ANALYSIS OF DIFFERENT ENCRYPTION STANDARDS ON GSM NETWORK

Author

Shikha Kuchhal
B.E (ECE), PGDCA, MCA, M Tech (ECE), Research Scholar
(A-3/17, NAND NAGRI, DELHI-110093)
Mob. 09811916446,
Email: shikhakuchhal4@gmail.com

ABSTRACT

GSM (**Global System for Mobile Communications**, originally ***Groupe Spécial Mobile***), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It became the de facto global standard for mobile communications with over 80% market share.It is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto, and umbrella cells. The coverage area of each cell varies according to the implementation environment. GSM was designed with a moderate level of service security. The system was designed to authenticate the subscriber using a pre-shared key and challenge-response. Communications between the subscriber and the base station can be encrypted. The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user, whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation. In this paper a new approach to encryption has been proposed which includes extra encryption with AES, DES and Triple DES algorithm. This technique is much simpler than existing techniques thus a more robust and efficient system is achieved.

Keywords: AES, DES, GSM, Key lengths, Security, Triple DES

I. INTRODUCTION

Security plays a very important part in wireless communication systems than in systems that use wired communication. This is mainly because of the ubiquitous nature of the wireless medium that makes it more susceptible to security attacks than wired communications. In the wireless medium, any eavesdropper can get over to whatever is being sent over the network. Also, the presence of communication does not uniquely identify the originator. To make things worse, any tapping or eavesdropping cannot even be detected in a medium as ubiquitous as the wireless medium. Thus security plays a vital role for the successful operation of a mobile communication system.

GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band. Main objective in mobile communication systems is security of data exchanged.

GSM uses several cryptographic algorithms for security like A5/1, A5/2 and A5/3. But it has been found that these algorithms are cracked by various practical attacks so these algorithms do not provide sufficient levels of security for protecting the confidentiality of GSM therefore it is desirable to secure data by additional encryption. In this paper I have done additional encryption by implementing DES, Triple DES, and AES algorithms on GSM Network.

This paper outlines the provision of encrypted information over GSM. For security of data in GSM networks such encryption and mechanisms to provide it are required. This paper also analyzes the effectiveness of these algorithms against brute force attack implemented in MATLAB environment. GSM, together with other technologies, is part of the evolution of wireless mobile telecommunications that includes High-Speed Circuit-Switched Data (HSCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). GSM uses stream ciphers for encryption which requires the data to be in binary form. This technique does encryption directly on symbols without going on to the bit level. Also, this technique does not require any hardware; it is totally based on software. Following sections discuss the proposed scheme:

- Section 2 describes the security requirements of Mobile Networks.

- Section 3 gives an overview of existing GSM encryption algorithms and various attacks on these.
- Section 4 walks through the used setup and settings for extra encryption on GSM. This section illustrates the performance evaluation methodology and the chosen settings to allow a better comparison.
- Section 5 gives a thorough discussion about the results, and Finally,
- Section 6 concludes this paper by summaries the key points and other considerations.

II. SECURITY REQUIREMENTS OF MOBILE NETWORKS

Security has become an important issue in current mobile and wireless networks. As the security measures for such networks increase, the tools and techniques used to attack such networks also increases. Wireless communications security in simple terms, is the procedures or methods used for protecting the communication between certain entities. Protection mechanisms are used to protect the entity from any third party attacks, such as impersonating an identity,

revealing a specific identity, data-hijacking or data modification, eavesdropping and so forth. Dedicated technologies for securing data and communication are required in wireless networks, which vary according to the type of wireless technology deployed. Security in mobile and wireless networks covers various issues, from authentication of a user accessing a certain network, to data encryption and data integrity. GSM, like many other large systems with large numbers of users, contains many valuable assets that need protection against misuse and deliberate attacks.

This section highlights the valuable assets that, in general, exist in a GSM Network, and that are crucial to protect for the best of the system's shareholders (subscribers and service providers).

A secure communication network provides the following facilities to its users [2]:

Confidentiality: The non-occurrence of the unauthorized disclosure of information. No one except the sender and the receiver should have access to the information being exchanged.

Integrity: The non-occurrence of the unauthorized manipulation of information. No one except the sender and the receiver should be able to modify the information being exchanged.

Authentication: The receiver's ability to ascertain the origin of a message. An intruder should not be able to masquerade as someone else.

Nonrepudiation: The receiver's ability to prove that the sender did in fact send a given message. The sender should not be able to falsely deny later that he sent a message.

Service Reliability: The ability to protect the communication session against denial of service attacks.

III. GSM ENCRYPTION AND ATTACKS

In GSM, A5 stream cipher is used [3]. Versions A5/1 and A5/2 were kept secret for a long period of time. A5/1 and A5/2 were reverse-engineered from a GSM handset and published by Briceno et al. [4]. After which attacks were quickly found for these algorithms.

The primary problem is the small key length of the session key Kc. The actual length of Kc is 64 bits. However, the last 10 bits of this key are specified to be 0 thus reducing the effective key size to 54 bits. Even though this key size is big enough to protect against real-time attacks (decrypting packets being transmitted in real-time), the state of the hardware available today makes it possible to record the packets between the MS and the BTS and then decode them at a later time. [7]. 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 preprocessing stage. Barkan et al. [3] 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 [3].

A new security algorithm, known as A5/3 provides users of GSM mobile phones with an even higher level of protection against eavesdropping than they have already [4,5]. A5/3 is based on the Kasumi algorithm, specified by 3GPP for use in 3G mobile systems. The A5/3 encryption algorithm specifically supplies signaling protection, so that sensitive information such as telephone numbers is protected over the radio path, and user data protection, to protect voice calls and other user generated data passing over the radio path [4, 5, 6]. The algorithm is so far believed to be stronger than A5/1 and A5/2 but an attack by Biham et al. shows that the key can be found faster than exhaustive key search [4].

ISSN 2229-5518

IV. REQUIREMENT OF EXTRA ENCRYPTION ON GSM

As discussed above GSM Encryption does not provide sufficient level of security to protect data. So there is need to improve GSM encryption algorithms for better security. In this paper extra encryption on GSM network is proposed using AES, DES and Triple DES encryption algorithms. For implementing and evaluating above encryption algorithms we have done the following steps:

1. Encrypt data with one of above mentioned algorithms.
2. Encode the encrypted data according to GSM.
3. Brute Force Attack has been done.
4. Time Taken to find a correct key is measured against different key lengths

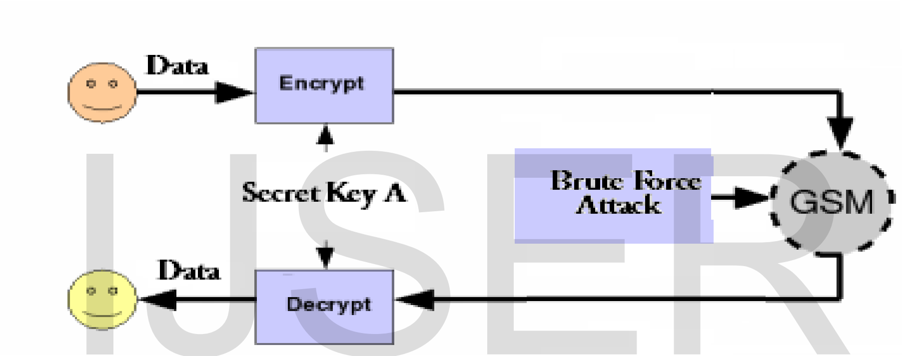

Fig. 1 Data Encryption

This paper analyzes the effectiveness of AES, DES and Triple DES encryption algorithms against brute force attack
on GSM networks. The comparison has been conducted by running brute force program against these algorithms.

4.1. IMPLEMENTATION SETUP

This section describes the implementation environment and the used system components. The implementation of DES,
TripleDES and AES uses classes available in JAVA package javax.crypto. Separate functions for encryption and decryption have been implemented in MATLAB using JAVA cryptography API.

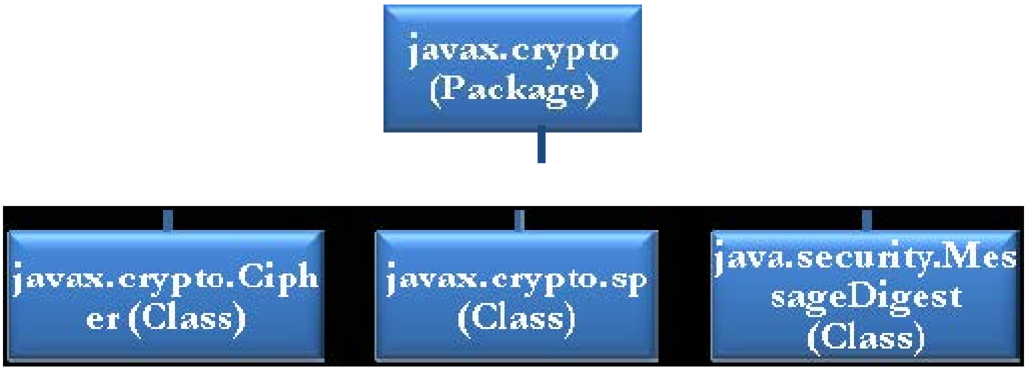

Fig. 2 Java Cryptography package

Brute force program is implemented in MATLAB environment. This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm.

4.2. METHODOLOGY USED

This section will discuss the methodology and its related parameters like: system parameters, experiment factor(s), and experiment initial settings.

4.2.1. SYSTEM PARAMETERS

The experiments are conducted using Intel 64bit processor with 512GB of RAM. The program is written in the MATLAB. The experiments will be performed couple of times to assure that the results are consistent and are valid to compare the different algorithms. This brute force attack has been done using Single PC. It can be enhanced by use of parallel computers with high computational powers to decrease the time required to find the key for above algorithms.

4.2.2. EXPERIMENT FACTORS

In order to evaluate the effectiveness of the compared algorithms against brute force program on GSM networks, the experimental factors must be determined. The chosen factors here to determine the effectiveness of encryption algorithms are the keylength and time taken to breach an algorithm by the brute force program.

4.2.3. EXPERIMENTAL INITIAL SETTING

We started the attack with 8 bit of key length and extended upto 48 bit. It can be further increased upto supported key length of AES algorithm i.e 256 bits. But for this high computational power is required in terms of parallel computers to breach the algorithms.

V. RESULTS AND DISCUSSIONS

This section will show the results obtained from running the brute force program on AES, DES and Triple DES. The results of the implementation have been shown below in the form of graphs.

The time of launch of brute force attack is shown at the start of the program as in Fig. 3.

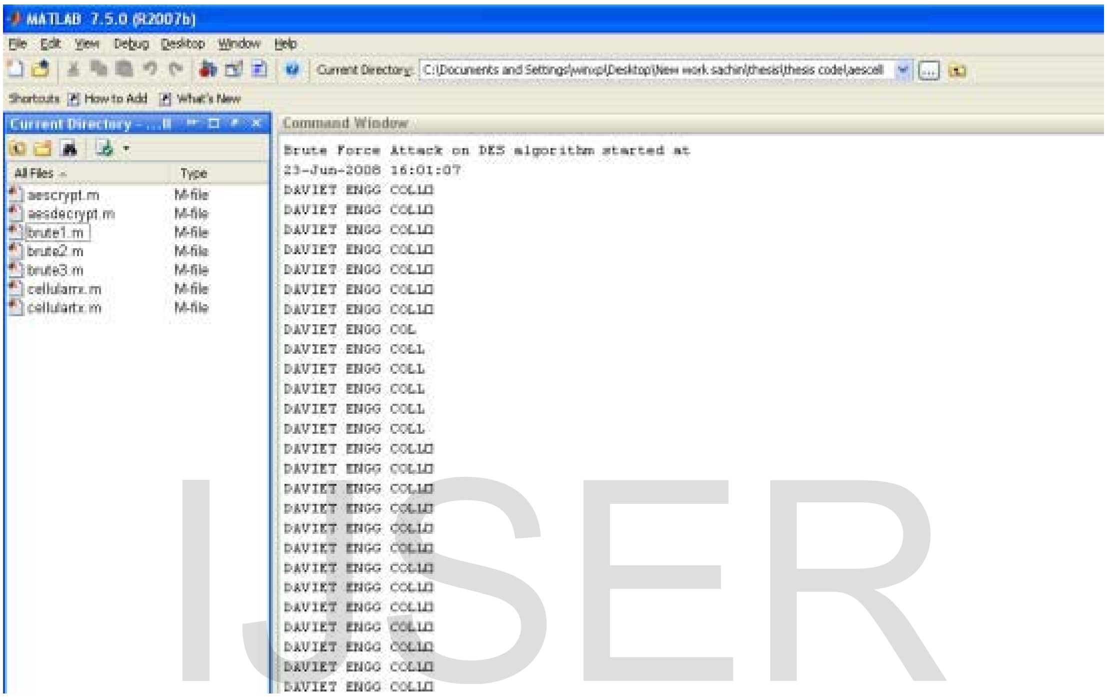

Fig. 3 Screenshot of running Brute Force Program

Fig. 3 Screenshot of running Brute Force Program The program exits on success of the attack on the encryption algorithm and tome of exit is shown below in Fig. 4

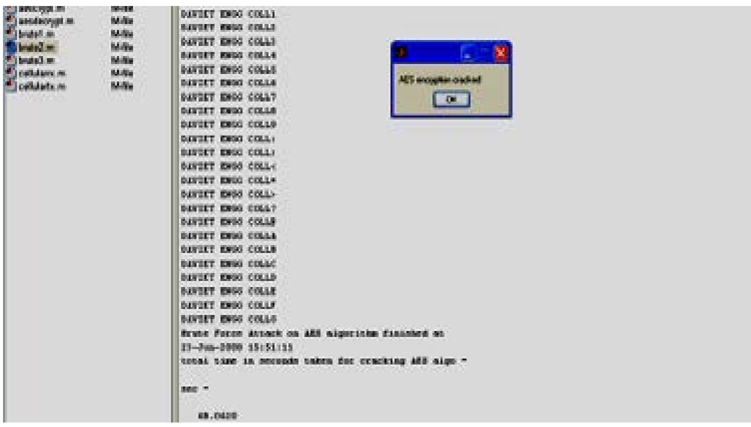

Fig. 4 Screenshot of cracked Algorithm

ISSN 2229-5518

It is highlighted here that the implementation has been performed assuming that the user has arrived at all the correct values of the key and only one value of the key is to be cracked. This has been done to save the time required.

The key length can be optimized to reduce the time taken for encryption and decryption process so that it does not slow down the system.

A. EFFECT OF KEY LENGTH VARIATION

We compare the change in Security performance by using different key lengths for encryption algorithms. Graphs are plotted between the times required to find the correct key and different keylengths. We have taken six different scenarios by increasing the length of the key.

TABLE 1:
DIFFERENT KEY LENGTH

1	8 bit
2	16 bit
3	24 bit
4	32 bit
5	40 bit
6	48 bit

Following are the Graphs for scenarios as stated in Table 1. These graphs show the Number of seconds required to breach the corresponding algorithm against brute force attack.

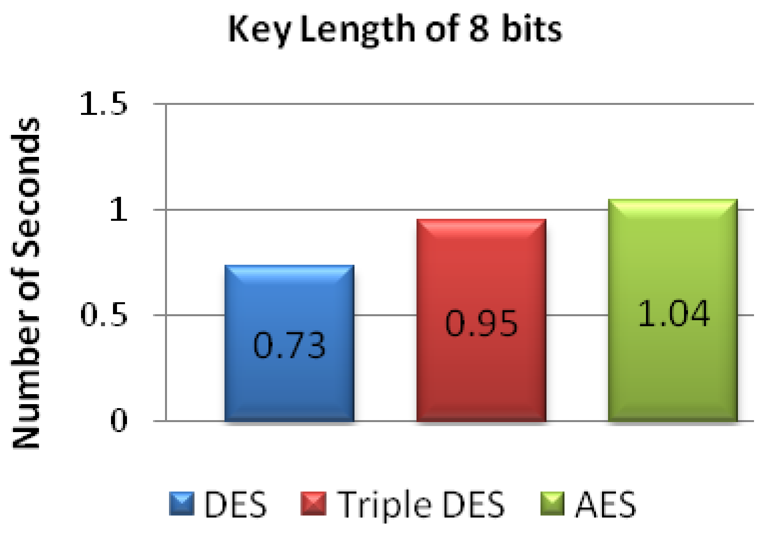

Fig. 5 Number of seconds required with key length of 8 bits

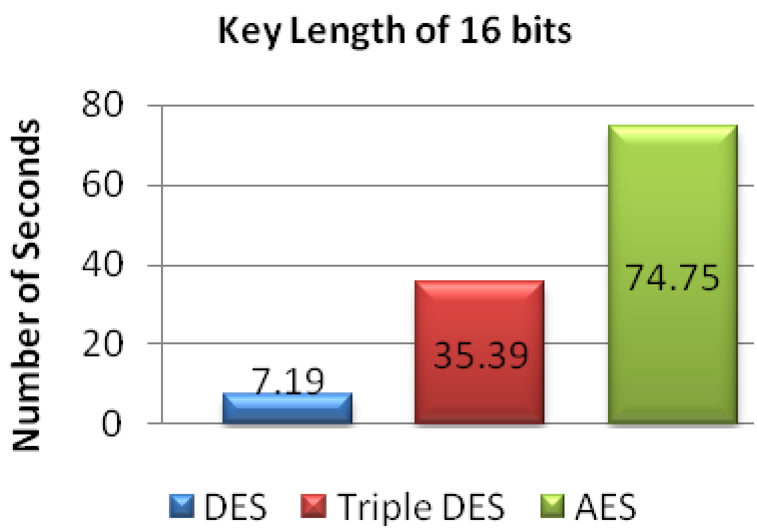

Fig. 6 Number of seconds required with key length of 16 bits.

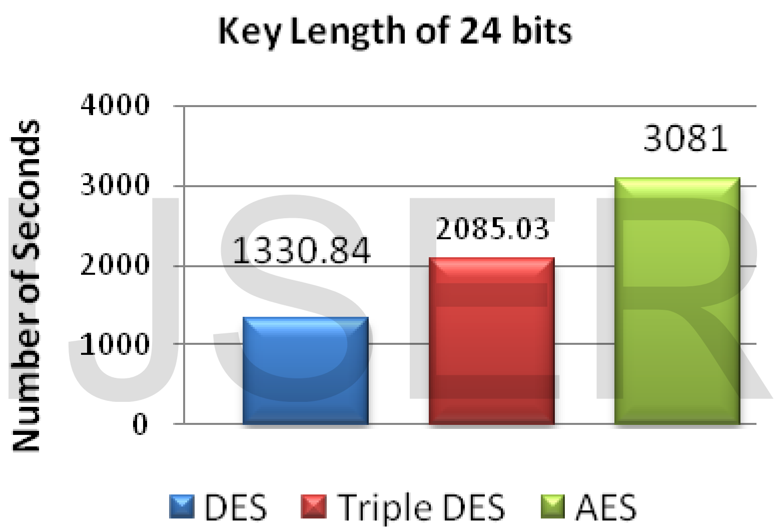

Fig. 7 Number of seconds required with key length of 24 bits.

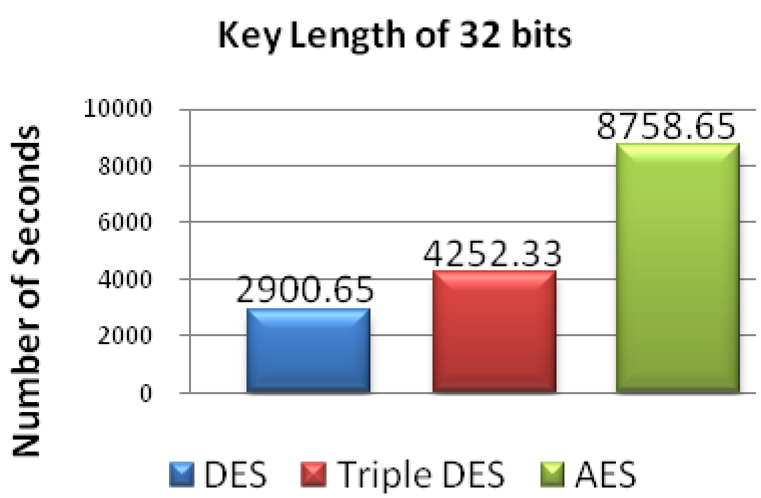

Fig. 8 Number of seconds required with key length of 32 bits.

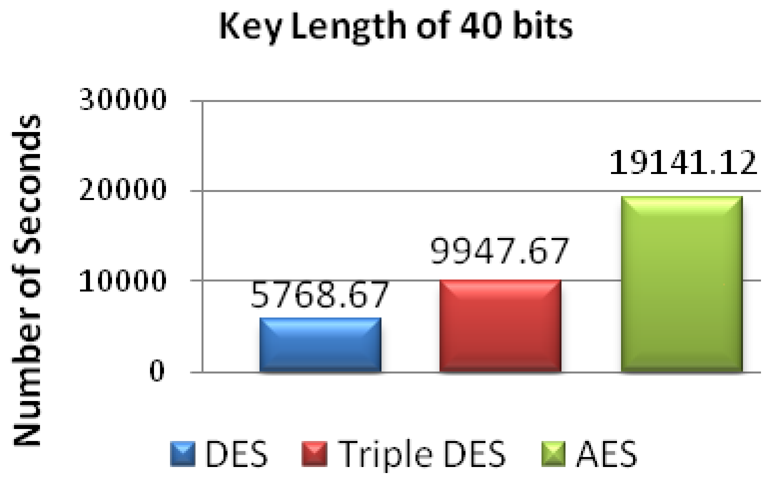

Fig. 9 Number of seconds required with key length of 40 bits.

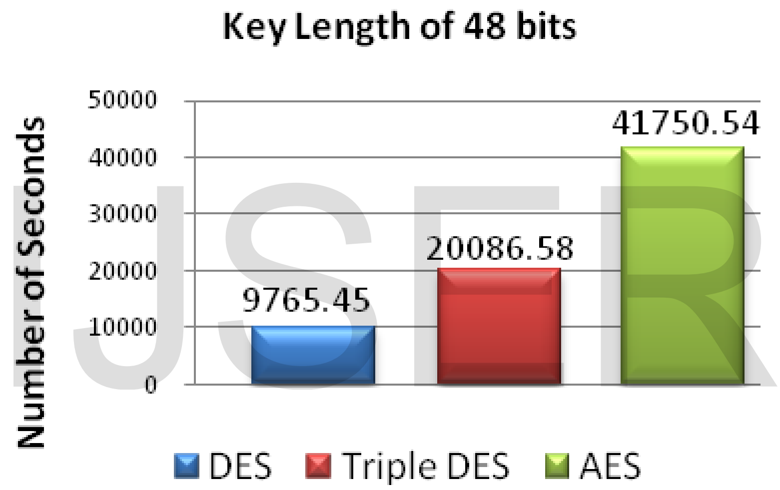

Fig. 10 Number of seconds required with key length of 48 bits.

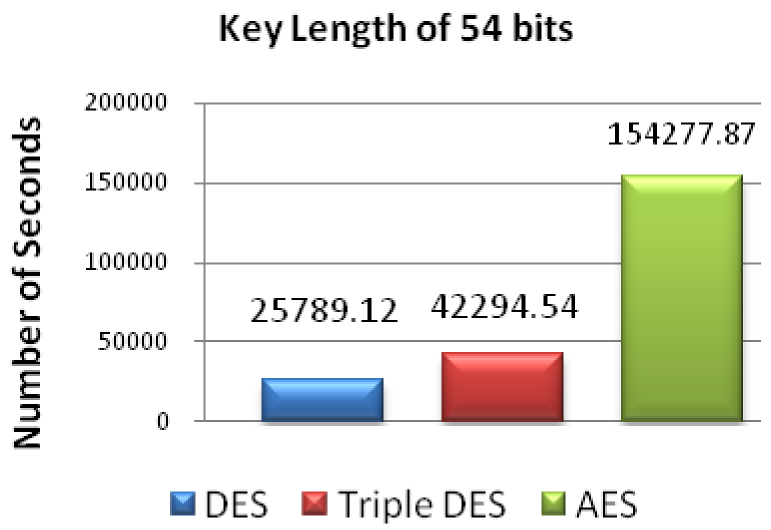

Fig. 11 Number of seconds required with key length of 54 bits.

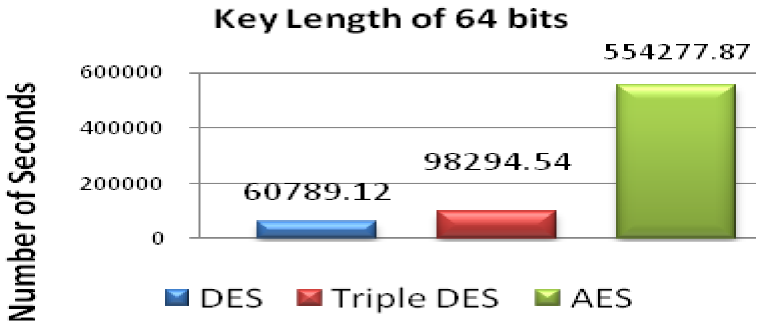

Fig. 12 Number of seconds required with key length of 64 bits.

The above graphs show the time taken to find a key by the brute force program on DES, triple DES and AES for different key lengths. From these graphs it is analyzed that time taken by brute force attack increases exponentially with increase in the key length. It is clear from the graphs that in case of AES algorithm brute force attack takes much more time to find a key therefore AES has better security than DES and Triple DES.

B. EFFECTIVENESS OF ALGORITHMS AGAINST BRUTE FORCE ATTACK

The results of the iterations of brute force program have been shown in fig. 13 and in Table 2. This Graph is plotted in the MATLAB environment. The above data and graph represents the effectiveness of AES DES and Triple DES algorithms against Brute Force attack. It is evident from the data presented that AES proves to be a better security against the brute force program than DES and Triple DES for securing GSM communications.

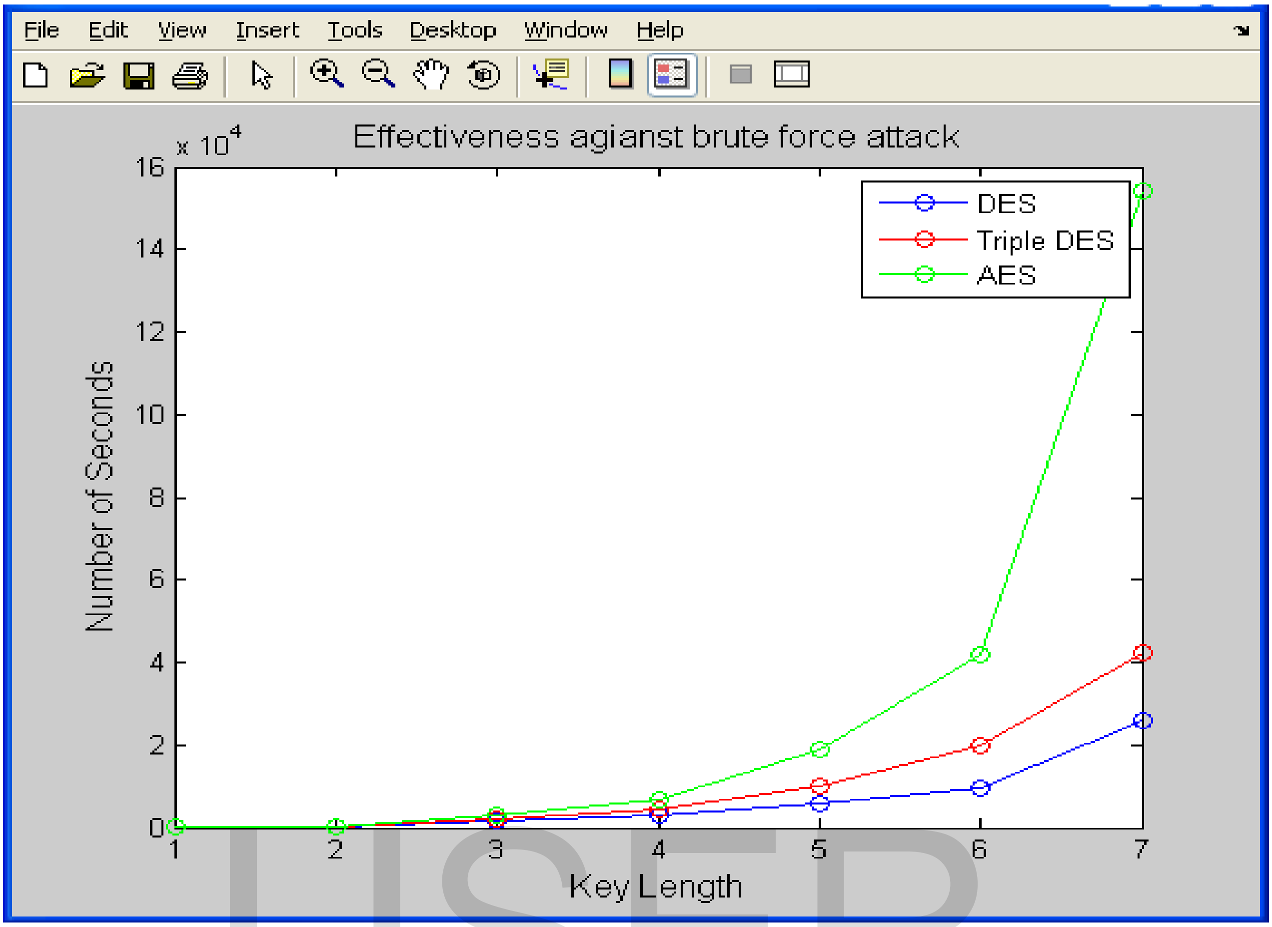

Fig. 13 Effectiveness of AES, DES and Triple DES against brute force attack

TABLE 2:

NUMBER OF SECONDS REQUIRED TO BREACH AES, DES AND TRIPLE DES ALGORITHMS.

Key Length (bits)	**DES (Seconds)**	**Triple DES Seconds)**	**AES (Seconds)**
8	0.73	0.95	1.04
16	7.19	35.39	74.75
24	1330.84	2085.03	3081
32	2900.65	4252.33	8758.65
40	5768.67	9947.67	19141.12
48	9765.45	20086.58	41750.54
56	25789.12	42294.54	154277.87
64	60789.12	98294.54	554277.87

VI. CONCLUSIONS

The presented results showed that AES has a better security against the brute force attack than other common encryption algorithms used; therefore it is an excellent candidate to be considered as a standard encryption algorithm for GSM Network.

SUMMARY OF THE KEY POINTS:

- AES proves to be better security than DES and Triple DES as it takes considerably much more time to break by the brute force program for a given key length
- Time Taken to break AES algorithm by a brute force program increases exponentially with increase in the keylengths.

REFERENCES:

(1) David G. W. Birch and Ian J. Shaw, “Mobile communications securityprivate or public”, IEE, June 1994.

(2) Ross Anderson, Mike Roe "A5 - The GSMEncryption Algorithm", 1994.

(3) "Wireless Security Handbook,” Auerbach Publications 2005.

(4) 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.

(5) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspect0s; 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.

(6) 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

(7) Michael Stausholm,, and Morten Dahl, Insecurity of GSM Communication December 15, 2006.

(8) Dr. S. Muhammad Siddique and Muhammad Amir “GSM Security Issues and Challenges” Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, an Parallel/Distributed Computing (SNPD’06) 2006

(9) W. Diffie, M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. 22, No. 6, pp.644-654, Nov. 1976.

(10) The Advanced Encryption Standard Network Security, Volume 2001, Issue 10, 31 October 2001, Pages 11-13 Marie A. Wright

(11) The Advanced Encryption Standard — Implementation and Transition to a New Cryptographic Benchmark Network Security, Volume 2002, Issue 7, 1 July 2002, Pages 7-9 Juan C. Asenjo

(12) Reducing the exhaustive key search of the Data Encryption Standard (DES)Computer Standards & Interfaces, Volume 29, Issue 5, July 2007, Pages 528-530 Raphael C.-W. Phan

(13) Hudson, R.L., "Snooping versus Secrecy," Wall StreetJournal, February 11, 1994, p. R14 Schneier, B., "Applied Cryptography," J. Wiley

(14) M. Wiener, “Brute force attacks on cryptographic keys”, October, 2001. [Online] Available at http://www.cl.cam.ac.uk/~rnc1/brute.html.

(15) Yang, H., et. al., "Securing A Wireless World," Proceedings Of The IEEE v. 94 no. 2 Feb. 2006, http://www.cs.ucla.edu/~hyang/paper/ProcIEEE05.ps

(16) Schneier, B., "Applied Cryptography," J. Wiley & Sons, 1994. [17] Van der Arend, P. J. C., "Security Aspects and the Implementation in the GSM System," Proceedings of the Digital Cellular Radio Conference, Hagen, Westphalia, Germany, October, 1988