Augmenting GSM Security Focusing on its Issues and Solutions

Meghna Sharma

Department of Computer Science, JECRC University, Jaipur, India

***Abstract*- Global System Mobile is the most widely used in Cellular Technology in the world. Everytime, Security is the main focus of all aspects. GSM suffers from 'n' number of security issues & factors. Despite from that fact , GSM framework has been designed in such a way so that it provide security features like authentication , data – integrity , prevents cloning & maintain secrecy of the user still when channel is receptive to man-in-middle attacks, replay attacks. Numerous algorithms like A5/1 , A5/2 , A5/3 has been used so far for the security but according to the practical implementation it has been found that these algorithms are less efficient, as desired. In this investigation article the emphasis is given on additional encryption algorithms those are best suitable to secure communication on the GSM Network.**

I. INTRODUCTION

In mid of 1980's GSM was created to develop a new combined mobile phone systems specifications. Hundreds of million users are using mobiles on their daily basis. GSM lacks in providing end-to-end security also in traffic confidentiality to its subscribers. The basic security services that a mobile telephony offer is – Anonymity, Authentication and confidentiality. Confidentiality of the data can be achieved by encrypting the information flow between the two communicating parties. Whereas in GSM networks, encryption is one between base stations and mobile terminals not to the rest of the network that transmit clear text. Hence, Radio link confidentiality is not sufficient to attain end-to-end security. [1]

To enhance the security in GSM the provision to provide security to data and such mechanism is required i.e Cryptography. Cryptography is an art of communication with secret data. It aims to prevent text from anyone who doesn't have the secret "key". Many Cryptographic algorithms are employed on GSM for security like A5/1, A5/2 , A5/3. Still these algorithms are not potentially active to set a security benchmark. Consequently, it is required to increase the security measures by using additional encryption algorithms.

Cryptosystem is a science in which the plain text is made meaningless to all but the deliberate user. The Process of hiding information by converting readable information into a non readable text is called encryption. The process of turning cipher text back to plain text is called decryption. Security of encryption mechanism is based on secret keys.

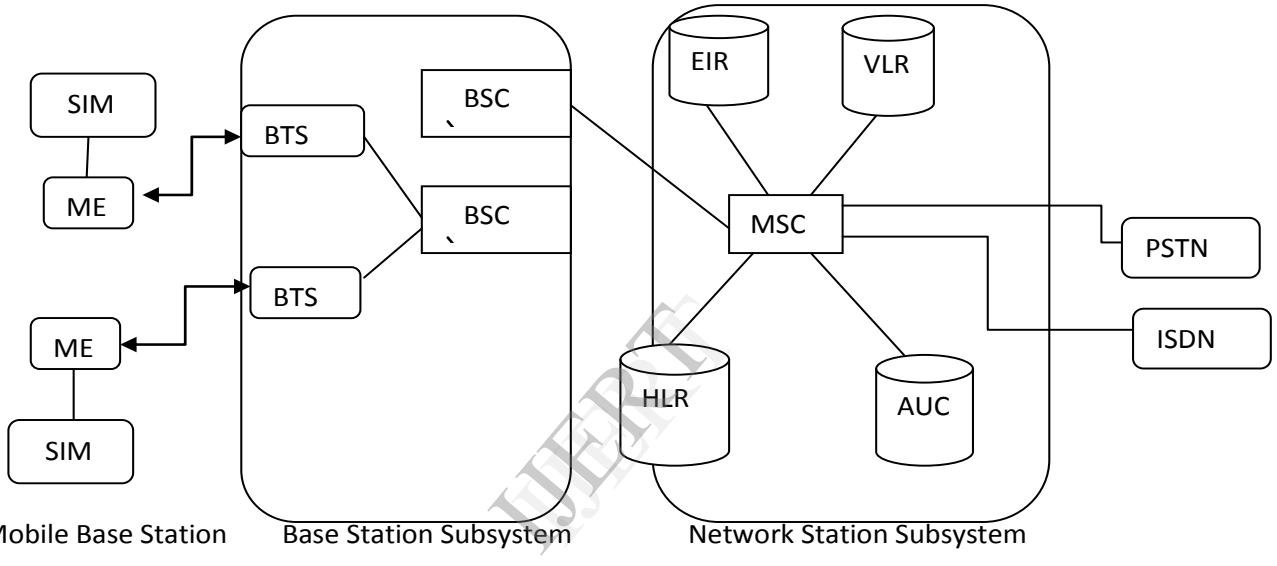
II. GLOBAL SYSTEM MOBILE (GSM)

At the beginning of 2007, the world wide numbers of mobile users reached to 2.83 billion people out of them 80.5% were

using GSM. GSM is now made up of over 745 million subscribers in 184 countries and the GSM family is now comprises EDGE, 3GSM and GPSR. [2]

GSM was proposed to implement strong authentication between the Mobile Station and MSC, as well as implementing strong data encryption for the over air transmission channel between MS and BTS.

The name first comes from a group called Group Special Mobile (GSM), which was formed in 1982 by the European Conference of Post and Telecommunications Administrations (CEPT) [3] GSM network can be divided into three parts :- The Mobile System (MS), The Base Station Subsystem and the Network Subsystem.



SIM: Subscriber Identity Module

ME: Mobile Equipment

BTS: Base Transreciever station

BSC: Base Station Controller

MSC: Mobile Station Controller

EIR: Equipment Identity Register

HLR: Home Location Register

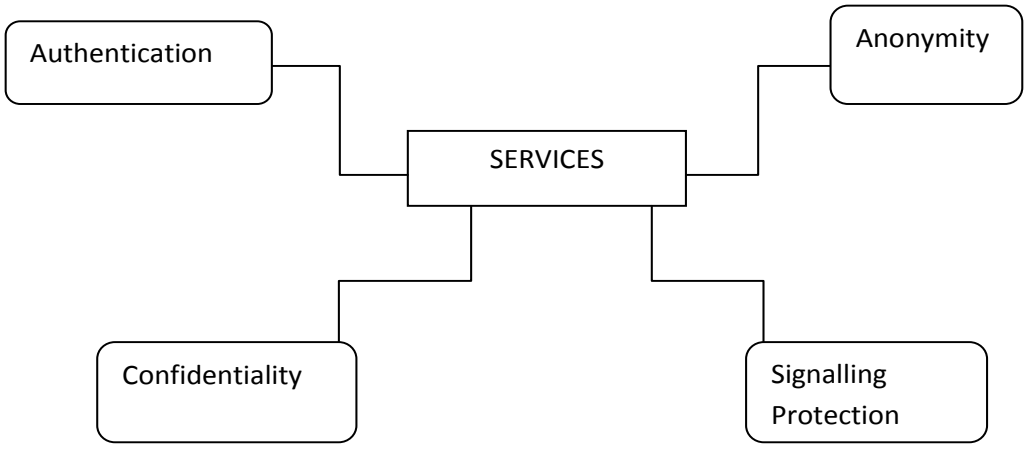
AuC: Authentication

VLR: Visitor Location Register

PSTN: Public Switched Telephone Network

ISDN: Integrated switched Digital Network

2.1) Services Provided By GSM:-



i. *Authentication:* - It is the technique to identify the user to the network operator using challenge and response mechanism. A random challenge is issued to the mobile, using authentication algorithm (A3) and key is assigned to the mobile and sends back the response[4]

ii. *Anonymity*: - This service prevents to fetch the original identity of the user by providing temporary identities. First of all, real identity is used and then temporary identity is issued so that privacy can't be cracked.

iii. *Confidentiality*: - Provides subscriber identity protection, user and signalling data confidentiality, subscriber identity confidentiality.

iv. *Signalling Protection*:- Sensitive information is protected over radio channels.

2.2) Purpose of Security Services:-

The aim of the security services is to make GSM as secure as Public Switched Telephone Networks. Number of potential threats may attack on the radio channel transmissions and channel can be easily intercepted. The GSM MOU Group produces guidance on these areas of operator interaction for members.

III. GSM ENCRYPTION AND ATTACKS

Basically, in GSM A5 algorithm with the versions of A5/1 and A5/2 are used.[5] The major problem is the small length of session key Kc . The genuine length of key is 64 bit but it is assumed that last 10 bits are '0' hence reducing the size of key upto 54 bit. Still this size of key is sufficient enough to handle attacks. Biryukov et al. [6] found a known-key stream attack on A5/1 requiring about two second of the key stream and recovers Kc in a few minutes on a personal computer after a somewhat large pre-processing stage. Barkan et al [7] have proposed a cipher text-only attack on A5/1 that also recovers Kc using only four frames, but with a relative high

complexity. A5/2 was also cracked and proved to be completely insecure. The attack required very few pseudo random hits and only 216 steps.

Then, a new security algorithm is used i.e. A5/3 which provides high level of protections against eavesdropping and based on kasaumi algorithm. These algorithms explicitly provide signalling protection that provides protection to sensitive information over radio path. This encryption algorithm is believed to be stronger than existing ones so far but an attack by Biham et al. Shows that keys can be found faster than complete key search [8].

IV. PROPOSED WORK

As per above reasons it has been understood that GSM doesn't provide sufficient level of security. Hence it is necessary to provide better encryption techniques for the enhancement of security.

In this investigation, emphasis is given on extra encryption proposed using AES, DES, and Triple DES. For implementation of such algorithms certain steps are be followed.

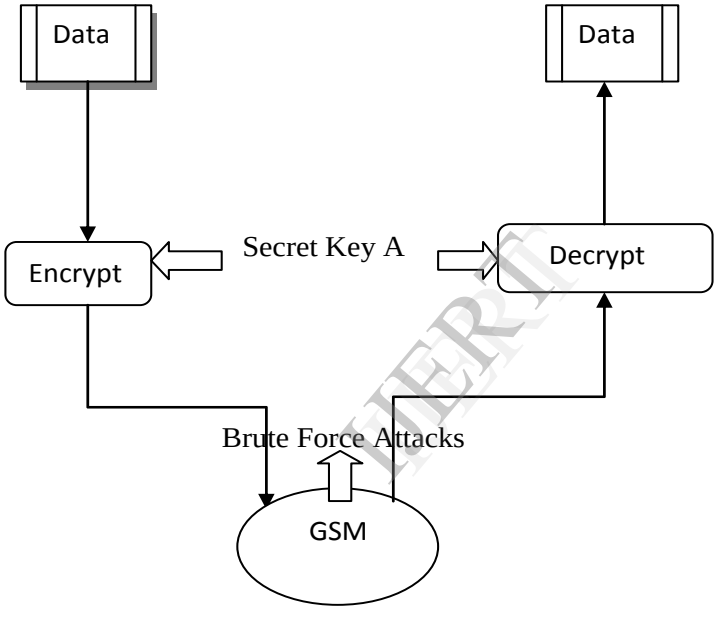


Fig: Data Encryption

4.1 Methodology Used:

Keys of different sizes are used to draw a conclusion on security performances by plotting graphs show the Number of seconds required to breach the corresponding algorithm against brute force attack.

Different Key Lengths are Used [9]:

S.No.	Key Length
1	8
2	16
3	24
4	32
5	40
6	48

Graphical Representation *(Comparison between different key length):-*

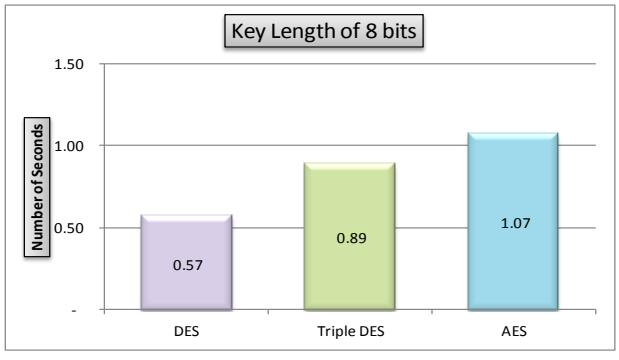


Fig: No of seconds using 8 bit key

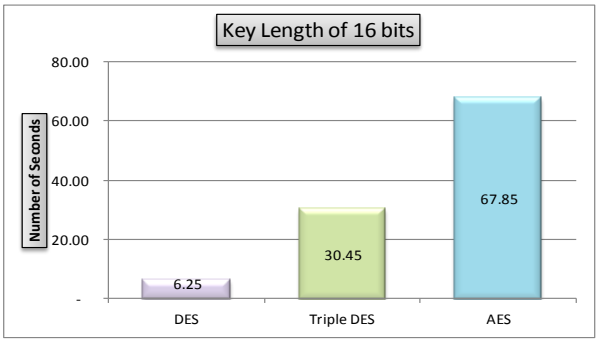


Fig: 16 bit key

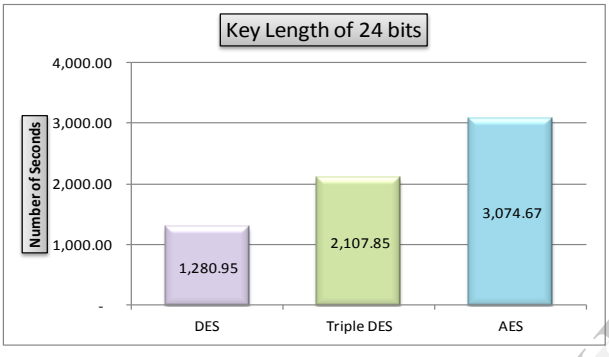


Fig: 24 bit key

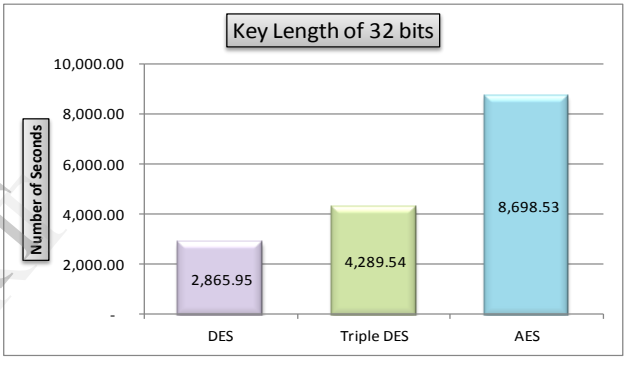


Fig: 32 bit key

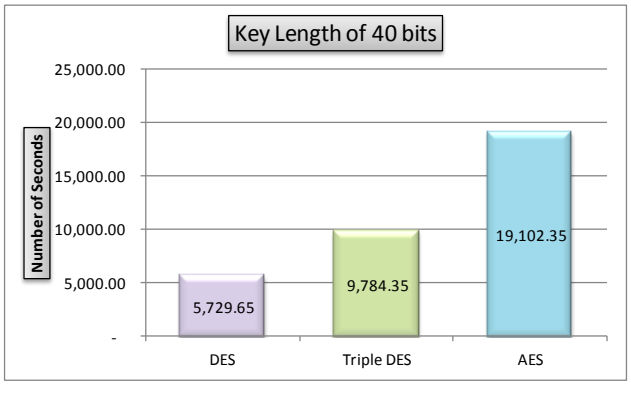


Fig: 40 bit key

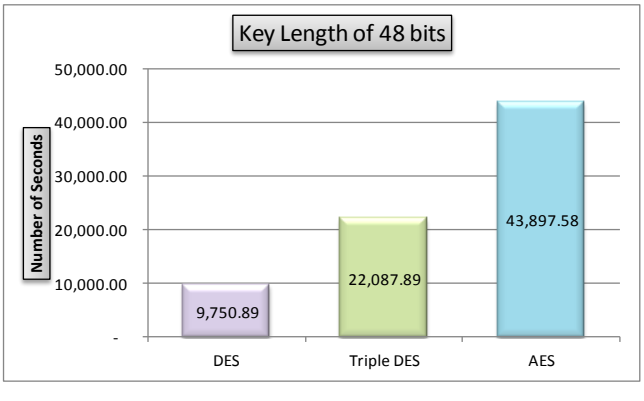


Fig: 48 bit key

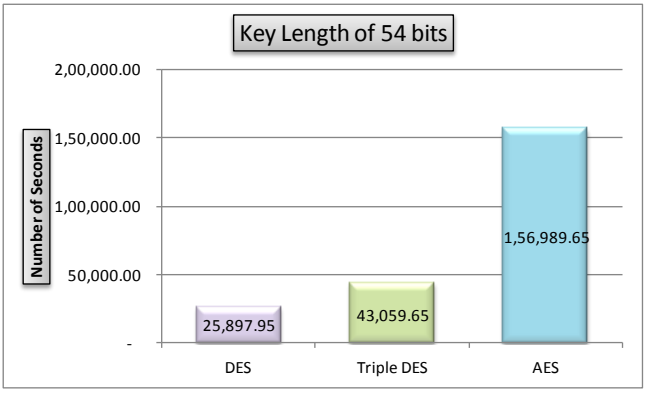


Fig: 54 bit key

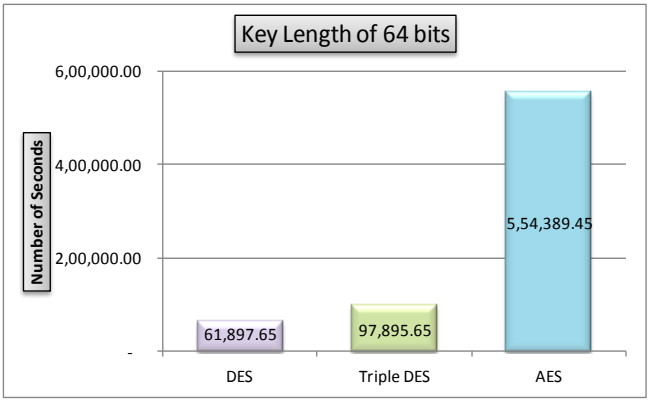


Fig: 64 bit key

These graphs show the time taken to find a key by brute force on DES, triple DES and AES for different key lengths and methodologically it has been analyzed that time taken in case of AES algorithm is more as compared to other and it increases with respect to the increase in key length. Hence AES has better security than DES and triple DES.

V. CONCLUSION

On the basis of above results it has been concluded that AES has a better security measured as compare to other common encryption algorithms .Therefore it can be considered as the better algorithm standard for GSM Network.

VI. REFERENCES

[1] Islam S, Ajmal, Mil Coll of Signal Nation University Science & Technology Pakistan, 2009

[2] P. Chandra "Bulletproof Wireless Security GSM. UMTS & Adhoc Security", Elesecier, 2005

[3] GSM Association

[4] Chi-Chun Lo and Yu-Jen Chen" Secure Communication Mechanisms for GSM Networks" IEEE.

[5] Ross Anderson, Mike Roe "A5- The GSM Encryption Algorithm, 1994"

[6] 3GPP TS 55.216: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEAJ Specifications

[7] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/33 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 4: Design and evaluation report.

[8] 3GPP TS 55.216: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEAJ Specifications

[9] IJCSNS International Journal of Computer Science and Network Security, Vol.10, 2010