Enhancement of A5/1 encryption algorithm

Enhancement of A5/1 encryption algorithm

Ria Elin Thomas, Chandhiny G, Katyayani Sharma, H Santhi and P Gayathri
School of Computer Science and Engineering, VIT University, Vellore- 632014, India

E-mail: hsanthi@vit.ac.in

Abstract. Mobiles have become an integral part of today's world. Various standards have been proposed for the mobile communication, one of them being GSM. With the rising increase of mobile-based crimes, it is necessary to improve the security of the information passed in the form of voice or data. GSM uses A5/1 for its encryption. It is known that various attacks have been implemented, exploiting the vulnerabilities present within the A5/1 algorithm. Thus, in this paper, we proceed to look at what these vulnerabilities are, and propose the enhanced A5/1 (E-A5/1) where, we try to improve the security provided by the A5/1 algorithm by XORing the key stream generated with a pseudo random number, without increasing the time complexity. We need to study what the vulnerabilities of the base algorithm (A5/1) is, and try to improve upon its security. This will help in the future releases of the A5 family of algorithms.

1. Introduction

GSM (expanded as Global System for Mobile communication) is been extensively used in the mobile networks for communication. GSM [1] has the architecture that has Mobile Stations, Base Service Stations etc., as shown in the Figure.1 below.

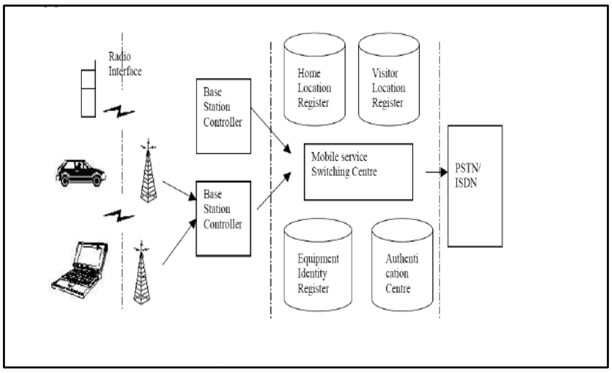


Figure 1. General Architecture of GSM

To provide Security in it, A5/x algorithms are used for encryption and is used to ensure privacy of all the conversations that happen on GSM mobile phones. A3 is used for authentication and A8 is used for generation of the cipher key. These algorithms are used along with A5/x algorithms which secures the information sent over the air interface in mobile networks. A5/1 is a stream cipher and is very fast. A5/1 is made up of linear feedback shift register (LFSR) and the working is explained in the experimental analysis section of this paper.

A5/1 [2] is the basic algorithm which we need to know in depth for future enhancements. In order to secure the GSM architecture, providing the security and privacy of data, enhancements in the existing algorithm is proposed and in order to fulfil this, we have XORing a randomly generated number with the resulting key stream, thereby not increasing the complexity.

The aim of this project is to analyse and get a clear idea about the A5/1 algorithm used for encryption purpose in the mobile network along with its security issues and threats. Through this project, our objective is to enhance the security in the algorithm and maintain its time complexity.

The section 2 deals with the related work. Section 3 talks about A5/1 algorithm. Section 4 about the E-A5/1 algorithm and section 5 discusses about the result in which the comparison of the execution time of the A5/1 and E-A5/1 algorithm.

2. Related Work

Authors in [3] have identified the security vulnerabilities of digital mobile communication systems along with the emerging threats. This paper provides a detailed knowledge on the issues that could be referred to while working with the future systems. Authors in [4], improvised the GSM network security by generating a new S-Box that improves the efficiency and is done in order to overcome the weakness in clocking mechanism that used in A5/1 stream cipher. Authors in [5], proposed a hybridA5/3 and encipher and decipher based RC6 algorithm also called (A5/3RC6) which encrypts the information over GSM network. The comparative performance analysis is also done.

Authors in [6] analysed 3 mobile operators in Greece, using a simulator, (U) SimMonitor, based on their applied security. They concluded that based on the numerical results and security measurements, mobile operators do not implement good security practices, thereby exposing their subscribers to potential risk. An improved Linear Feedback Shift Register based stream cipher was proposed for the A5 family. [7] This algorithm comprised of a variable tapping scheme, a non-linear combination function, a new clocking mechanism, and a key-generation mechanism with increased number of registers and improved lengths of these registers. The randomness of this algorithm was also evaluated using MATLAB.

Authors in [8], proposed that A5/1 with image bit-plane separation can be used for encryption of images over wireless networks. They converted each bit plane into a stream of data and XORed it with a keystream that is generated by the A5/1 algorithm. This was evaluated with respect to AES algorithm, keeping it as a benchmark.

In [9], authors proposed a modified A5/1 algorithm which improves the level of randomness, by introducing a new S-box generation. They have, however, concluded that their proposed algorithm has more complexity compared to the original algorithm.

Authors in [10], have surveyed and analysed the security threats, challenges, and provided solutions for the mechanisms inherent in all edge paradigms that has to be used with other paradigms in the future, while highlighting capable synergies and places of collaboration.

Authors in [12] has explained new vulnerabilities and threats in mobile network which has been upgrading day by day. The drawbacks act as a major concern for the security and the performance of mobile networks, since attacks can affect the whole network and various problems. Here, the security issues are studied in detail and classified. Attacks and counter measures for them are also surveyed in this paper.

Authors in [13], took the help of a simulator, Simulink, to better understand the flaws in the A5/1 algorithm, and determined three vulnerabilities in it. Using Simulink, they could better capture the working of the clocking unit, and proposed modification of the majority function and developing the link of the second register, thereby addressing the three weaknesses.

In [14], the authors analysed the weaknesses of the GSM network and gives a detailed description on how to audit the GSM networks to find the vulnerabilities. A cryptanalysis was performed on A5/1 and Trivium. [15] Using Cube attack, the authors could retrieve the key bits and linearly independent functions of trivium and A5/1 algorithms respectively.

Authors in [16], took a hand in improving the security of GSM by addressing two of the weaknesses in A5/1. They improved clocking mechanism by introducing a new function, and replaced the original linear combining function with a cryptographically better non-linear function. In [17], the authors attempted to increase the length of the generated keystream sequence by applying a unit delay in the A5/1 algorithm. This was simulated in Simulink.

Authors in [19] surveyed about the A5/1 and W7 for protecting the distribution of digital images in an effective and secure way. Histogram analysis, Randomness Tests, etc, are done for the enhancement of the algorithms. It is implemented in MATLAB. In [20], the authors reviewed and selected the best algorithm for speech transmission in GSM. They concluded their paper, saying that AES-Rjindael algorithm is best suited for the wireless network which is resource constrained.

Authors in [21], tried to improve the A5/1 by making the linear operator into a non-linear feedback mechanism. The proposed algorithm was implemented in MATLAB. An enhanced A5/1 algorithm was proposed [24] and its parameters (like the time period of the changing states, the vector of 3 bits that select the shuffling of LFSR, and the parameters that cause the selection of the tapings for all the LSFRs) were analysed.

Authors in [25]- modified the A5/1 stream cipher by running several statistical tests like frequency test, serial test, runs test etc., for enhancing the security in it. Authors in [26], have explained about the simulation of A5/3 and A5/1 algorithms in detail along with the need of this simulation.

Authors in [27] -explains about the attack done in assistance with hardware, on the well-known A5/1 stream cipher. Improvisation of 16% in the computational time is done.

Authors in [28] -have briefly presented about the most important flaws in security stream of the GSM network and in its channels,that are used for transportation purposes. It also provides some practical solutions to apply and to improve the security of present 2G systems.

A detailed description of the A5/1 algorithm along with the cryptanalysis done was mentioned in [29]. The authors also gave their view of a practical approach for cryptanalyzing the A5/1 algorithm. Authors in [30]- talks about the real-time attacks on PC with the GSM algorithm and a best algorithm which is suited for securing speech in GSM networks is proposed in addition to it.

In most of the papers, the security is increased by increasing the complexity. They are trying to modify the hardware by increasing the size of the LFSR registers. They have linked AES with A5/1 algorithm that increases the storage complexity and in many papers only partial solutions have been provided for enhancing the security of GSM network. But here we are trying to enhance the security without increasing the complexities.

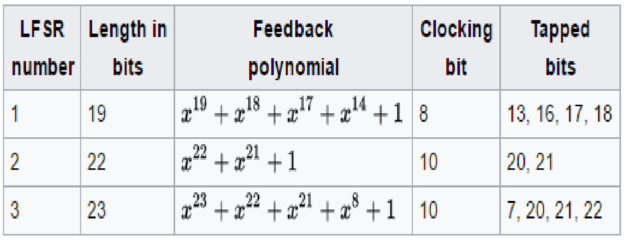
Thus, from the above papers, we get to know the vulnerabilities and security issues involved in the A5/1 algorithm and also about the modifications that were proposed. Most of the modifications require hardware and does not address the complexity issues.

3. A5/1 Encryption Algorithm

A5/1 (stream cipher) which is used to provide the security for the communication in GSM cellular network. This algorithm is one of the seven categories specified for GSM. Transmission in GSM is in the form of bursts and one burst is sent like every 4.615 millisecond in a unidirectional channel which contains 114 bits that are available for information.

We use A5/1 to produce each burst a 114-bit sequence of keystream time to time, which is then XORed with 114 bits prior to modulation. A5/1 uses three linear feedback shift registers. A register is said to be clocked, if clocking bit matches with clocking bit of one or more registers. A5/1 uses a combination of LFSRs with different clocking. The three registers are given below.

Table 1. LFSR polynomials



LFSR number	Length in bits	Feedback polynomial	Clocking bit	Tapped bits
1	19	$x^{19}+x^{18}+x^{17}+x^{14}+1$	8	13, 16, 17, 18
2	22	$x^{22}+x^{21}+1$	10	20, 21
3	23	$x^{23}+x^{22}+x^{21}+x^{8}+1$	10	7, 20, 21, 22

A5/1 is initialized by using 64-bit key together with a publicly known 22-bit frame number. The older GSM implementations used Comp128v1 for key generation, which had 10 key bits fixed at zero, that results in 54-bit key length. This drawback was removed by introducing Comp128v2 and that resulted in 54-bit key length. When it operates in GPRS/EDGE mode, the higher bandwidth radio modulation the larger 348 bit frames are produced. Thereafter, A5/3 can be used in a stream cipher mode to maintain the confidentiality. Indexing of the bits with least significant bit (LSB) is 0.

A majority rule is used in the clocking of the registers in a stop/go way. A clocking bit is associated with each register. For each cycle, the majority bit is determined by clocking bit examination of all the three registers. If the clocking bit agrees with the majority bit then a register is said to be clocked. Therefore, for every step at least two or three registers are clocked, with probability of ¾ for each register.

The initial step is the setting of register to zero. For 64 cycles, the 64-bit key that is secret, is allowed to mix in the following scheme: for every cycle, the ith key bit gets added to least significant bit of every register by using XOR. Every register is clocked afterwards. Likewise, for 22 cycles the 22 bits of frame numbers are added. After this the whole system is clocked using the majority clocking method for 100 cycles where the output is discarded. Once this is completed, the generation of two 114-bit sequence of output keystream shown in figure.2, by the cipher would be ready and where 114 for downlink and last 114 for uplink done could be seen.

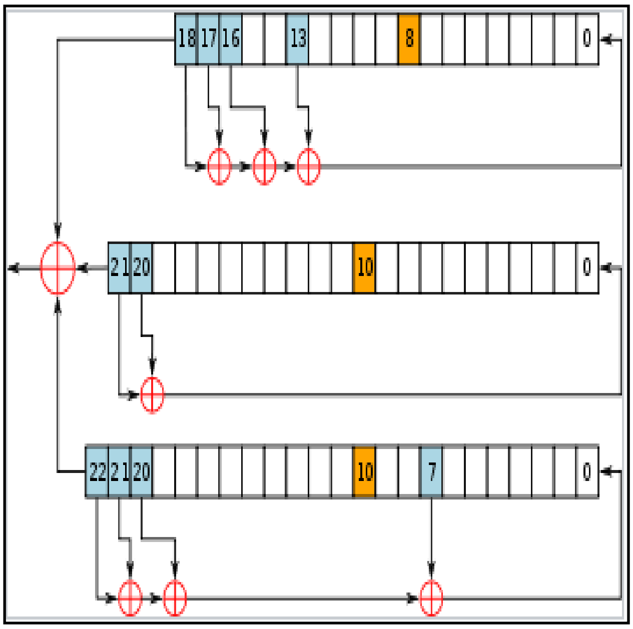


Figure 2. A5/1 key stream Generator

4. Enhanced A5/1 Algorithm

Here, we are XORing a 114-Bit random number with the key stream which is finally XORed with the plain text to get the cipher text which is big. Thus, like during the man-in-the-middle attack, if the attacker tries to decrypt the encrypted conversation in GSM mobile network, it takes more time and is difficult to decode it without a key. By doing this XOR function, the time complexity is also not increased but decreased. Thus, by this way, our proposed work is said to be more effective than the previous one. Figure represents the key stream generator of enhanced A5/1 algorithm.

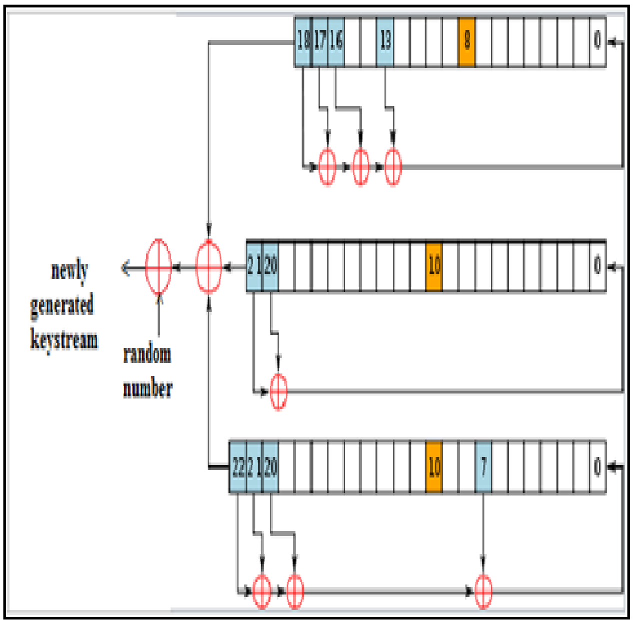


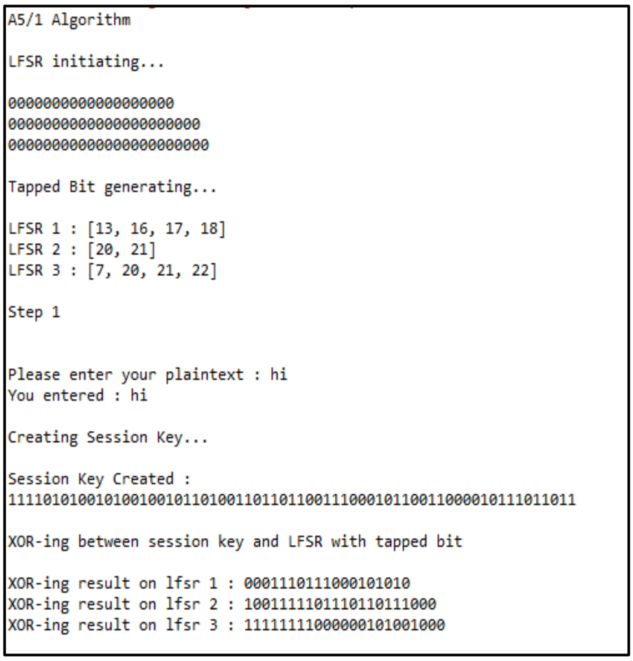
Figure 3. Enhanced A5/1 Key Stream Generator

The modified pseudo code for A5/1 algorithm is explained below.

A5/1 Algorithm
Input: 64 bit session key(secret key), 22 bit frame bits(plain text).
Output: Cipher text size 228 bits.
Process
Step1: Initialize 3 registers are set to zero
Step 2: Load 64 bits session key(secret key) + 22 bits of frame number(public key), session key and frame number is XORed bit-by-bit with the LSB(least significant bits), and the registers are clocked regularly.
Step 3: (100) times the registers are cycled and discarding any output(all registers are closed irregularly the majority function identify the shifted registers)
Step 4:(228) times the register are cycled (clocked irregularly the majority function identify the shifted registers) to generate the key stream.
Step 5: add random generated number by XORing with the resulting keystream to find final keystream
Step 6: all steps repeated for the next frame.
Step 7:end

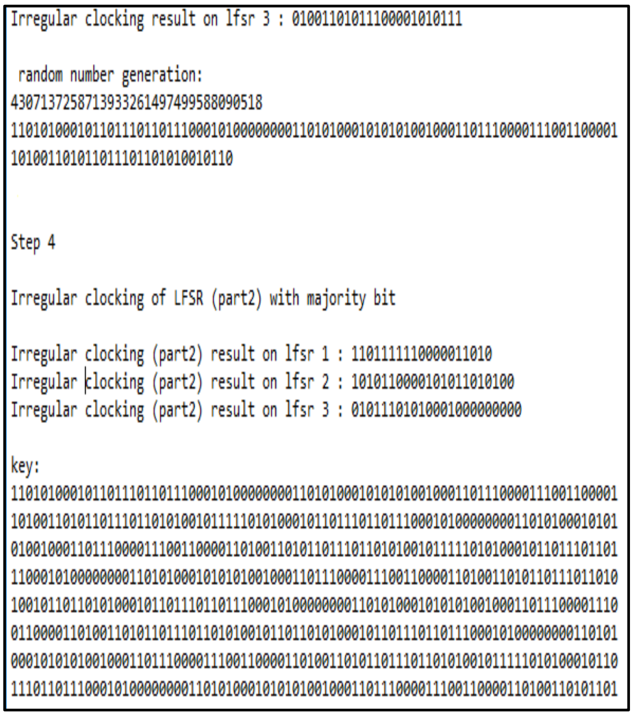
5. Result and Analysis

The key stream is generated after XORing with the random number generated initially and the final cipher text that is generated after XORing the plain text with the obtained key stream is shown in the images. Python language is used here, to perform the modifications proposed. Python IDE of version 3.5 is used. Figure 4 represents the random number that is generated and is also XORed to get the key. Figure 5 shows the session key that was generated. Figure 6 depicts the cipher text.



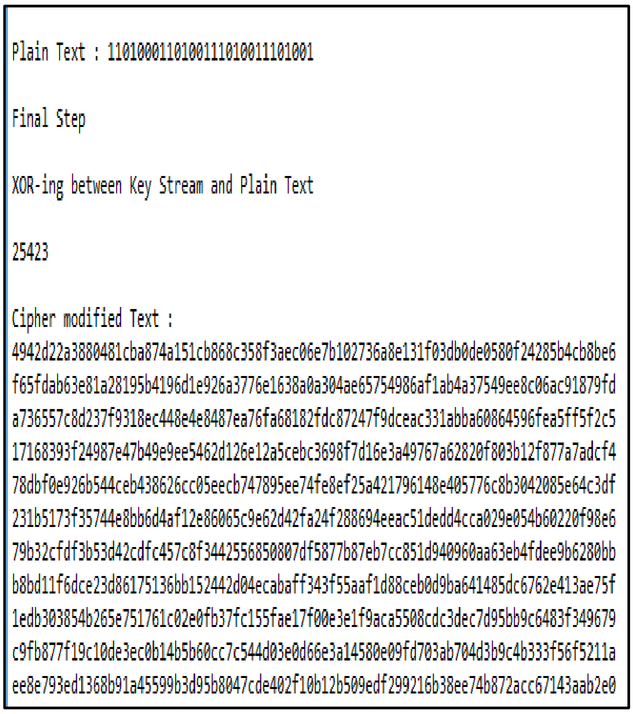
```
A5/1 Algorithm

LFSR initiating...

0000000000000000000
0000000000000000000000
00000000000000000000000

Tapped Bit generating...

LFSR 1 : [13, 16, 17, 18]
LFSR 2 : [20, 21]
LFSR 3 : [7, 20, 21, 22]

Step 1


Please enter your plaintext : hi
You entered : hi

Creating Session Key...

Session Key Created :
11110101001010010010110100110110110011100010110011000010111011011

XOR-ing between session key and LFSR with tapped bit

XOR-ing result on lfsr 1 : 0001110111000101010
XOR-ing result on lfsr 2 : 1001111101110110111000
XOR-ing result on lfsr 3 : 11111111000000101001000
```

Figure 4. Session Key generation



```
Irregular clocking result on lfsr 3 : 01001101011100001010111

 random number generation:
4307137258713933261497499588090518
1101010001011011101101110001010000000011010100010101010010001101110000111001100001
101001101011011101101010010110

Step 4

Irregular clocking of LFSR (part2) with majority bit

Irregular clocking (part2) result on lfsr 1 : 1101111110000011010
Irregular clocking (part2) result on lfsr 2 : 1010110000101011010100
Irregular clocking (part2) result on lfsr 3 : 01011101010001000000000

key:
1101010001011011101101110001010000000011010100010101010010001101110000111001100001
1010011010110111011010100101111101010001011011101101110001010000000011010100010101
0100100011011100001110011000011010011010110111011010100101111101010001011011101101
1100010100000000110101000101010100100011011100001110011000011010011010110111011010
1001011011010100010110111011011100010100000000110101000101010100100011011100001110
0110000110100110101101110110101001011011010100010110111011011100010100000000110101
0001010101001000110111000011100110000110100110101101110110101001011111010100010110
1110110111000101000000001101010001010101001000110111000011100110000110100110101101
```

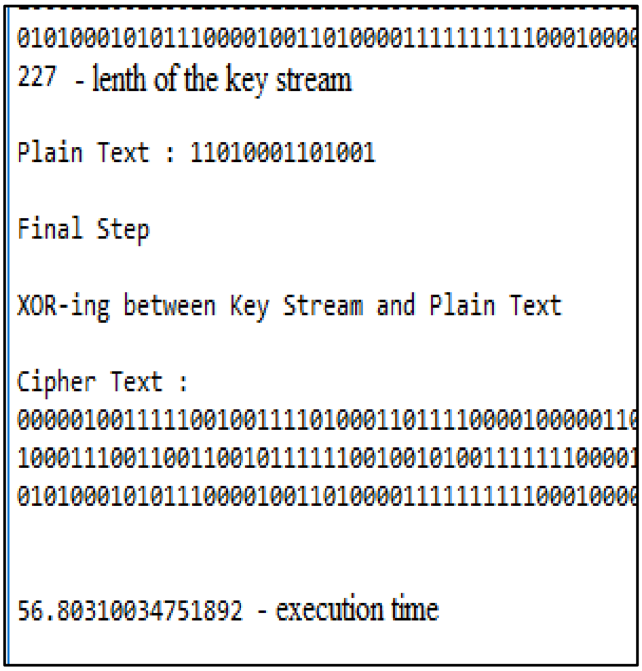
Figure 5. Random number generated



```
Plain Text : 1101000110100111010011101001

Final Step

XOR-ing between Key Stream and Plain Text

25423

Cipher modified Text :
4942d22a3880481cba874a151cb868c358f3aec06e7b102736a8e131f03db0de0580f24285b4cb8be6
f65fdab63e81a28195b4196d1e926a3776e1638a0a304ae65754986af1ab4a37549ee8c06ac91879fd
a736557c8d237f9318ec448e4e8487ea76fa68182fdc87247f9dceac331abba60864596fea5ff5f2c5
17168393f24987e47b49e9ee5462d126e12a5cebc3698f7d16e3a49767a62820f803b12f877a7adcf4
78dbf0e926b544ceb438626cc05eecb747895ee74fe8ef25a421796148e405776c8b3042085e64c3df
231b5173f35744e8bb6d4af12e86065c9e62d42fa24f288694eeac51dedd4cca029e054b60220f98e6
79b32cfdf3b53d42cdfc457c8f3442556850807df5877b87eb7cc851d940960aa63eb4fdee9b6280bb
b8bd11f6dce23d86175136bb152442d04ecabaff343f55aaf1d88ceb0d9ba641485dc6762e413ae75f
1edb303854b265e751761c02e0fb37fc155fae17f00e3e1f9aca5508cdc3dec7d95bb9c6483f349679
c9fb877f19c10de3ec0b14b5b60cc7c544d03e0d66e3a14580e09fd703ab704d3b9c4b333f56f5211a
ee8e793ed1368b91a45599b3d95b8047cde402f10b12b509edf299216b38ee74b872acc67143aab2e0
```

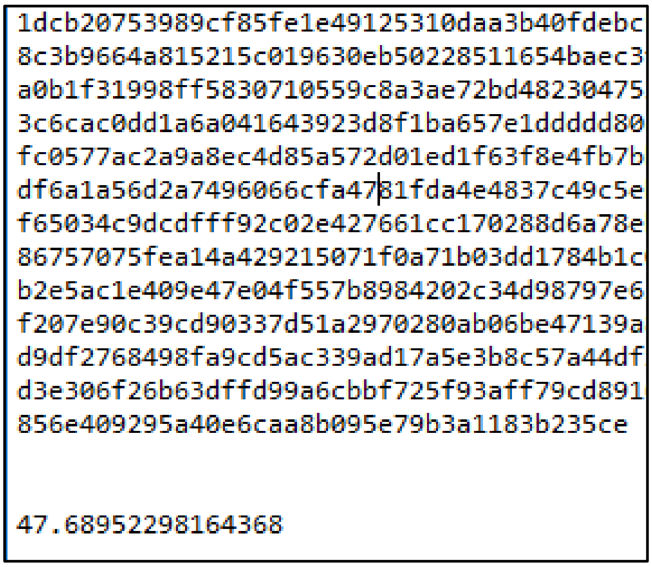
Figure 6. Cipher text

The execution time comparison with the existing and proposed system is made below.



```
01010001010111000010011010000111111111100010000
227  - lenth of the key stream

Plain Text : 11010001101001

Final Step

XOR-ing between Key Stream and Plain Text

Cipher Text :
00000100111110010011110100011011110000100000110
1000111001100110010111111001001010011111111000001
01010001010111000010011010000111111111100010000



56.80310034751892 - execution time
```

Figure 7. Execution time for Existing system.



```
1dcb20753989cf85fe1e49125310daa3b40fdebc
8c3b9664a815215c019630eb50228511654baec3
a0b1f31998ff5830710559c8a3ae72bd48230475
3c6cac0dd1a6a041643923d8f1ba657e1ddddd80
fc0577ac2a9a8ec4d85a572d01ed1f63f8e4fb7b
df6a1a56d2a7496066cfa4781fda4e4837c49c5e
f65034c9dcdfff92c02e427661cc170288d6a78e
86757075fea14a429215071f0a71b03dd1784b1c
b2e5ac1e409e47e04f557b8984202c34d98797e6
f207e90c39cd90337d51a2970280ab06be47139a
d9df2768498fa9cd5ac339ad17a5e3b8c57a44df
d3e306f26b63dffd99a6cbbf725f93aff79cd891
856e409295a40e6caa8b095e79b3a1183b235ce


47.68952298164368
```

Figure 8. Execution time of Enhanced A5/1 Algorithm.

Figures. 7 and 8 clearly show that the proposed system execution time is less than the existing system thus, time complexity is not modified and the security is also enhanced in this A5/1 algorithm. Thus, the cipher text and the key stream generated are huge and decoding will take more time and so E-A5/1 algorithm is considered to be as more secured with less time complexity. The space complexity is increased, but could be maintained by compressing it and then encrypting the message with the key stream generated. The key is 228-bit but uses 114 bit for uplink and 114-bit for downlink. So, here 114-bit random number is generated and used for encryption.

6. Conclusion

In this paper, we have analysed the threats and vulnerabilities of A5/1 from the existing papers and have proposed the modified algorithm which does not increase the time complexity. Improving the security in A5/1 will also help to understand the security needs that are to be met when releasing future versions of the A5 algorithm. Our proposed algorithm does not need any extra hardware requirements and so it is inexpensive. Maintain the time complexity and also making it hard for the attackers to decrypt the message is done in this paper. The future enhancements could be done in reducing the storage size of the cipher text by maintain it hard for the attackers to crack it. This could also be tried in GSM simulation to check whether the huge cipher texts could be used for communication or not. And also, the authentication could be checked using hash values in E-A5/1 algorithm which gives us a secured communication in GSM. As a whole, A5/1 algorithm is studied in details on the process of its working and also some enhancements in it are made.

References

[1] D'Orazio C J, Lu R, Choo K K R and Vasilakos A V (2017) A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps *Applied Mathematics and Computation* 523–544

[2] Sinha K, Darshani M P and Kumari S (2017) Enhanced, Efficient End-to-End Voice Encryption Using A5 / 3RC6 over GSM Network **1** 1981–1986

[3] Gkioulos V, Wolthusen S D and Iossifides A (n.d.) (2016) A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE) 2 School of Mathematics and Information Security , Royal Holloway , University of London , United Kingdom 3 Department of Electronics Engineering

[4] Marappan D (2017) Securing Mobile Technology of GSM using A5 / 1 Algorithm 111–113

[5] Jeske D and van Schaik P (2017) Familiarity with Internet threats: Beyond awareness *Computers & Security* **66** 129–141

[6] Xenakis C, Ntantogian C and Panos O (2016) (U) Simonton: A mobile application for security evaluation of cellular networks. *Computers & Security* **60** 62–78

[7] Singh A K and Bora B S (2016) Design of Enhanced Pseudo-Random Sequence Generator usable in GSM Communication **3** 530–534

[8] Naveen C (2016) Image Encryption Technique Using Improved A5 / 1 Cipher on Image Bitplanes for Wireless Data Security

[9] Ali M (2016) Improvement Majority Function in A5/1 stream cipher Algorithm **34**

[10] Roman R, Lopez J and Mambo M (2016) Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges *Future Generation Computer Systems* **28** 1-19

[11] Sarika S, Pravin A, Vijayakumar A and Selvamani K (2016) Security Issues in Mobile Ad Hoc Networks *Procedia Computer Science* **92** 329–335

[12] Mavoungou S, Kaddoum G, Taha M and Matar G (2016) Survey on threats and attacks on mobile networks *IEEE Access* **4** 4543–4572

[13] Sadkhan S B and Jawad N H (2015) Simulink Based Implementation of Developed A5/1 Stream Cipher Cryptosystems. *Procedia Computer Science* **65**(Iccmit) 350–357

[14] Bird R, Canada B C and Layers A G S M (2015) Investigating Vulnerabilities in GSM Security

[15] Islam S and Haq I U (2014) Cube Attack on Trivium and A5 / 1 Stream Ciphers 1–7

[16] Madani M and Chitroub S (2014) Enhancement of A5 / 1 Stream Cipher Overcoming its Weaknesses. *The Tenth International Conference on Wireless and Mobile Communications (ICWMC)* 154–159

[17] Sadkhan S B and Jawad N H (2014) Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay. *Iraqi Academic Scientific Journal* **22** 622–633

[18] Bhal A S and Dhillon Z (2014) LFSR Based Stream Cipher (Enhanced A5/1). *International Journal of Computer Applications* **57** 32–35

[19] Jolfaei A and Mirghadri A (2014) SurveyImage Encryption Using A5 1 and W7 1–8

[20] Kulkarni M M (2013) Encryption Algorithm Addressing GSM Security Issues- A Review **2** 268–273

[21] Kaur R and Bajaj N (2012) Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher *International Journal of Computer Applications* **57** 32–35

[22] Narcisse O and Post E (2012) Security in the Global System for Mobile Communications GSM

[23] Gold S (2011) Cracking GSM *Network Security* **2011** 12–15

[24] Bajaj N (2011) Effects of Parameters of Enhanced A5/1 *International Journal of Computer Applications* **2** 7–13

[25] Zakaria N H, Seman K and Abdullah I (2011) Modified A5/1 Based Stream Cipher for Secured GSM Communication. *International Journal of Computer Science and Network Security (IJCSNS)* **11** 223–226

[26] Sankaliya A R and Mandloi A (2011) Implementation of Cryptographic Algorithms for GSM Cellular Standard Ganpat University *Journal of Engineering & Technology* **1** 14–18

[27] Gendrullis T, Novotný M and Rupp A (2008) A real-world attack breaking A5/1 within hoursvLecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5154 *LNCS* **9404** 266–282

[28] Toorani M and Shirazi A A B (2008) Solutions to the GSM security weaknesses *Proceedings - The 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies NGMAST* 576–581

[29] Stockinger T (2005) GSM network and its privacy - The A5 stream cipher 1–13

[30] Biryukov A, Shamir A and Wagner D (2001) Real Time Cryptanalysis of A5/1 on a PC. *Fast Software Encryption* **1999** 1–16