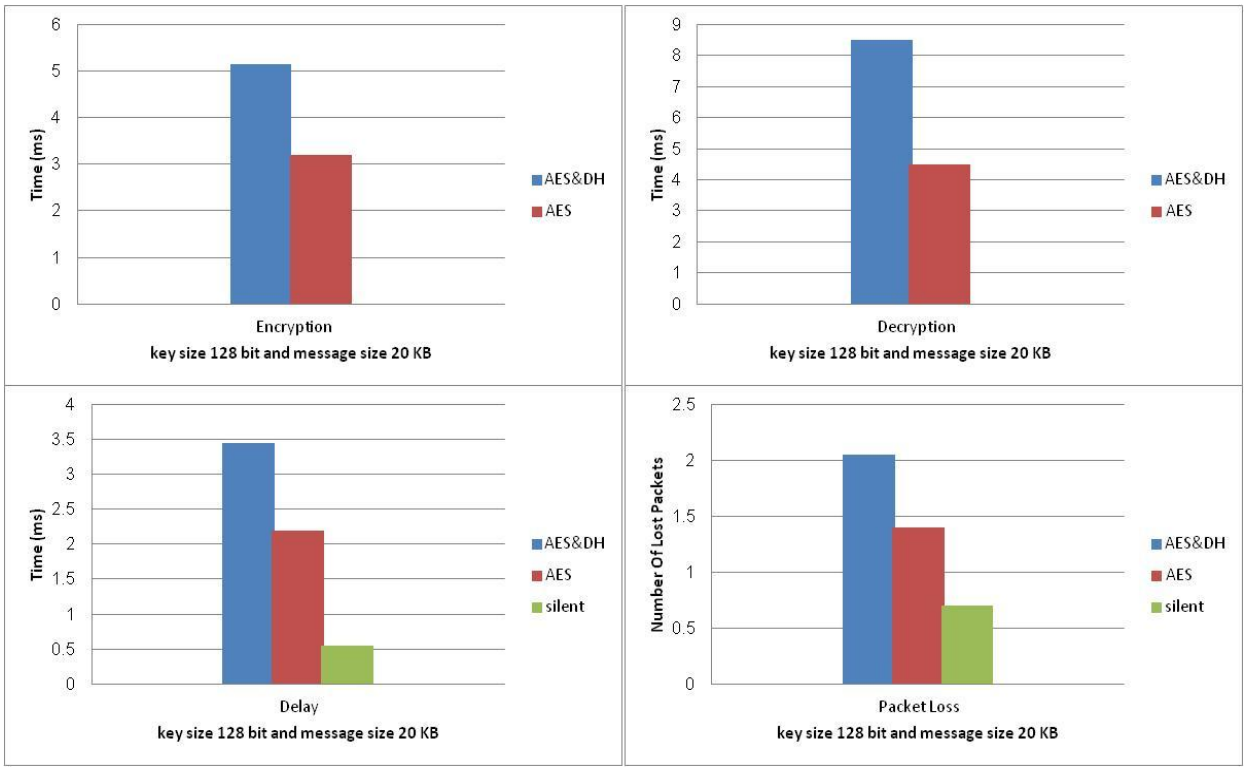



Figure 4.2:Scenario 1 results (128 key, 20 KB message)

In Figure 4.2 It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH. If we average the encryption time, we get 3.2 ms for the AES alone vs. 5.15 ms for AES-DH; or 1.95 ms increase. In the same way, if we average the decryption time, we get 8.5 ms for the AES-DH vs. 4.5 ms for AES alone; around 4 ms increase. If we repeat the same analysis for the propagation delay we get around 1.25ms and 2.9 msincrease, and on average the number of  lost we get around 0.65 ms and 1.35 ms increase.

**2. <u>Scenario with key size 192 (bit), message size 20 (KB) and with router 108 (MB/S):</u>**

A key size of 192 bit is used with a messagesize of the sender as 20016 bytesincluding 16 bytes for key. It will be receiving 20 KB.

The results show the average time for (AES-DH) and (AES only) algorithm and normal way (silent). we captured three parameters while running the sessions: execution time for both

encryption and decryption processes, propagation delay, and number of lost packets. It usesthe fixed messageSize (20 KB) and key size (192 bit)as shown in Figure 4.3.

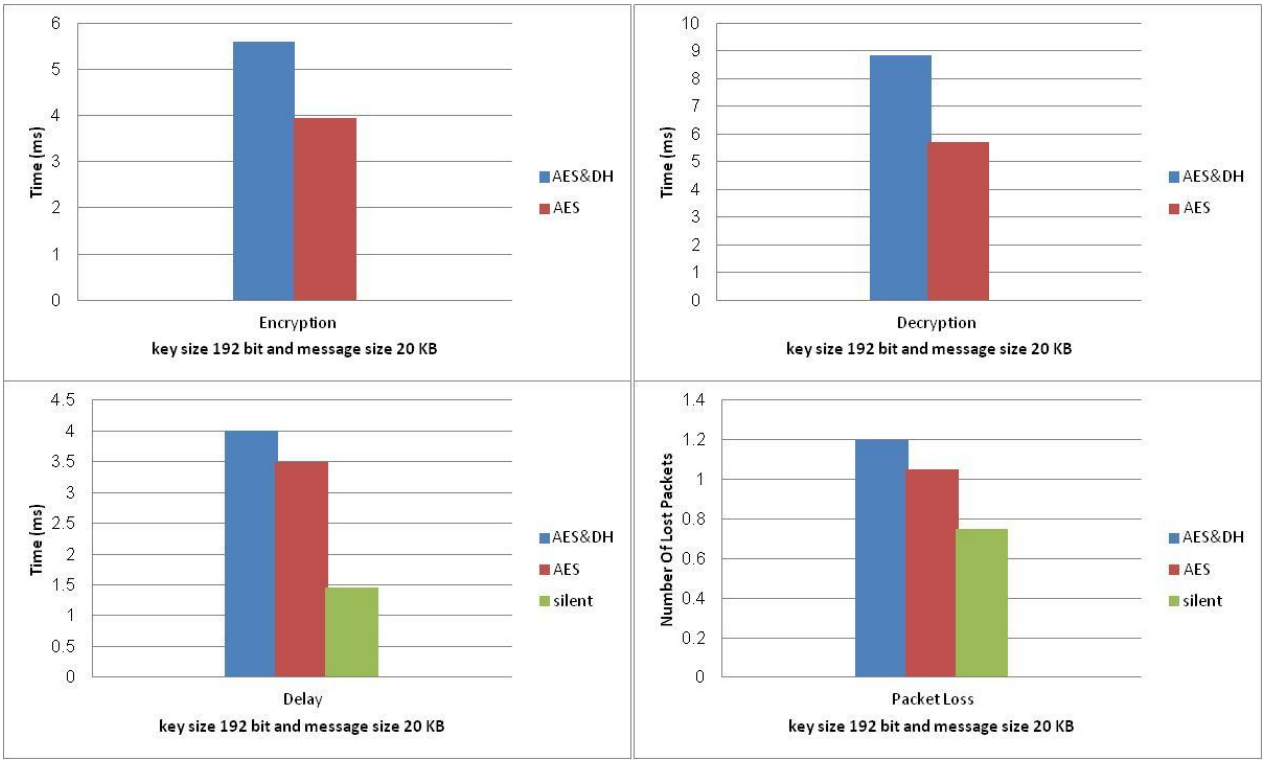



Figure 4.3:Scenario 2 results (192 key, 20 KB message)

In Figure 4.3 It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH. If we average the encryption time, we get 3.95 ms for the AES alone vs. 5.6 ms for AES-DH; or 1.65 ms increase. In the same way, if we average the decryption time, we get 8.85 ms for the AES-DH vs. 5.7 ms for AES alone; around 4 ms increase. If we repeat the same analysis for the propagation delay we get around 1. 5 ms and 2.5 ms increase, and on average the number of lost we get around 0.15 ms and 0.45 ms increase.

### 3. Scenario with key size 256 (bit), message size 20 (KB) and with router 108 (MB/S):

A key size of 256 bit is used with a messagesize of the sender as 20016 bytes, including 16 bytes for key. It will be receiving 20 KB.

The results show the average time for (AES-DH) and (AES only) algorithm and normal way (silent). we captured three parameters while running the sessions: execution time for both

encryption and decryption processes, propagation delay, and number of lost packets. It usesthe fixed messageSize (20 KB) and key size (256 bit), as shown in Figure 4.4.

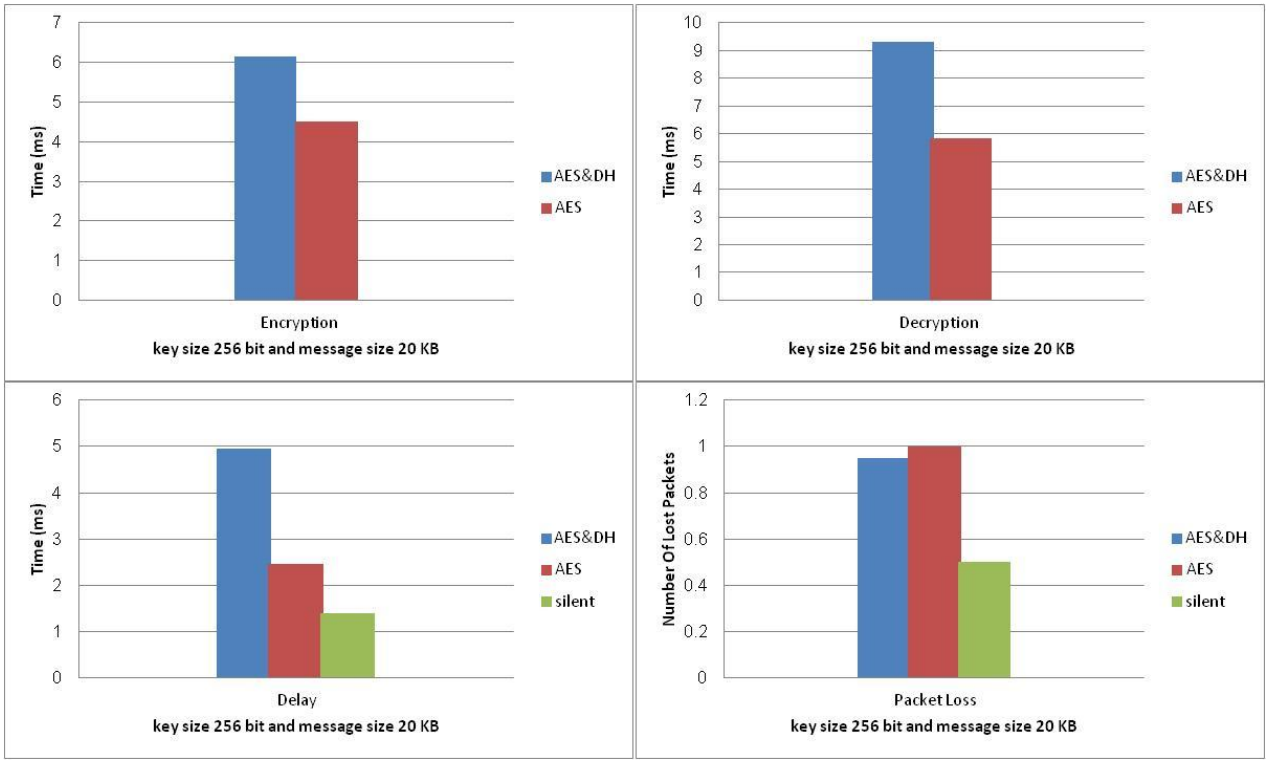



Figure 4.4:Scenario 3 results (256 key, 20 KBmessage)

in Figure 4.4 It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH. If we average the encryption time, we get 4.5 ms for the AES alone vs. 6.15 ms for AES-DH; or 1.65 ms increase. In the same way, if we average the decryption time, we get 9.3 ms for the AES-DH vs. 5.85 ms for AES alone; around 3.4 ms increase. If we repeat the same analysis for the propagation delay we get around 2.5 ms and 3.5ms increase,and on average the number of lost we get around 0.05 ms increase for AES-DH and 0.45 for silent.

**4. <u>Scenario with key size 256 (bit), message size 10 (KB) and with router 108 (MB/S):</u>**

A key size of 256 bit is used with a messagesize of the sender as 10016 bytes, including 16 bytes for key. It will be receiving 10 KB.

The results show the average time for (AES-DH) and (AES only) algorithm and normal way (silent). we captured three parameters while running the sessions: execution time for both encryption and decryption processes, propagation delay, and number of lost packets. It uses the fixed messageSize (10KB) and key size (256 bit) as shown in Figure 4.5.

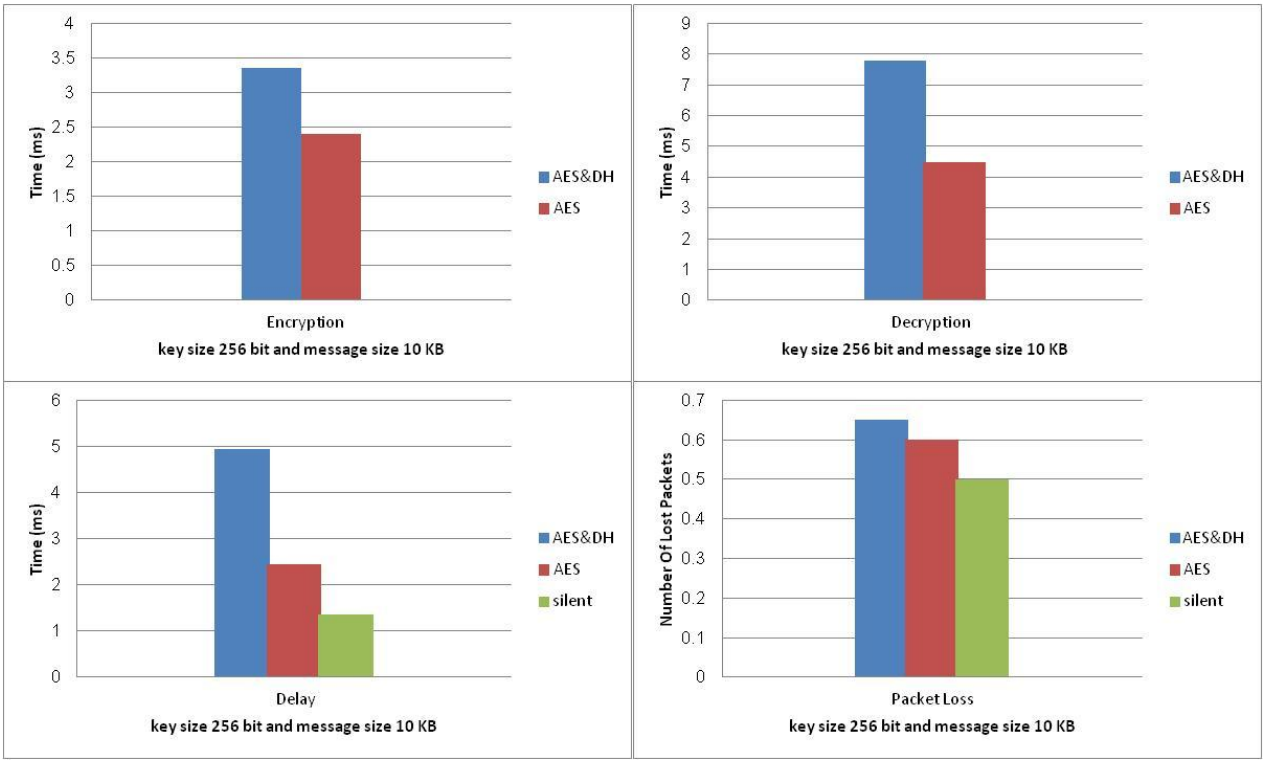



Figure 4.5:Scenario 4 results (256 key, 10 KB message)

In Figure 4.5 It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH. If we average the encryption time, we get 2.4 ms for the AES alone vs. 3.35 ms for AES-DH; or 1 ms increase. In the same way, if we average the decryption time, we get 7.8 ms for the AES-DH vs. 4.5 ms for AES alone; around 3 ms increase. If we repeat the same analysis for the propagation delay we get around 2. 5 ms and 3.6 ms increase, and on average the number of lost we get around 0.05 ms and 0.25 ms increase.

**5. <u>Scenario with key size 256 (bit), message size 40 (KB) and with router 108 (MB/S):</u>**

A key size of 256 bit is used with a messagesize of the sender as 40016 bytes, including 16 bytes for key. It will be receiving 40 KB. The results show the average time for (AES-DH)

and (AES only) algorithm and normal way (silent). we captured three parameters while running the sessions: execution time for both encryption and decryption processes, propagation delay, and number of lost packets. It uses the fixed messageSize (40 KB) and key size (256 bit) as shown in Figure 4.6.

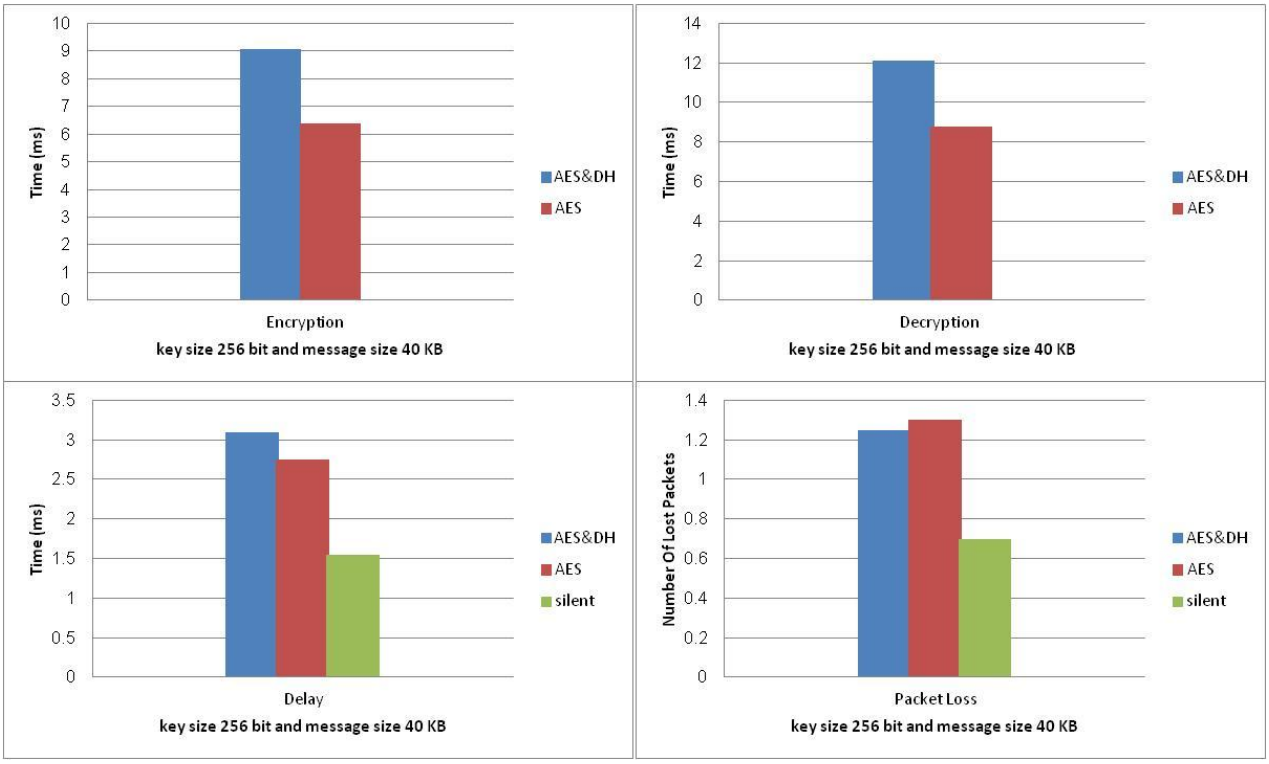



Figure 4.6Scenario 5 results (256 key, 40 KB message)

In Figure 4.6 It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH. If we average the encryption time, we get 6.4 ms for the AES alone vs. 9 ms for AES-DH; or 2.6 ms increase. In the same way, if we average the decryption time, we get 12 ms for the AES-DH vs. 8.8 ms for AES alone; around 3 ms increase. If we repeat the same analysis for the propagation delay we get around 0.35 ms and 1.5 ms increase, and on average the number of lost we get around 0.05 ms increase for AES-DH and 0.55 for silent.

**6. <u>Scenario with key size 256 (bit), message size 10 (KB) and with router 54 (MB/S):</u>**

It has used the same key size messageas in the fourth experiment, but using different devices which are router 54 megabyte per second, and PC with different properties (CPU 1800 GHz, RAM 2GB),Samsung mobile device. This device is (Grand prime+) CPU 1 GHz, RAM 4 GB.

The results show the average timefor (AES-DH) and (AES only) algorithm and normal way(silent).we captured three parameters while running the sessions: execution time for both encryption and decryption processes, propagation delay, and number of lost packets.It uses the fixed messageSize (10 KB) and key size (256 bit) as shown in Figure 4.7.

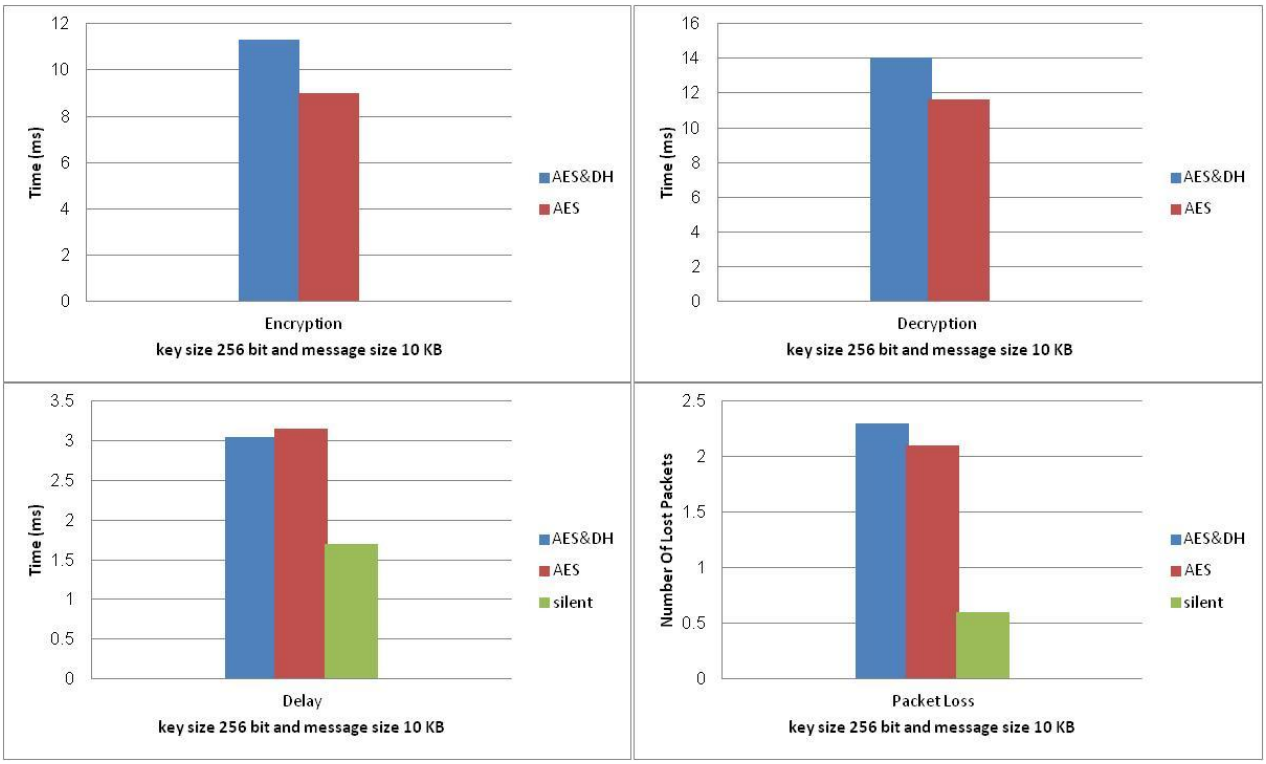



Figure 4.7: Scenario 6 results (256 key, 10 KB message)

In Figure 4.7It is obvious that in the four plots that the AES algorithm is slightly faster than the AES-DH except the propagation delay. If we average the encryption time, we get 9 ms for the AES alone vs. 11.3 ms for AES-DH; or 2.3 ms increase. In the same way, if we average the decryption time, we get 14ms for the AES-DH vs. 11.6 ms for AES alone;

around 2.6 ms increase. If we repeat the same analysis for the propagation delay we get around 0.1 ms increase for AES and 1.45 for silent, and on average the number of lostwe get around 1.2 ms increase for AES-DH and 1.7 for silent.

**The effects of the key size and messagesize:**The results show the effects of the key size and message size on the encryption and decryption average time for AES only while using the changed messageSize (10,20 and 40 KB) and changed key size (128, 192 and 256) bit, as shown in Figure 4.8.

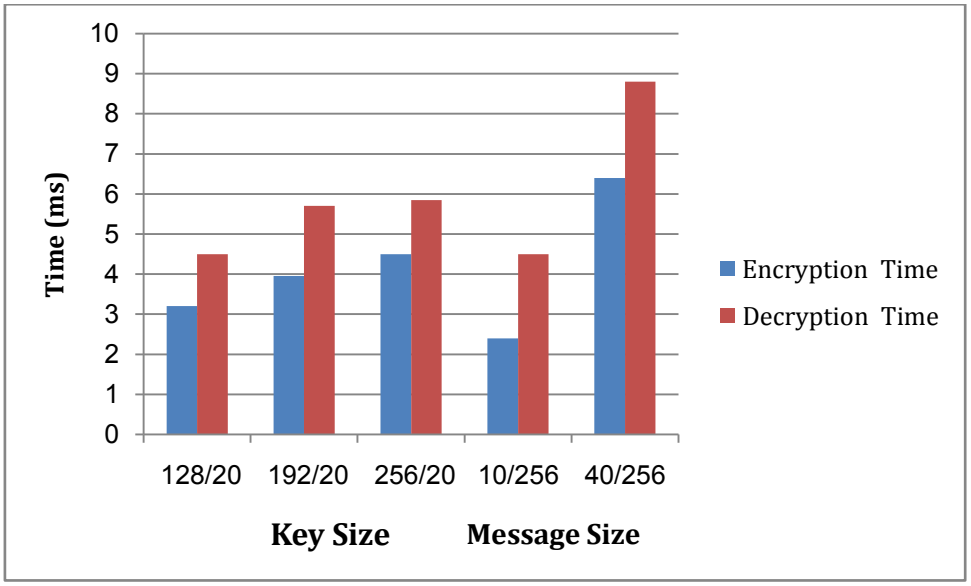



Figure 4.8: The results show the effects of the key size and messagesize on the Encryption & Decryption average time for AES only.

The results also show the effects of the key size and messagesize on the encryption and decryption average time for AES-DH while is using the changed messageSize (10,20 and 40 KB) and changed key size (128, 192 and 256) bit, as shown in Figure 4.9.

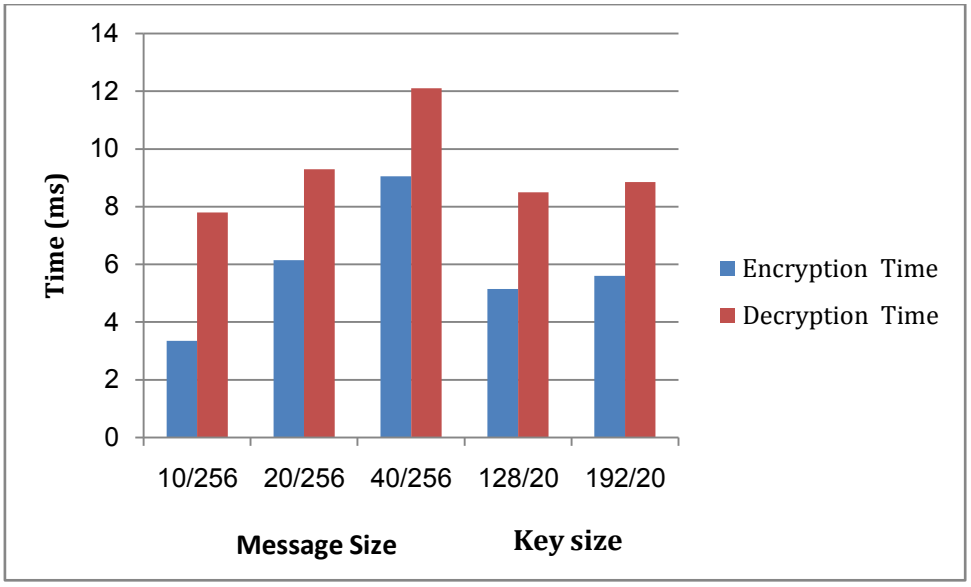



Figure 4.9: The results show the effects of the key size and messagesize on the Encryption & Decryption average time for AES-DH.

**The result conclusion:**The overall objective of experimentis to show how secure and speedy each algorithm has been; the results show that the speed and security of AES and AES-DH algorithmaredifferent depending on the key size (128, 129and 256 bits)andmessagesize (10,20 and 40 KB).

However, we must analysis the result, It is obvious that in the four plots for each scenario that the AES algorithm is slightly faster than the AES-DH. For example, if we average the encryption time for the three cases (key sizes: 128,192 and 256 bits) we get 3.8 ms for the AES alone vs. 5.5 ms for AES-DH; or 1.7 ms increase. In the same way, if we average the decryption time, we get 24 ms for the AES-DH vs. 16.5 ms for AES alone; around 8 ms increase. If we repeat the same analysis for the propagation delay we get around 4.5 ms increase, and on average the number of lost packets is almost the same for both cases. It is obvious that we have added some overhead due to the extra work being done specially during encryption and decryption processes to engage the DH algorithm, but we can say that the summation of all three times (encryption, decryption and delay) has increased by 14.5

ms in total (average of the three key sizes), which is totally acceptable for voice communication.

To get more insights into the behavior of both algorithms, we carried another set of experiments by fixing the key size to 256-bit and tested with three messagesizes (10 KB, 20 KB and 40 KB). The experimental results of this test are shown in Figures above. Based on this set of experiments we find: there is an added overhead in the three-time plots (encryption, decryption and delay), but for the number of lost packet, the performance is almost equal, it is also obvious in these plots, that the larger the packet, the better (i.e., less overhead is added). if we perform the time analysis by averaging the total times for the three messagesizes, we get the following numbers: encryption time has increased by 5 ms, decryption time has increased by 10 ms, and propagation delay time has increased by 5 ms. Therefore, the average total overhead is around 20 ms, which is compatible with the pervious result (14.5 ms).The following table 4.6 showsthe conclusion result[26] [27] [28].

Table 4.6:The result conclusion

| **scenario No.** | **AES** | | **AES&DH** | |
|---|---|---|---|---|
| | **speed** | **security** | **Speed** | **Security** |
| 1 | Fast | Very Less | Fast | Less |
| 2 | Fast | Very Less | Somewhat Fast | Less |
| 3 | Somewhat Fast | Less | Somewhat Fast | High |
| 4 | Fast | Less | Somewhat Fast | Secure |
| 5 | Somewhat Slow | Secure | Somewhat Slow | Very Secure |

In this module the researcher aims to choose the best scenario (scenario No. 3) in terms of speed (high speed) and security (more secured) for the two approaches. When using a key size of 256 bit and a messagesize of20 KB forAES-DH algorithm, speed was higher than

any other key size or messagesize and security was also better. Furthermore, using the same scenario, the voice data that the receiver listens to the has been fine without delay and he has enough time to decrypt it.In this experiment the researchercompares between (AES-DH) algorithm and other algorithm (AES) to show if we improve security and speed without delay.

The results have shown that we can get a significant increase in the encryption strength at a very small overhead for our algorithm AES-DH compare with basic algorithm (AES), We believe this small overhead which was incurred by added time of encryption and decryption is worth the effort to increase the security level of the channel and is still valid for voice communication. Table 4.7 shows theoverhead percentage for AES-DH for the six cases of our experiment.

Table 4.7:The Overheadresult for AES-DH.

| **scenario No.** | **AES&DH** | |
|---|---|---|
| | **Key size/ Messagesize** | **Overhead %** |
| 1 | 128/20 | 7% |
| 2 | 192/20 | 5% |
| 3 | 256/20 | 7% |
| 4 | 256/10 | 6% |
| 5 | 256/40 | 6% |
| 6 | 256/10 | 4% |

## 4.5 Validation

In this section we provide some analysis on the validity of our technique and its worthiness versus the small amount of overhead incurred by the added work of employing the DH algorithm on top of the AES.

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain. Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised.

Based on the methodology used, attacks on cryptosystems are categorized as follows:

- **Brute force attack:**In this module we assume that both algorithmswere attacked by brute force attackers for different key sizes (128, 192 and 256 bit keys), and we show the possible number of key combinations.

  The number of combination for each algorithm is will take from rounds to check every possible key combination starting with "0000." Given sufficient time, a brute force attack is applicable to any algorithm and is unable to break any algorithm because it depends on the length of the real key and the standard if the key length exceeds 128 bit is safe from this attack. For example, the brute force attack on a 4-bit key is to take,maximum, 16 rounds to check every possible key combination[49].Table 4.8 summarizes these numbers.

Table 4.8:possible number of key combinations

| **key size** / **Algorithm** | **AES Combinations** | **AES&DH Combinations** |
|---|---|---|
| 128 bit | $3.4x10^{19}$ | $11.56x10^{76}$ |
| 192 bit | $6.2x10^{28}$ | $38.44x10^{114}$ |
| 256 bit | $1.1x10^{38}$ | $1.21x10^{154}$ |

The probability of the hacker's success to decipher the channel for both AES and AES-DH.

**First scenario:**There is a physical argument that a 128-bit for AES key is computationally secure against brute-force attack. Just consider the following:

- Supercomputer: K Computer.
- Speed: 10.51 Pentaflops = 10.51 x $10^{15}$ Flops [Flops = Floating point operations per second]
- Flops required per combination check = 1000 (very optimistic but just assume for now)

- Combination checks per second = $(10.51 \times 10^{15}) / 1000 = 10.51 \times 10^{12}$
- Seconds in a Year = 365 x 24 x 60 x 60 = 31536000
- No. of Years to crack AES with 128-bit Key = $(3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$
  $= (0.323 \times 10^{26})/31536000$
  $= 1.02 \times 10^{18}$ years
  = 1 billion billion years
- No. of possible time to hack the key by hacker = $1/1.02 \times 10^{18}$ years = $0.98 \times 10^{-18}$

**Second scenario:**There is also a physical argument that a 128-bit for AES-DH key is computationally secure against brute-force attack. Just consider the following:

- Supercomputer: K Computer
- Speed: 10.51 Pentaflops$10.51 \times 10^{15}$ Flops [Flops = Floating point operations per second]
- Flops required per combination check = 1000 (very optimistic but just assume for now)
- Combination checks per second = $(10.51 \times 10^{15}) / 1000 = 10.51 \times 10^{12}$
- Seconds in a Year = 365 x 24 x 60 x 60 = 31536000
- No. of Years to crack AES-DH with 128-bit Key = $(11.56 \times 10^{76}) / [10.51 \times 10^{12}) \times 31536000]$
  $= (1.099 \times 10^{64})/31536000$
  $= 3.484 \times 10^{56}$ years
  = 3 billion billion years
- No. of possible time to hack the key by hacker = $1/3.484 \times 10^{56}$ years = $0.287 \times 10^{-56}$

Table 4.9 below, shows the probability of the hacker's success to decipher the channel for both AES and AES-DH.

Table 4.9:The probability of the hacker's success to decipher the channel

| **key size** / **Algorithm** | **AES Probability** | **AES-DH Probability** |
|---|---|---|
| 128 bit | $0.980 \times 10^{-18}$ | $2.87 \times 10^{-57}$ |
| 192 bit | $0.534 \times 10^{-37}$ | $8.62 \times 10^{-96}$ |

| | | |
|---|---|---|
| 256 bit | $0.302 \times 10^{-56}$ | $2.74 \times 10^{-134}$ |

It is obvious that hacker's chances to succeed are much harder with the AES-DH method.It will take him many billions of years to manage to get the correct key combinations; and this validates our original claim that we can reach a total new level of security with this added layer and we have made it almost impossible for any hacker to compromise the voice channel and decrypt the VoIP data.

- **Meet-in-the-middle attack:**The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place[50].Table 4.10 below, shows the complexity timefor AES and AES-DH.

Table 4.10: Meet-in-the-middle attack

| Algorithm | AES | AES-DH |
|---|---|---|
| 128 bit | $2^{126.1}$ | $2^{128}$ |
| 192 bit | $2^{189.7}$ | $2^{201}$ |
| 256 bit | $2^{254.4}$ | $2^{261.2}$ |

- **Chosen-ciphertext attack:**Is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption[51]. Table 4.11 below, shows the complexity time for AES and AES-DH.

  Table 4.11: chosen-ciphertext attack

| Algorithm | AES | AES-DH |
|---|---|---|
| 128 bit | $2^{54}$ | $2^{87}$ |
| 192 bit | $2^{65}$ | $2^{109}$ |
| 256 bit | $2^{76}$ | $2^{182}$ |

- **Chosen-plaintext attack:**In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of

determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA and DH is also vulnerable to chosen-plaintext attacks[51]. Table 4.12 below, shows the complexity time for AES and AES-DH.

Table 4.12: Chosen-plaintext attack

| Algorithm | AES | AES-DH |
|---|---|---|
| 128 bit | $2^{61}$ | $2^{77}$ |
| 192 bit | $2^{73}$ | $2^{90}$ |
| 256 bit | $2^{80}$ | $2^{110}$ |

- **Square attack:**It is an extension of differential cryptanalysis. Differential analysis looks at pairs of inputs that differ in only one-bit position, with all other bits identical. Integral analysis, for block size b, holds b-k bits constant and runs the other k through all 2k possibilities. For k=1, this is just differential cryptanalysis, but with k>1 it is a new technique[52]. Table 4.13 below, shows the complexity time for AES and AES-DH.

Table 4.13: Square attack

| Algorithm | AES | AES-DH |
|---|---|---|
| 128 bit | $2^{114}$ | $2^{154}$ |
| 192 bit | $2^{139}$ | $2^{189}$ |
| 256 bit | $2^{188}$ | $2^{235}$ |

- **Plain-text sensitivity attack:** A cryptosystem should be sensitive.To ensure itsensitive we should measure it by tools for our cryptosystem against this attack. However, the percentage of change in bits of cipher text obtained after encryption of plaintext, which is derived by changing single bit from the original plaintext from the bits of cipher text obtained after encryption of original plaintext. With the change in single bit of plaintext, there. must be ideally 50% change in bits of cipher text to resist differential cryptanalysis (chosen-plaintext attack) and statistical analysis[55], TheHD result is very close to the optimal value (50%)is 0.491511 (49%).

- **Key sensitivity attack:**Key sensitivity is very important for any cryptosystem because any change in the secret key will get different ciphered audio.However, the percentage of change in bits of cipher text obtained after encryption of plaintext using key, which is flipped by single bit from the original key, from bits of cipher text obtained after encryption of plaintext using original key, which requires ideally 50% change in cipher text bits to resist linear and statistical attacks.In our experiment we test Hamming Distance (HD)as a new metric measurement.It is used to quantify the avalanche effect in audio andthe optimum HD value is 50%[55]. In ourexperiment the HD value is very close to the optimal value (50%)is 0.498536 (49%).

- **Timing attack:**They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is being possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long[54]. Table 4.15 below, shows the complexity time for AES and AES-DH.

Table 4.15: Timing attack

| Algorithm | AES | AES-DH |
|---|---|---|
| 128 bit | $0.32 \times 10^9$ | $0.51 \times 10^9$ |
| 192 bit | $1.50 \times 10^9$ | $2.22 \times 10^9$ |
| 256 bit | $4.12 \times 10^9$ | $6.0 \times 10^9$ |

# Chapter Five:Conclusion and Future works

## 5.1 Conclusion

In this work, we have designed module for securing a VoIP channel by combining the AES encryption algorithm and the DH key-exchange algorithm. We have experimented with a real testbed including two mobile devices and a SIP server. We have shown that the module will increase the security level of the voice channel at a very small overhead (between 4% and 7%) of execution time between AES and AES combine with DH for all scenario which was incurred by added time of encryption and decryption.Since VoIP calls are usually low-cost or almost free service these days, it is currently wide spread among billions of Internet users; and therefore, VoIP calls can be subjected to several types of attacks like eavesdropping, capturing packets, and interference. So, it is of great importance that we increase the security of these channels to maintain high level of confidentiality for the users. By combining the two algorithms in one process that we have called (AES-DH); we have benefited from AES's speed and DH's strength.

In the future, we plan to investigate and experiment our strategy with other algorithms and other kinds of media like video and chatting, and probably experiment on a bigger testbed.

## References


1. H. Fathi, S.S. Chakraborty, R. Prasad. (2009)." Voice over IP in Wireless Heterogeneous Networks". *Springer Netherlands.*

2. SivanagaswathiKallam. (2015). "Diffi-Hellman: Key Exchange and Public Key Cryptosystems". Math and Computer Science Department Indiana State University TerreHaute,IN,USA 9-30-2015.

3. Prateek Gupta, Vitaly Shmatikov. (2007). " Security Analysis of Voice-over-IP Protocols". *The National Science Foundation's under grants.*

4. Abdullah Azfar, (2014). "A Study of Ten Popular Android Mobile VoIP Applications: Are the Communications Encrypted?", *HawaiiInternational Conference*.

5. Saran Chiwtanasuntorn, (2014). "Perseus on VoIP: Development and implementation of VoIP platforms". *International Conference*.

6. Munef Zaid, (2015). "Securing VoIP in SIP Mobile Network". Computer *Science and Information Technology Journal*.

7. Voznak, M., Rozhon, J.: Performance testing and benchmarking of B2BUA and SIP Proxy. In: Conference Proceedings TSP 2010, Baden near Vienna, pp. 497–503 (2010).

8. Jianqiang Xin. (2007). "Security Issues and countermeasure for VoIP". *SANS Institute InfoSec Reading Room.*

9. Subashri, T. (2014). "Confidentiality of VOIP Data Using Efficient ECDH Key Exchanging Mechanism". *International Conference*.

10.Byounghee Son,(2013)." VoIP encryption module for securing privacy". *Multimed Tools Appl,*

11.Chittaranjan Pradhan, (2013). " Chaotic Variations ofAes Algorithm",*International Journal.*

12.Mr Prashant B Kumbharkar, (2014). " A Secure Overlay Dynamic Multicast Network with Load Balancing for Scalable P2P Video Streaming Services".*international journal of advanced computer technology*.

13.Jean-Franc Raymond ,AntonStiglic.(2009)." Security Issues in the Diffie-Hellman Key Agreement Protocol ". Cyber Infrastructure Protection.

14.Sans, (2005). Voice Over Internet Protocol (VoIP) and Security, https://www.sans.org/reading-room/whitepapers/voip/voice-internet-protocol-voip-security-1513, Accessed by 15-1-2014.

15.Forouzan, A., B., (2006). Data Communications & Networking (sie). Tata McGraw-Hill Education.

16.Stein, Y. and Malepati, H. (2008). Implementation of the AES algorithm on Deeply Pipelined DSP/RISC Processor, Accessed by 15-7-2014.

17.JaeikChoa, b , Ken Choi b , Jongsub Moon. (2013). "Power dissipation and area comparison of 512-bit and 1024-bit key AES". Computers & Mathematics with ApplicationsVolume 65, Issue 9, May 2013, Pages 1378-1383.

18.Rebahi.Y.,et al.:(2008)."Performance analysis of identity management in the Session Initiation Protocol (SIP)". in IEEE/ACS International Conference on Computer Systems and Applications 31 March-4 April 2008.

19.R. Vargic, et al. (2011)."Provisioning of VoIP services for mobile subscribers using WiFi access network". TelecommunSyst 18 October 2011.

20.Seung pyo Hong, et al.(2013). "Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA". Mathematical and Computer ModellingVolume 58, Issues 1–2, July 2013, Pages 254-260

21.Kilinc&Yanik.( 2014). "A Survey of SIP Authentication and Key Agreement Schemes". IEEE Communications Surveys & Tutorials Volume: 16, Issue: 2, Second Quarter 2014 .

22.HarjitPal Singh et al., (2014). "VoIP: State of art for global connectivity—A critical review". Journal of Network and Computer ApplicationsVolume 37, January 2014, Pages 365-379.

23.AchyutParajuli, (2015). " Survey of security features in Ultraprivate Smartphone technology".*Scientific Research Journal*.

24.Sahmoud Shaaban, (2013). "Enhancement the security of AES against modern attacks by using variable key block cipher". *International Arab journal of e-technology*. Vol. 3,No 1.

25.Demirici, J. and Mironov.( 2006)" cache-collision timing attacks aginst AES" *cryptographic hardware and embedded system*.pp.201-215.

26.Shan L, Jiang N. (2009)."Research on security mechanisms of SIP-based VoIP system." In Proc. of Int. Conf. on Hybrid Intelligent Systems, vol. 2, pp. 408–410.

27. Yoon S,Jeong J,Jeong H. (2010)."A study on the tightening the security of the key management protocol for VoIP". In Proc. of New Trends in Information Science and Service Science, pp. 638.

28.P.Premkumar, D.ShanthiD. (2014). "An Efficient Dynamic Data Violation Checking Technique For Data Integrity Assurance In Cloud Computing". International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.

29.B. Padmavathi, S. RanjithaKumarier.(2013). "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique".International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

30.Ching-Wei Chen, Markus Cremer. (2009)." Improving Perceived Tempo Estimation by Statistical Modeling of Higher-Level Musical Descriptors". Presented at the 126th Convention 2009 May 7–10 Munich, Germany.

31.M. Kas, B. Yargicoglu, I. Korpeoglu, E. Karasan, (2010). " A survey on scheduling in IEEE 802.16 mesh mode". IEEE Communications Surveys & Tutorials 205–221.

32.X. Wei, Y. Bouslimani,& K. Sellal, (2012)."VoIP Based Solution for the Use over a Campus Environment". 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), PP 1-5.

33.Jung Ji-Young,Seo Dong-Yoon & Lee Jung-Ryun, (2013). "VoIP Call Admission Control Scheme Considering VoIP on-off Patterns",*International Conference on Information Networking (ICOIN),* PP 271 – 385.

34.S. Sethi& V.Y. Hnatyshin, (2013). "The Practical OPNET User Guide for Computer Network Simulation",*CRC Press*.

35.Di Wu, (2008)."Performance Studies of VoIP over Ethernet LANs",*Thesis, Department of Computer andInformation, Auckland University of Technology*.

36.Mehaswari,K.Punithavalli, (2011). Design and Implementation of multipath routing approach for secured and reliable data delivery over VoIP.Publication in (IJAER- Vol:2).

37.P. Montoro, E. Casilari, (2009)"A comparative study of VoIP Standards with Asterisk". *Forth international conference On Digital telecommunication*.

38.Issam Mahdi Hammad, (2010) "Efficient Hardware Implementations For The Advanced Encryption Standard (AES) Algorithm" *Master Thesis, Dalhousie University Halifax, Nova Scotia*.

39.Monica Liberatori et al, (2007)"AES-128 Cipher. High Speed, Low Cost FPGA Implementation",*IEEE, pp. 185-20*0.

40.J. Rosenberg et al,(2006). "The Session Initiation Protocol (SIP) and Spam", draft-ietf-SIPping-spam-02, March 6, 2006.

41.D.Ambika,V.Radha.(2012). " Secure Speech Communication – A Review".

42.Harsh Kumar Verma, Ravindra Kumar Singh, (2012)." Performance Analysis of RC6,Twofish and Rijndael Block Cipher Algorithms".

43.Alo, U., R., and Firday, N., H., (2013). Voice over Internet Protocol (VOIP): Overview, Direction and Challenges. Journal of Information Engineering and Applications, Vol.3, No.4.

44.M. Han, D. Li, T. Jeong, (2011)."Adaptive security model in real-time intrusion detection environment".*Information-International Interdisciplinary Journal 14 (4) 1272–1482.*

45.H.S. Choi, J.H. Choi, J.T. Kim, (2008). "Low-power AES design using parallel architecture", in: *ICHIT'08, pp. 413–416*.

46.S. Pangpronpitag and P. Kasabai,(2012). "MSDES:More SDES Key Agreement for SRTP",*in I.J.C.T.E., Vol 4,No. 5*.

47.Baronak, I.,& Halas, M. (2007). Mathematical representation of VoIP connection delay. Radioengineering, 16(3), 77–85.

48. Mark Collier,(2005). "Basic Vulnerability Issues for SIP Security.pdf ", Chief Technology Officer Secure Logix Corporation.

49. Daniel J. Bernstein,(2005). " Understanding brute force ".The author was supported by the National Science Foundation under grant CCR– 9983950.
50. HuseyinDemirci, Ali Selcuk. (2008). " A Meet-in-the-Middle Attack on 8-Round AES".
51. Charles Bouillaguet, Nathan Kelle.(2011)." Low Data Complexity Attacks on AES". supported by the Koshland center for basic research.
52. Michael Tunstall. (2012)."Improved “Partial Sums”-based Square Attack on AES".
53. Alex Biryukov and Dmitry Khovratovich. (2010)." Related-key Cryptanalysis of the Full AES-192 and AES-256". Dmitry Khovratovich is supported by PRP ”Security& Trust” grant of the University of Luxembourg.
54. Emilia K¨asper, Peter Schwabe.(2010). "Faster and Timing-Attack Resistant AES-GCM".
55. Mousa Farajallah (2015). "Chaos-based crypto and joint crypto-compression systems for images and videos". UNIVERSITE DE NANTES, 2015. English.,

# Appendix I