INVESTIGATIONS IN BRUTE FORCE ATTACK ON GSM BASED ON DES AND AES

Almas Zahra[1] Professor Danish Raza Rizvi[2]
[1]M.Tech Scholar [2] Assistant Professor
[2] Computer Science & Engineering Department
[2] JMI, New Delhi

Abstract— With the increase in the demand of wireless and mobile devices day-by-day, a need for maintaining more secure connection comes up. The more secure a connection is , the better and satisfactory will be its performance. Security is an extremely challenging issue in mobile and wireless systems these days. A number of issues come up in terms of network security and this directly affects throughput and QoS of cellular systems. Among different types of security issues, the most common ones are ensuring the anonymity of parties involved, authenticating the parties to each other and confidentiality of the message. Even wired networks used to have various security issues but the wireless and mobile systems are prone to all these vulnerabilities plus many more risks inherent to wireless and mobile systems. GSM, a cellular system for mobile communication uses some version of A5 algorithm for ensuring security but we observed that DES is secure than A5 algorithm. Further, AES is even found to be far more secure than DES also as it takes more time to attack AES based security system as compared to either A5 or DES based systems.

Key words: Security issues, Brute force attack, DES, AES.

I. INTRODUCTION

Let's begins by introducing the basics of cryptography. We have a plaintext which we secure by a second input called key to get the locked cipher text. The algorithms used can be symmetric algorithms (that uses secret keys) or asymmetric (that uses a public and a private key) . Either block or stream ciphers exits. While block ciphers operates on a fixed block of plaintext to produce the same sized block as cipher text, the stream ciphers operates on individual digits, one at a time. We here will be studying two symmetric block ciphers namely DES and AES.

Talking about the GSM network security, A5 algorithm is being used currently. Once the subscriber authenticates itself to the system, now it's the time for communication between the system and subscriber which needs to be protected against fraudulent access using A5. It is a stream cipher. It has a key length of 64 bits but ideally only 54 bits are put to use as the last 10 bits are all set to zeroes. Thus the address space ie reduced from 2^{64} to 2^{54}.[2]

II. SECURITY ISSUES

Wireless systems are usually mobile and make use of on air interface. So, anyone can capture the radio signals with the suitable equipment over air. Also mobile devices have numerous limitations like limited storage, relatively smaller memory and weak encryption.
One major limitation is of limited bandwidth in case of wireless and mobile devices as in these the bandwidth is being shared between many devices and users and this sharing is a result of channel contention. This also offers a serious challenge in terms of QoS of wireless systems.
When it comes to cellular system, the underlying infrastructure is huge, massive and quite complex as it comprises of a number of entities working together in a coordinating manner. Due to mobile nature of the devices it again becomes a challenge to provide security on each and every communication path.

Due to open wireless access medium , there is a lack of physical barrier that can protect against an attacker.

Another issue associated with the wireless networks is of limited power. They consume lot of power to operate and so suffer a limited time battery life. The processors installed are day by day increasing in power consumption but still they are not capable of carrying out high processing.[3]

All the above issues and some more create a relatively unreliable connection with high rate of errors across the medium.

Keeping in mind the above limitations we now head towards identifying the various security issues in cellular systems. Some of them are as follows:

A. Authentication*:*

It is an assurance that the entity is who he/she claims to be. Authentication of the involved parties towards each other is an important concern so as to ensure that the right people are using the communication network. Cellular systems have large number of subscribers , with different service providers that too scattered across the world so , there is a need of cross region and cross provider authentication and this itself is a extremely big issue.[4]

B. Confidentiality:

It is an act of assurance of data privacy. It creates a confidence among the parties involved that no one else can read/get their message except of the specific intended entity(s).[4]

C. Access control:

Some sort of role based database needs to be maintained to allow restricted access to certain files

D. Location detection:

Hiding the current location of the mobile device due to privacy is needed. With the introduction of IP based networks , this has become a mojor issue as often the actual lopcation is not clear.[4]

Other issues could be message **integrity** so as to send message intact, use of **OS(s) for mobile devices**,

downloaded contents from web and the **viruses and malware** coming along with these downloaded contents.

III. DES

Data Encryption Standard initially known as the Data Encryption Algorithm was adopted in 1977 by National Institute of Standards and Technology (NIST) as an information processing 'federal' standard.

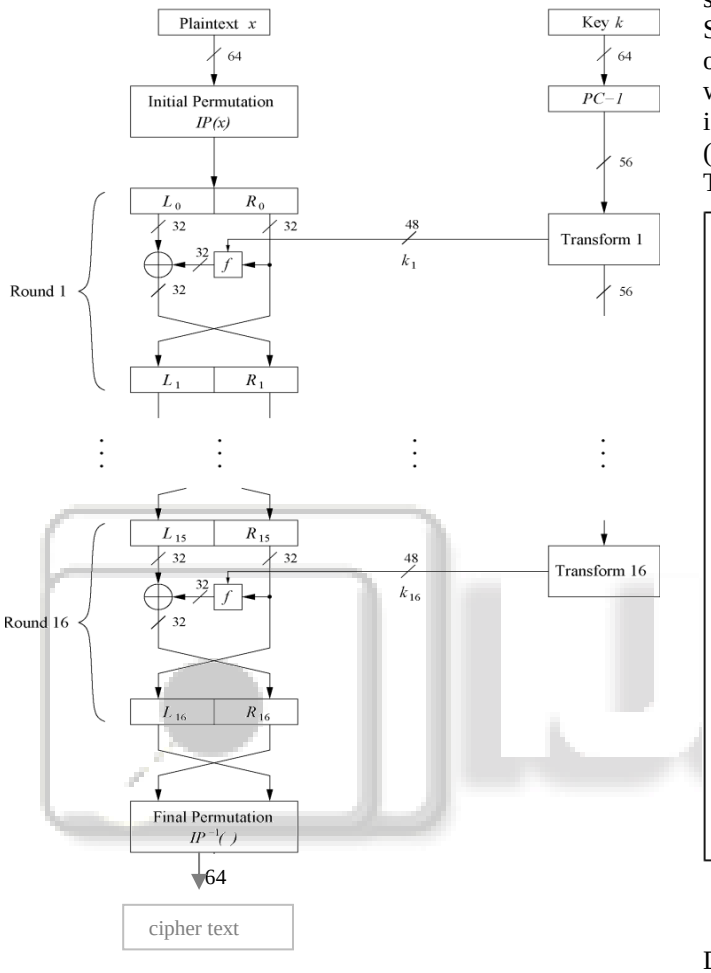

Fig. 1: DES

It is a 64 bit block cipher i.e. it encrypts a 64 bit block at a time. It is a symmetric cipher as well. The cipher text is also of 64 bits. The key has 64 bits too but the effective key length is of 56 bits as the last 8 bits are reserved for parity checks.

Its structure is as follows:

First of all an initial permutation (IP) is done on a 64 bit input which rearranges its bits to produce a permuted input. The original key is passed through PC-1 (permuted choice 1) where it is permuted/contracted then transformed using a left circular shift followed by another permutation(called PC-2) to produce 48 bit sub key (Ki) for each round. Now there are 16 rounds of similar structure that works on two halves of the input using a similar function 'f' with left and right halves swapped.

The detail structure of function 'f' is comprised of 4 steps:

1. Expansion(E)
2. XOR with the round key
3. S-box substitution
4. Permutation

Expansion(E) takes a 32-bit input from R_{i-1} to produce a 48-bit output by splitting it into eight 4-bit blocks and copying the extreme bits of each block to output in a particular manner.

The XOR of the E-box output is then done with the 48-bit subkey(K_i).

S-boxes are eight in number with 6-bit input and 4-bit output each. Each S-box can be considered a 4x16 matrix with each cell treated as (i,j) where $0 \le i \le 3$ and $0 \le j \le 15$. Here, i=Dec(b1,b6) and j=Dec(b2,b3,b4,b5) for a block B (b1,b2,b3,b4,b5,b6).

The P-box is a simple permutation of the input.

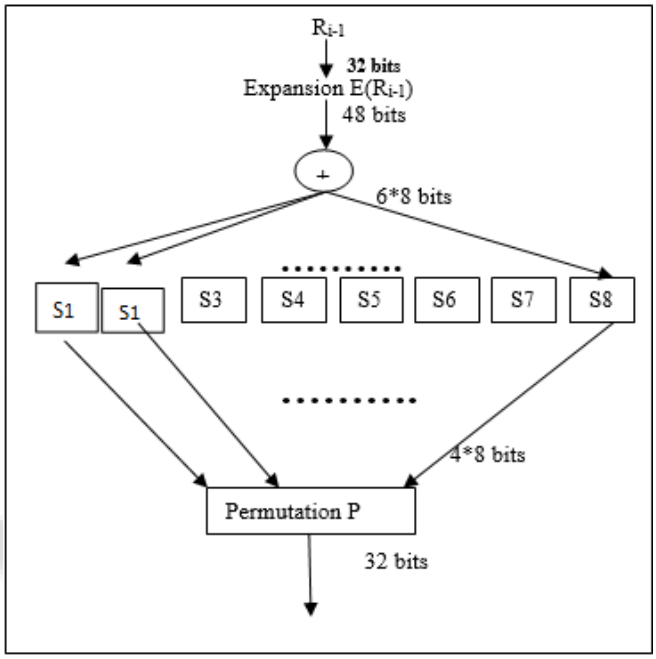

Fig. 2: DES 'f' function

DES decryption is almost the same procedure as the encryption with ciphertext and key being input to the algorithm. But the keys are used here in reverse order i.e. K_{16} for first cycle, K_{15} for second cycle and so on till last cycle.[7]

Criticisms of DES:

- DES is slow.
- It has a small key size of 56 bits only thus offering a small key space to an attacker as for any plaintext-ciphertext pair(x,y) , we were to test for 2^{56} keys till we reach the situation { $DES_k^{-1}(x)=y$ } and such an exhaustive search is quite easy.
- The design of the 8 S-boxes were kept secret so it was considered that there are security flaws in it and if it is revealed to an attacker, he can easily break the algorithm.

IV. AES

In order to overcome the criticism of the DES , in 2001 the Rijndael algorithm came up with the name of Advanced Encryption Standard. DES had a small block size. So to make the new algorithm more secure, the block size needs to be increased.

AES has a block size of 128 bits. The key size is varying here. It can have a key of 128,192 or 256 bits. The number of cycles can be either 10,12 or 14.The key size is dependent upon the number of rounds chosen i.e. for 10 rounds key is of 128 bits, for 12 rounds key has 192 bits and for 14 rounds the key has 256 bits.

The structure of the algorithm is as follows:

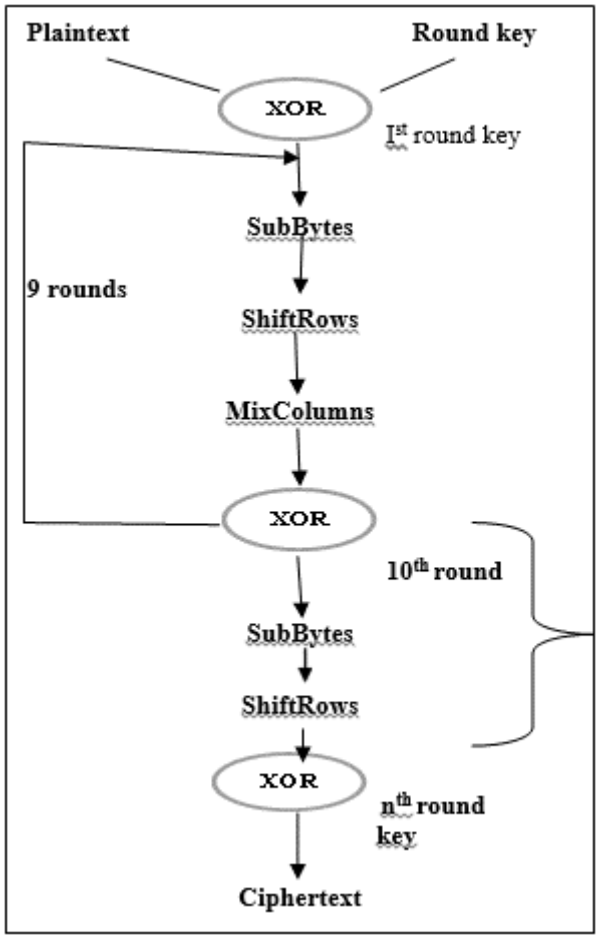

Fig. 3: AES flowgraph

Here, the 128 bit plaintext is divided into 16 bytes and then arranged into a 4x4 matrix .In every round these bytes of the plaintext has to go through 4 different stages namely Substitute byte , Shift Row , Mix column and Add Round Key. Their implementations are as follows: [1]

Substitution byte(SubsByte): Here each byte entry of the matrix is replaced by another byte of a 16x16 matrix by dividing the byte into two nibbles of four bits each,The most significant bit of this nibble is a the row index and the last significant bit of this nibble is the column index to the existing 16x16 matrix. Thus an entry can be fetched from it and replaced .

Shift row: It is a simple permutation. In this the rows of the 4x4 matrix are left circularly shifted by certain places.Example :the first row is not shifted at all , the second row is shifted by one place,the third row is shifted by two places and the fourth row is shifted by three places as follows:

!	@	#	$
%	^	&	*
(	)	_	+
~	=	<	>

⇩

!	@	#	$
^	&	*	%
_	+	(	)
>	~	=	<

Mix column: It makes use of the arithmetic cover. Here the matrix is left multiplied by another matrix whose cells represents bytes.

$$\begin{pmatrix} 3 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} ! & @ & \# & \$ \\ \% & \wedge & \& & * \\ (&) & \_ & + \\ \sim & = & < & > \end{pmatrix}$$

Add round key: in this a XOR operation of the plaintext block or the current block with the key or the expanded key is done respectively.

Positives of AES:

- It is more secure due to larger block size of 128 bits and longer key space of 2^{128},2^{196} or 2^{256} offers far more resistance to an attacker .
- It has high hardware , software performance as it is faster. It works even more speedily on small devices like smart phones, smart cards etc.
- It is flexible enough due to varying number of rounds and key sizes**.**

In decryption the various encryption steps are reversed as Inverse byte substitution, Inverse mixcolumn , Inverse shift rows.[6]

V. BRUTE FORCE ATTACK

It is a trial-n-error based method of attacking any cryptographic system with the intent of capturing useless information like password, PIN (Personal Identification Number). It tries every possible key to break a cipher. It not tries to decrypt the cipher as such rather generate all possible key combination till a match is found. Practically , as such all cipher can be cracked using this. Any cipher that can be cracked only through brute force attack is considered fairly secure. A simple form of brute force attack may hold a dictionary of all possible words or very common passwords

and iterate through it to get a match (dictionary attack) while a more complex attack is when various key combinations are generated(exhaustive search).[8]

The brute force attack as such is quite time consuming and so it can be protected only by taking larger sized keys. More the key size, larger will be the time taken to crack it and vice versa. Larger key size may take even not just hours and days but months and years to execute and crack the system. We can observe from the data given below that larger the key size, more will be the time required.[5]

Following facts are there to indicate the time and the number of machines needed for brute force attack on various key sizes.

Table.1: Brute force attack figures

Key size in bits	**Time required**	**No. of machines required to search in 1 day**	**No. of machines required to search in 1 week**
40	~1.2 hrs	13	2
56	~2300 yrs	~8,37,000	~120
64	~5.9 yrs	~$2.14*10^{8}$	~$3.0*10^{6}$
128	~$11*10^{24}$yrs	~$4*10^{27}$	~$5.6*10^{26}$

Brute force attack on DES has a key space of 2^{56} while AES offers a much larger key space of 2^{128}.

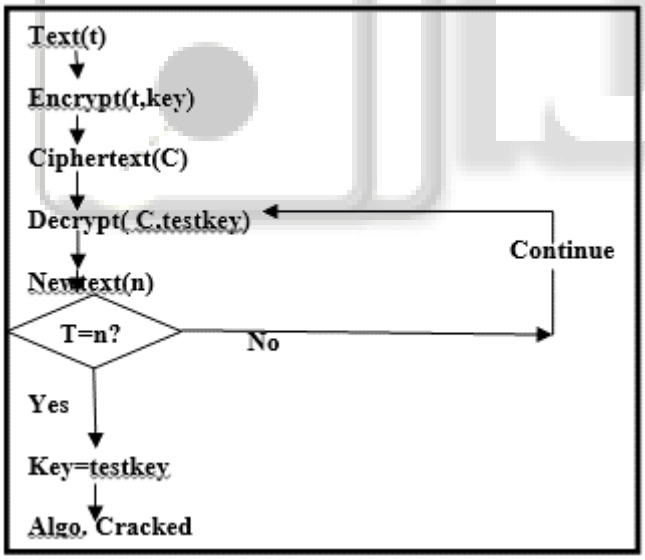

Fig. 4: Brute force attack

VI. DES VS AES

A comparison between the two algorithms is summarized based on certain factors:

Table. 2 :DES vs AES

Factors	**DES**	**AES**
Block size	64 bits	128 bits
Key size	56 bits	128,192,256 bits
Key space	2^{56}	2^{128} or more
Cycles	16	10,12,14
Security	Low	High
Cryptanalysis resistance	More prone to linear and differential cryptographic attacks; weak S-boxes	Strong against linear and differential attacks
Speed	Slow	Fast
Complexity	Less	High
Key used for encryption and decryption	Same	Different
Required work factor for brute force attack	2^{56}	2^{128} or more
Encyption /Decryption time	More	Least
Time taken in seconds by brute force attack to search last two bits(approx..)	24.8980sec	31.3410sec

VII. CONCLUSION

The algorithms used by GSM based cellular systems for security have a number of inherent weaknesses while dealing with authentication and confidentiality. This paper focuses on the brute force attack on DES and AES. both the theoretical comparisons and the experimental analysis is done. Based on this study, it is observed that AES is much faster than DES in terms of encryption and decryption. Also AES is more secure wrt DES as it takes more time to crack the larger 128 bit key of AES. As AES is more secure than DES, So it is suggested to replace DES and A5 used on GSM network for security by AES.

REFERENCE

[1] http://jellytelecom.blogspot.in/2013/03/gsmcallmanagement-procedures.html
[2] http://www.roggeweck.net/uploads/media/Student_GSM_Traffic_Management.pdf
[3] "Efficient Method For Securely Managing Passwords" By Asma Tanveer, Aihab Khan,Malik Sikander Hayat Khiyal,Syed Afaq Hussain ,Little Lion Scientific R& D.
[4] file:///X:/wwwdocs/cse57406/ftp/cellular_security/index.html
[5] "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" by B. Padmavathi, S. Ranjitha Kumari, IJSR.
[6] http://www.ijcaonline.org/volume8/number12/pxc3871763.pdf

[7] "Analysis and Comparison between AES and DES Cryptographic Algorithm " By Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, IJEIT.
[8] http://files.sma.de/dl/2585/GSM_UMTSUEN084111.pdf
[9] http://www.academia.edu/3600346/NPA_Protocol_for_Secure_Communications_in_GSM_Cellular_Network
[10] http://ijeit.com/vol%202/Issue%205/IJEIT1412201211_39.pdf
[11] www.ijcem.org/papers102011/ijcem_102011_08.pdf

