ISSN (Online): 2230-7893
www.IJCEM.org

Investigations in Brute Force Attack on Cellular Security Based on Des and Aes

Neeraj Kumar
Assistant Professor (SEE)
Shobhit University, Meerut
iet_neeraj@yahoo.com

Abstract

In this paper the Brute force attack on cellular security based on DES and AES is carried out. It is shown that AES is more secure against brute force attack as compare to DES and A5 encryption algorithms. In the existing GSM network, A5 encryption algorithm is used which does not provide good security because of short length of encryption key. As a result, a new encryption algorithm is required to improve the security of GSM. So, AES algorithm is being proposed to improve the security of GSM instead of A5.

Keywords: DES, AES, A5, GSM, Key lengths, Security.

1. INTRODUCTION

Security plays a more important part in wireless communication system than in the systems that use wired communication. This is mainly because of the ubiquitous nature of the wireless medium that makes it more susceptible to secure attacks than the wired communications. In the wireless medium, anyone can listen to whatever is being sent over network. Also, the presence of communication does not uniquely identify the originator (as it does in the case of a pair of coaxial cable or optical fibers). To make the things worse, any tapping or eavesdropping can not 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 is a system that is used daily by hundred of million of people [2, 3].

1.1 Security Issues In Wireless System

Wireless systems contain all vulnerabilities of wired systems, plus they may have extra vulnerabilities according to their physical behavior [1]. It is so easy to follow the information traffic without being spotted by the system owners. Everybody may capture the radio signals with the suitable equipments over air. Because of the wireless devices are usually mobile, they have less storage capability, memory and weak encryption algorithm (A5). Also network bandwidth of the wireless systems is relatively smaller than wired systems.

2. EXISTING ENCRYPTION ALGORITHM (A5) ON GSM

There are three algorithm used in GSM security that are A3, A5 and A8. A5 is a stream cipher used for encryption in GSM, A3 and A8 are one way functions take place in authentication phase.A3 algorithm is used by GSM network to authenticate the mobile subscriber. The A5 is the algorithm used for encryption in GSM mobile phones [2]. It can be used on both voice and data connections. It is stream cipher that uses a 64 bit secret key but the last 10 bits are set to be zero. This reduces the key space from 2^{64} to 2^{54}. Assuming that the A5 algorithm has an effective key length of 40 bits (Instead of 64) and brute force attack break it with a work factor of 2^{40}[3].

3. BRUTE FORCE ATTACK

A brute force attack is defined as a brute- force search to break a cipher by trying each possible key. In most cases, a cipher is considered secure if it can only be broken by brute force .The attacks depend on the block cipher, or the key length of any encryption algorithm. A typical brute force attack involves exhaustive key search, equivalent to a situation where a thief tries every possible combination in the lock of safe [3, 4].

3.1 Implementation

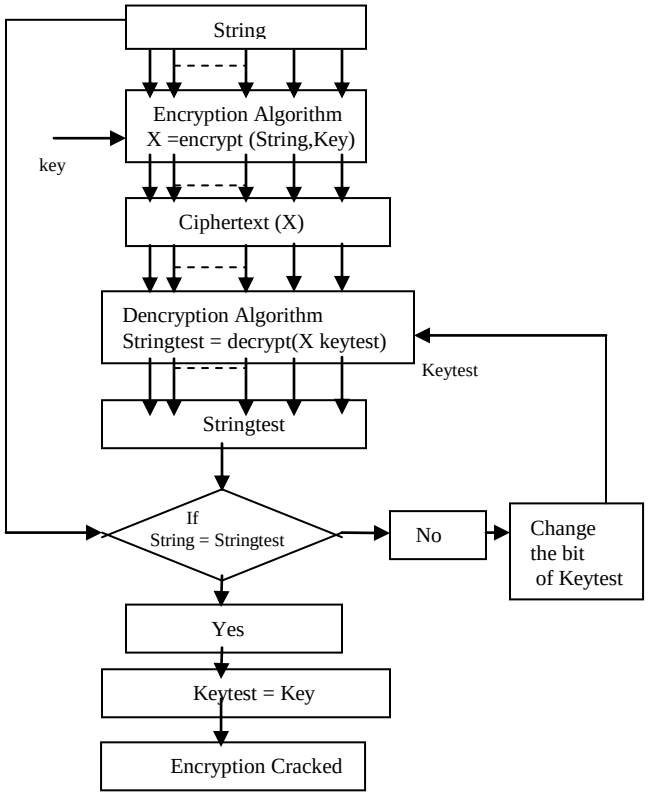

Fig1. Implementation Cycle diagram

ISSN (Online): 2230-7893
www.IJCEM.org

String = 'University Institute of Engineering and Technology'
Key = 'Shobhit University'
Keytest = 'Shobhit Universi'

3.1.1 IMPLEMENTATION STEPS OF BRUTE FORCE ATTACK

Brute force attack algorithm can be explained from the flow diagram given above.

Step followed in brute force cryptanalysis are as follows

1. Plain text string is being encrypted with cipher key.
2. Using encryption algorithm ciphertext X will be generated.
3. Now with the help of assumed key is being "Keytest" decryption algorithm is being implemented.
4. "String test" will be the output of above step.
5. Now original plaintext string is being compare with stringtest.

If match found then keytest become key then encryption algorithm has been cracked. If matched does not found then 1 bit of the keytest is changed and again stringtest will be generated.

4. RESULT

This section will show the result obtained from running the brute force attack program on DES and AES encryption algorithm.

4.1 BRUTE FORCE ATTACK ON DES (DATA ENCRYPTION STANDARD) ALGORITHM

In DES, Data are encrypted in 64-bit blocks using 56 bit key and transform 64-bit input in a series of steps into 64-bit output [7, 8]. Brute force attack can break DES with work factor of 2^{56}.

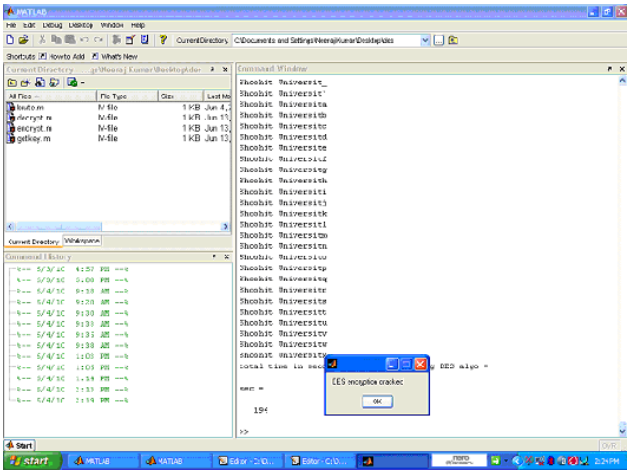

Fig2. Number of seconds required to break the DES algorithm against brute force attack [9,10]

The above figure 2 shows the time taken to find a key by brute force attack program on DES.

4.2 BRUTE FORCE ATTACK ON AES (ADVANCED ENCRYPTION STANDARD) ALGORITHM

In AES, Data are encrypted in 128 -bit blocks using 128 bit key and transform 128 -bit input in a series of steps into
128-bit output [5, 6]. Brute force attack can break AES with work factor of 2^{128}.

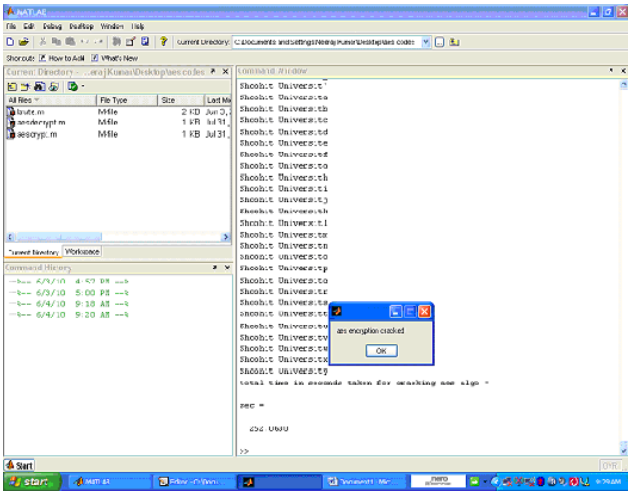

Fig 3. Number of seconds required to break the AES algorithm against brute force attack [11]

The above figure 3 shows the time taken to find a key by brute force attack program on AES.

4.3 COMPARISION TABLE

Algorithms	A5	DES	AES
Key length in bits	40	56	128
Brute force attack break it with work factor of	2^{40}	2^{56}	2^{128}
Brute force attack for searching last two bits	Few second	194 Seconds	252.0630 seconds
Speed	9.6 kb/s	28Mb/s	70.2 Mb/s
Ciphering	Bit by bit ciphering	Block of ciphering	Block of ciphering
Complexity	Less	High	Very high
Security	Less	High	Very high

Table 1

Table 1 shows the comparison between A5 (Encryption Algorithm of Mobile), DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

5. CONCLUSIONS

The presented results showed that AES algorithm is more secure against brute force attack as compare to A5 and DES algorithm. If AES algorithm would be use on GSM network then GSM would be more secure.

6. REFERENCES

[1] A framework for security analysis of mobile wireless networks, Theoretical Computer Science, In Press, Accepted Manuscript, Available online 5 September 2006, Sebastian Nanz and Chris Hankin.

[2] Secure Communication Mechansism for GSM, IEEE Transactions on consumer electronics, Vol 45, No-4,November 1999, Chi-chun Lo and Yu-jen chen.

[3] GSM Security and Encryption, David Margrave, George Mason University.

[4] Differential and linear cryptanalysis for 2-round SPNs , Information Processing Letters, Volume 87, Issue 5, 15 September 2003, Pages 277-282 Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung and Seonhee Yoon.

[5] Impossible differential cryptanalysis of 7- round Advanced Encryption Standard(AES),Raphel C-W Phan, 9 April 2003.

[6] J. Daemen: Annex to AES proposal Rijndael. http://www.esat.kuleuven.ac.be/~rijmen/rijndael/PropCorr.PDF, (1998).

[7] Linear cryptanalysis method for DES cipher. EUROCRYPT 1993, Matsui, M. (1993).

[8] National Institute of Standards and Technology: Data Encryption Standard (DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, (2001).

[9] The Mathworks: Matlab , The Language of Technical Computing. http://www.mathworks.com/products/matlab, (2001).

[10] The Mathworks: Galois Field Computations. http://www.mathworks.com/access/helpdesk/help/toolbox/ comm/, Communications Toolbox, (2001).

[11] N.D Vasumathy, G. Velmathi, and N. Splavos "On the Rijndael Encryption algorithm Implementation with MATLAB software Programming".