Proc. of the 2nd International Conference on Electrical, Communication and Computer Engineering (ICECCE)
12-13 June 2020, Istanbul, Turkey

Voice Cipher Using Rc4 Algorithm

Marwah Kamil Hussein
Department of Computer Information Systems
University of Basrah, Iraq
lava85k@gmail.com

***Abstract*— Encryption plays a major role in achieving privacy, especially in communications and information systems such as military systems, banks, telecommunications and individuals, and in mobile phone networks in particular. The (GSM) standard provides a level of privacy that may not be sufficient for some users, as this study is presented a proposed system for applying audio coding in cellular communication networks from the beginning (mobile) to the end (mobile (via the standard mobile communications system) GSM), and in this standard is used the A5 algorithm for audio coding is only for transmitting stations, while for the rest of the network it is without transmitting coding the data as it is, so we in this study proposed the application of RC4 algorithm with A5 algorithm through encryption keys controlled by the sender and receiver in audio coding from start to finish to ensure complete encryption and privacy in network phone calls and the tool used in this the research is a matlab program to create a simulated environment for the transmission between the sender and the receiver to add the RC4 algorithm for these stages and one of the results of the study using the RC4 algorithm in the transmission model in the telephone network can achieve greater privacy in telephone calls communication without affecting the sound quality through the two encryption keys controlled by both ends connection.**

Keywords—information security, GSM, network wireless, A5 encryption, RC4.

I. Introduction

Information security means keeping your information under your direct and complete control, that's meaning of no it can be accessed by anyone else without your permission, and be aware of the risks involved on letting someone access your private information, you definitely do not want others to have it an introduction to your private information [1].

It is clear that most people want to maintain privacy their sensitive information, especially the subscribers of GSM networks that have many security issues where one of the most important issues is the sharing of information between wired networks and GSM networks wireless, which does not provide a protected voice connection from start to end as the sound travels through various media A5 encryption algorithm is used only at distribution (Al-Tor) stations to encrypt calls and it is in the rest of the network without encryption, and we know that the A5 packet is standard because it is used by car phone companies and it is very easy to break it and eavesdrop on phone calls by a party other than the sender and receiver, and from here the reliability of the subscribers in the network is not provided, and it is possible Solve this problem by using additional new packet options with the A5 algorithm that deals with the voice coding process in phone calls from start to end in the car phone networks.

Through the automobile network, which is the best tool for this study, the packet used for this task is the RC4 algorithm, which ensures that mobile phone subscribers have more reliability, privacy and security in the communication channel [2].

Mobile phone networks are among the most widely used networks around the world and they are used before governments, companies and banks on all economic, political and social levels, hence the importance of privacy in this type of network [3], where one of the algorithms A5/1 and A5/2 is used in the process of encoding the voice of phone calls in distribution stations only and the sound is before it reaches a station the transmission is not encoded and audio coding is not achieved from start to finish, it is well known that this type of standard is standard and it is easy to decode and access the original sound during the communication process [4].

Hence the problem of this study, which revolves around achieving a secure connection to the mobile phone subscribers from beginning to end, through the process of coding sound from start (sender) to end (receiver) through the RC4 algorithm, using the keys for encryption and decryption is controlled between the ends of the call.

We find that the most serious threat to mobile phone networks is the process of eavesdropping on calls and may cause it damage to the service company or subscribers to this network, and this can be done by cloning the smart card (SIM card), or what is known as impersonation, and from here we cannot guarantee the customer privacy in the communication process neither on the part of the company nor on the part of another party, even in the case of movement between local and global networks [5].

It is very important to point out the importance of this research, which is achieving confidentiality and privacy in phone calls in the car phone network, and that through the security binaries that they are subject to a number of encryption keys that are difficult for an attacker to gain access to or guess that the encryption and decryption key is only between the sender and receiver in the communication process, thus narrowing the process entry to another party through the use of an additional tool that is controlled by the parties of the call or automatic image, where the key is loaded randomly.

We can summarize the main objectives of this research in several axes:

- Learn about the mechanism of mobile phone network (GSM)

978-1-7281-7116-6/20/$31.00 ©2020 IEEE

- Learn about the standard algorithms used to encode audio in a mobile phone network.
- Add the RC4 algorithm to the transmission model in mobile phone networks to encode the audio in calls to add more privacy and reliability to the communication process without an increase in the number of bits transmitted and the effect of sound quality through the decoder and decode keys between the parties to the conversation.

II. RESEARCH STRUCTURE

A. *Previous Studies*

- Dr. Noha Hassan Abd Al-Rizk [6]
  From the Sudan University of Science and Technology and Jia to obtain a master's degree, the study discussed the concept of ciphering voice in mobile networks by car companies and the perfect alternative to the A5 algorithm it could be RC4 where it proved possible to replace the A5 packet cells with the RC4 algorithm without it affects the communication quality and the increase in the size of the transmitting diodes. The study reached several results: The most important thing is that by changing the A5 algorithm, we can deviate from the standard and achieve better privacy in the contact content. Among the recommendations in the future studies recommended by the study discuss the practical application of this it is a package, especially on sound, and it is also possible to replace the A5 algorithm with one of the RC4 algorithms or AES or DES to bring privacy and security to the side of mobile phone and call services and that the change in the A5 packet properties does not affect the communication quality and the tools used in this study Matlab program.

- Dr. Khalid and Abdulaziz University [7]
  A scientific paper from the *International Journal of Distributed Systems IJDPS* discusses the use of the DES algorithm before the telecommunications companies to generate random keys to encrypt calls at distribution stations in the phone companies. The car where the Matlab program was used to create a simulated environment for the car phone network and the study arrived to many results: Among them, by using the DES packet socket, more confidentiality and privacy can be achieved in the communication channel that are between the conversation parties. The DES algorithm can be used to encode the communication channel without altering the sound quality the sender (sending diodes).

- Sarab Mageed and Asraa Nafe [8]
  A scientific paper from the *University of Baghdad College of Computers*, the study discussed the possibility of safe voice transmission over a network internet through full encryption based on the RC4 algorithm and because mobile phone networks are economically expensive and insecure as calls can be vulnerable to attack and exposure to eavesdrop. The practical application of this study is the Android application and the results were evaluated through the average irrigation score MOS is a term that refers to the ability to provide a different priority for different applications, users, or streams for data, or to ensure a certain level of performance for data flow.

In this paper, we suggest a new approach to modifying the RC4 encryption algorithm streamlined reliance on indivisible polynomial. This research consists of proposals: *First proposal:* Modify the key of the Rc4 algorithm streamlined encoding. *Second proposal:* Modify the Rc4 encryption algorithm for streamlined encryption using one key and indivisible polynomial (XOR) process replacement. *Third proposal:* merging the first and second proposals. *Quarterly proposal:* Modify the RC4 encryption algorithm for streamlined encryption using XOR operation binary indivisible polynomial.

After implementing the proposed system in this research, a number of results were obtained and through these results The proposed system has been evaluated due to the use of the binary key, and it provides a high level of complexity resist large attacks, so it will be very difficult to guess the key, for example, to decode an encrypted message consisting of 8 bits, the attacker needs (30 * 28) an attempt to possibly switch the keys using one key 212 * Needs 31 key probability attempts to use the binary decoder key.

B. *Discuss The Results of This Study With The Previous Studies*

This research discusses the practical use of the RC4 algorithm for coding audio in phone calls in mobile phone networks by both ends of the communication process (the transmitter) and (the receiver) with the A5 algorithm originally used by automobile phone networks through controlled and decrypted keys only by the parties to the phone call to ensure more privacy and reliability in the communication process, and after designing the proposed application, many results have been reached, including: -

- The ability to use the RC4 algorithm with the A5 algorithm to encode audio in telephone networks the car, and through its use, we can guarantee the user of the car phone networks more security, especially that by using this algorithm we can deviate from the standard and one of the most important goals encryption is out of the ordinary.
- Also it can be allowed for the user to control the encryption keys by himself, so as to ensure more of reliability in the communication process, especially in international calls that travel between the medium wired and non-wired. It can be summed up the difference between this study and the father of the previous studies mentioned in that the previous studies concluded to me.

Use the RC4 bellow beacon as an alternative to the A5 algorithm on the communication networks side to protect the company services and phone calls services as in Noha Hassan's study, but this study is discussed use the RC4 algorithm to encode audio in phone calls in mobile phone networks from start to finish, with switches controlled by the contacts only.

III. ENCRYPTION METHOD USED

This standard is based on Lucifer algorithm, which uses a 56-bit encryption key Bit, and requires that both the transmitter and receiver have the same secret key. A year later one from the application of the Data Encryption Standard (DES), three university professors developed another coding system that launched it has a name (RSA), and this system uses a public key and a private key instead of using only one key. Although this system was very suitable for hardware computer complex, but it was later hacked. This remained the case until (Phil Zimmerman) in 1986 developed an RSA encryption program, but it is characterized by the use of a 128-bit key, called (Pretty Good Privacy- PGP). Where I used a system of quantitative coding, and this system uses photons to send secret encryption keys, you hide each key using the most well-known principle of quantum mechanics, which is Heisenberg's principle of doubt, and when exchanging quantum keys, no one can ever know these keys. All emails, phone calls, or financial exchanges encrypted with these keys will be in complete safety [9].

A. GSM (Global Systems Mobiles)

It is the global system for mobile communication (mobile), and it is the current compatible network in all countries of the world. GSM has combined a combination of TDMA and FDMA technologies. Whereas, it uses eight slides of time with the time that the carrier supports eight channels at full rate or sixteen channels with half the full rate of frequency separation between one channel and another 211 kHz note that the mobile transmission channels occupy 961 MHz for reception. N-915 MHz for transmission.

The maximum transmission capacity depends on the classification of the mobile station and it ranges between the values 1.8, 2, 5, 8 and 21 watts and equipped with an internal function to prevent interference with controlled programmed transmission power and swing power at the beginning and end of the time slice. The power fluctuation reduces the impact of interference and helps prevent dead spots in coverage due to the fading of different paths [10].

B. GSM Network Work

When the MS (mobile) device is turned on, it tries to connect to the network, hoping to allow it he or she authorizes the network to use its resources. This can happen for the parent network or even if you are in case of roaming and roaming, network services other than the parent network are used. The MS mobile device it works in connection with the BTS located in the same place or in other words, the BTS covering this area where is the mobile. BTS's routinely broadcasts (transmits) frequencies to enable the mobile (MS (from capturing the strongest signal. This change in BTS does not happen like this, but the mobile MS)) it measures the signal strength and if it finds a better signal than it is, it sends the measurement to BTS and BTS in turn it sends it to the BSC which is monitored for BTS's and sees if this change in BTS can be converted or deliver the mobile to the new BTS, and this method is called Handover. But then the BTS 23 the new one does not follow the current BSC, it raises the matter to MSC to take the appropriate action, which is by calling the new BSC and the delivery of the new BTS mobile phone because the BSC cannot speak to another BSC, then the mobile is not BSC and not BTS, and this usually happens when we are in a mode of transportation, such as a car so we change both. In both cases the MS and MSC / MSC mobile phones work together to make deliveries handover smoothly, the network is reserving a channel in the new BTS to enable Handover delivery even if we were during a call. For the next call to us, meaning if someone wants to call you, it is necessary the network must know where the (MS) mobile phone is, and under which MSC, BSC, and any BTS you are the network can deliver the call, here we learn the importance of the HLR home record and the VLR record visitors [11].

C. A5 Algorithm

There are several applications for this algorithm and the most common are:

- A5/0 used by countries under United Nations sanctions, does not come with coding. A 5/1 is the most powerful version used in Western Europe and America.
- A5/2 is the weaker version used mainly in Asia. As with the A8 and A3, this algorithm was secretly developed but had some descriptions unofficial algorithms can be found in the internet [12].

The structure of the A5 is shown in the figure below:

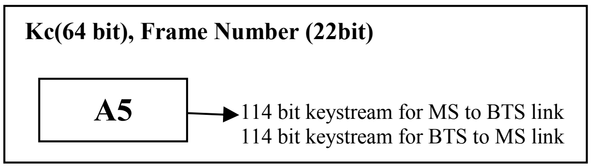

Kc(64 bit), Frame Number (22bit)
A5
114 bit keystream for MS to BTS link
114 bit keystream for BTS to MS link

Fig. 1. Architecture of A5 algorithm.

It is used in Europe and the United States. A5/2 was some of the weakest algorithm intentional exported regions. A5/1 developed in 1987, when the GSM was not taken into account for use outside Europe, the A5/2. It was established in 1989, both of which were initially classified. However, the overall design was leaked in 1994, and the algorithms were engineered in 1999 before Marc Briceno from GSM phone. In the year 2111, about 131 million GSM subscribers rely on A5/1 to protect the confidentiality of their voice communication.

Note: The first original algorithm was renamed to A5/1. Other algorithms include A5/0 which means that there is no encryption at all. Generally, the A5 algorithm after the A5/1 name has been changed to A5 / X. Most of the A5 / X algorithms are much weaker than. A5/1, A5 / 3 available in teamwork for wireless connections.

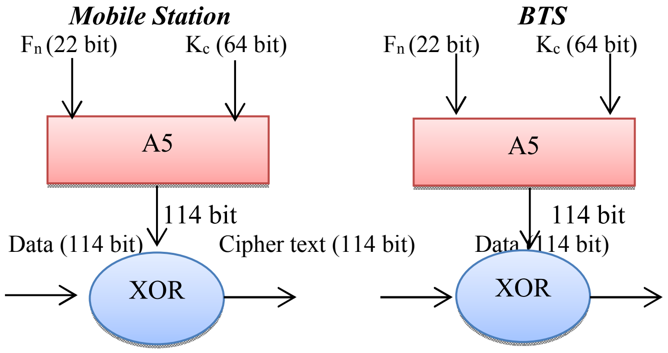


Fig. 2. Encryption method.

D. RC4 Algorithm

The RC4 algorithm was designed by Ron Revest, and is a common type of encryption algorithm (stream cypher) meaning you can generate the key for encryption during the communication process and encode it in the text in the same moment it is sent, RC4 uses a variable length key from 1 to 256 bytes to format a table the coding is about 256 bytes. In each session, each element in the coding table is replaced every time at least an element in each course, and these packets were used in many programs, the most famous of which is programming or kicking [13].

This packet works in two stages, the first stage is the main setup and the second stage is encoding, the main coding setup phase is the most difficult stage in which the cipher key variable is generated using the two status attributes, the key and once the encryption key is produced, it will proceed to the second stage, which is the stage of entering the encryption key on the text to create an encrypted message where the content of the messages is converted to dual format (0,1) each bit of the message is compared to the encryption key using the logical gate XOR. The number of comparisons will be based on the number of rounds used to produce the second encoded text, in case decoding gets the opposite.

The secret key is created, which is like a password in the simplest sense, and this is used to generate it coding table A coding table is used to generate 256-bit random text that may be used for encoding original text and last This random text is compared to the original text using the logical portal XOR This process is repeated according to the number of rounds required, and the more the number of rounds, the more difficult it becomes. Access to the secret key, and the length of the generated key can be variable.

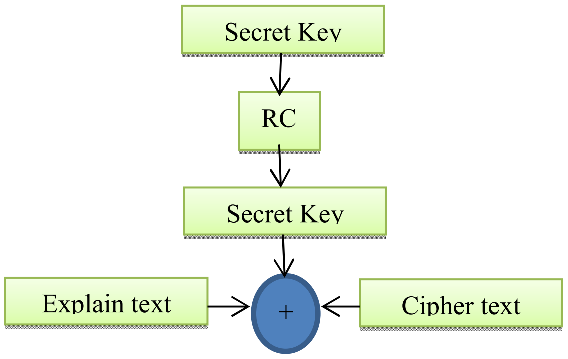


Fig. 3. RC4 encryption method.

Fig. 3, It represents the RC4 algorithm method of encryption where every session process key is generated this key is used to generate another key with a length of 256 bits. This key is used for encryption the clear text is according to the following formula:

[K] → [Key stream] XOR plant text → encrypt text

The method of generating the session key is a key stream from the key entered by both ends of the connection it varies according to the desire to complicate obstetrics, but the standard method used.

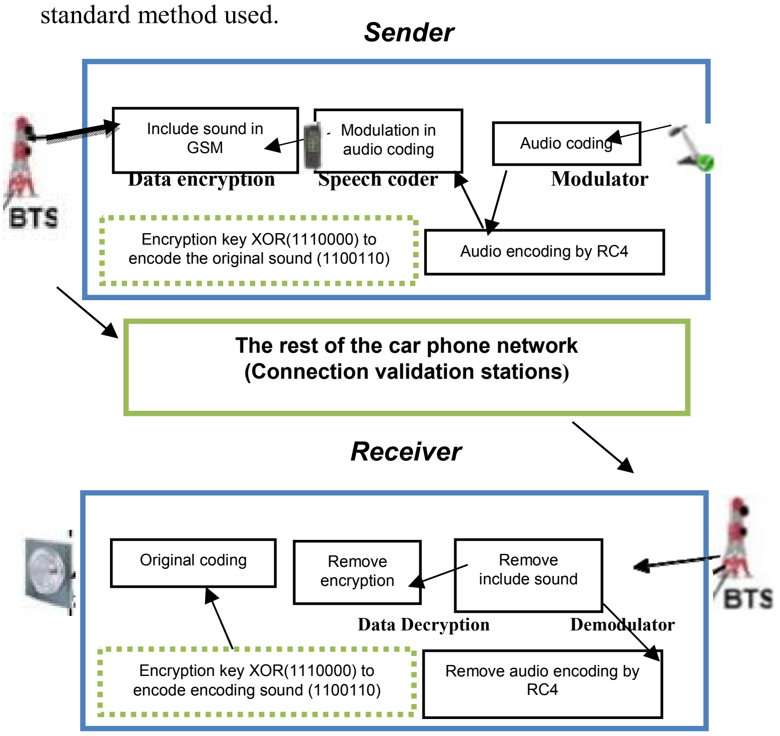

Sender
Include sound in GSM
Modulation in audio coding
Audio coding
Data encryption
Speech coder
Modulator
BTS
Encryption key XOR(1110000) to encode the original sound (1100110)
Audio encoding by RC4
The rest of the car phone network (Connection validation stations)
Receiver
Original coding
Remove encryption
Remove include sound
BTS
Data Decryption
Demodulator
Encryption key XOR(1110000) to encode encoding sound (1100110)
Remove audio encoding by RC4

Fig. 4. Idea of research

In this research, the basic idea is where the sender records his voice message via the microphone after opening the communication channel between the sender and the receiver, and the sound is converted to dual signals (0 1). The binaries are cut on the mechanism of the mobile phone network and then the encryption key is mixed with, diodes transmitted according to the steps of the RC4 algorithm using the XOR valve, which produces diodes a new hub which results in coded diodes that are sent over the mobile phone network, and will be used the Matlab program in simulating the communication channel between the transmitter and receiver. The RC4 algorithm will be used to alter the binary signal according to the following steps using the Matlab program [14][15][16].

- ***First step:*** Converting a similar signal to a binary digital signal, and vice versa.
- ***Second step***: Modulating the second audio signal according to the generated encryption key and according to steps RC4 encryption algorithm.
- ***Third step*****:** to include sound in the communication channel between the sender and the receiver.
- **Step four:** Decode the sound in the communication channel between the transmitter and Receiver, after

step four is finished, the audio is decoded according to the encryption key used for the encoding.

IV. EXPERIMENTAL RESULTS

The simulated application model for transmission in mobile phone networks is designed using the Matlab program as an application tool used in this study from the analogy to the conversion stage digital, the stage of adding the RC4 algorithm to the input diodes, and the audio segmentation stage to 21 a second. The following figure represents the first stage of the transmission (sampling)

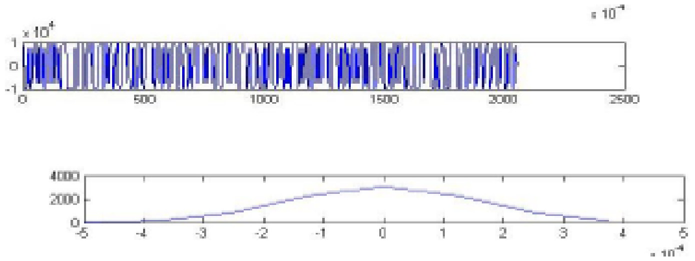


Fig. 5. The quantization stage illustrates the conversion from analog to digital

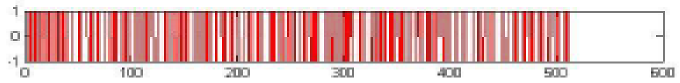


Fig. 6. Shows the RC4 coding stage after modulating the input diodes

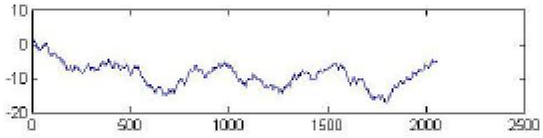


Fig. 7. Indicates inclusion of the signal

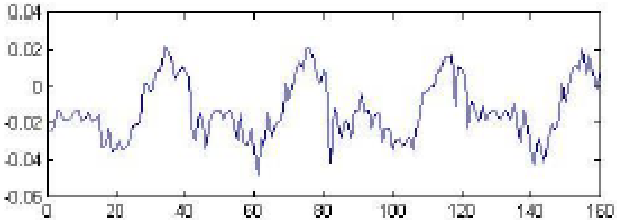


Fig. 8. Indicates the signal received from the transmitter

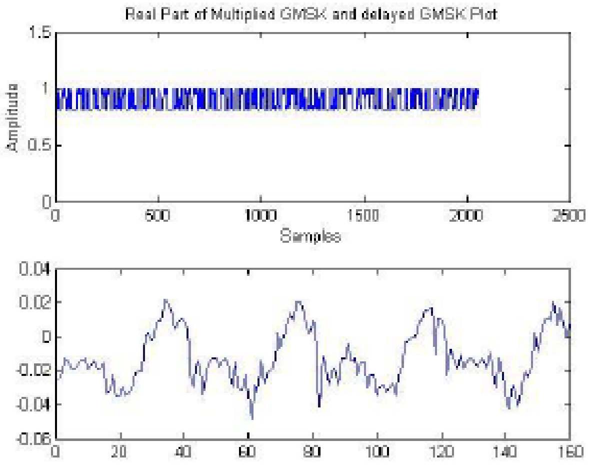
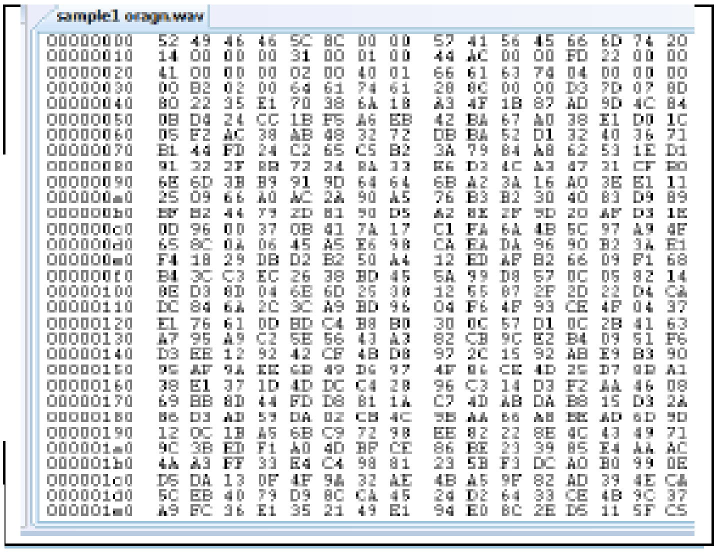


Fig. 9. Unclear explains the message.

TABLE 1. SHOWS THE VALUES OF THE TRANSMITTED SOUND

-0.0176	0.0105	0.0104	0.0109	-0.0129	0.0068	-0.0040
0.0062	-0.0008	0.0034	-0.0034	0.0005	0.0049	0.0048
-0.0301	-0.0174	-0.0186	-0.0092	-0.0032	0.0027	0.0092
				-0.0068	-0.0091	-0.0137

TABLE 2. DEMONSTRATES A SAMPLE OF THE PRE-SCROLL

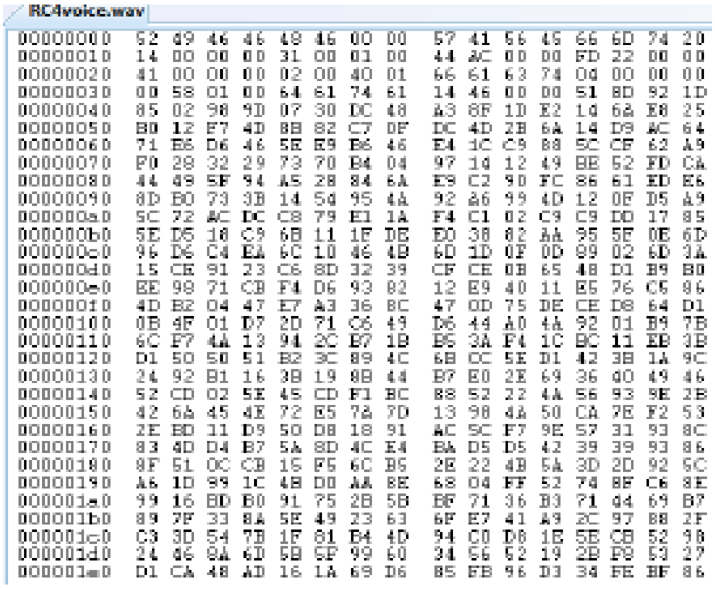


```
00000000  52 49 46 46 5C 8C 00 00  57 41 56 45 66 6D 74 20
00000010  14 00 00 00 31 00 01 00  44 AC 00 00 FD 22 00 00
00000020  41 00 00 00 02 00 40 01  66 61 63 74 04 00 00 00
00000030  00 B2 02 00 64 61 74 61  28 8C 00 00 D3 7D 07 8D
00000040  80 22 35 E1 70 38 6A 18  A3 4F 1B 87 AD 9D 4C 84
00000050  0B D4 24 CC 1B F5 A6 EB  42 BA 67 A0 38 E1 D0 1C
00000060  05 F2 AC 38 AB 48 32 72  DB BA 52 D1 32 40 36 71
00000070  B1 44 FD 24 C2 65 C5 B2  3A 79 84 A8 62 53 1E D1
00000080  91 32 2F 8B 72 24 8A 33  E6 D2 4C A3 47 31 CF 8D
00000090  6E 6D 3B B9 91 9D 64 64  6B A2 3A 16 A0 3E E1 11
000000a0  25 09 66 A0 AC 2A 90 A5  76 B3 B2 30 40 83 D9 89
000000b0  BF B2 44 79 2D 81 90 D5  A2 8E 2F 9D 20 AF D3 1E
000000c0  0D 96 00 37 0B 41 7A 17  C1 FA 6A 4B 5C 97 A9 4F
000000d0  65 8C 0A 06 45 A5 E6 98  CA EA DA 96 90 B2 3A E1
000000e0  F4 18 29 DB D2 B2 50 A4  12 ED AF B2 66 09 F1 68
000000f0  B4 3C C3 EC 26 38 BD 45  5A 99 D8 57 0C 05 82 14
00000100  8E D3 8D 04 6E 6D 25 38  12 65 87 2F 2D 22 D4 CA
00000110  DC 84 6A 2C 3C A9 BD 96  04 F6 4F 93 CE 4F 04 37
00000120  E1 76 61 0D BD C4 B8 B0  30 0C 57 D1 0C 2B 41 63
00000130  A7 95 A9 C2 5E 56 43 A3  82 CB 9C E2 B4 09 51 F6
00000140  D3 EE 12 92 42 CF 4B D8  97 2C 15 92 AB E9 B3 90
00000150  95 AF 9A EE 6D 49 D6 97  4F 86 CE 4D 25 D7 9D A1
00000160  38 E1 37 1D 4D DC C4 28  96 C3 14 D3 F2 AA 46 08
00000170  69 BB 8D 44 FD D8 81 1A  C7 4D AB DA B8 15 D3 2A
00000180  86 D3 AD 59 DA 02 CB 4C  5B AA 66 A8 BE AD 6D 9D
00000190  12 0C 1B A5 6B C9 72 98  EE 82 22 8E 4C 43 49 71
000001a0  9C 3B ED F1 A0 4D BF CE  86 BE 23 39 85 E4 AA AC
000001b0  4A A3 FF 33 E4 C4 98 81  23 5B F3 DC A0 B0 99 0E
000001c0  D5 DA 13 0F 4F 9A 32 AE  4B A5 9F 82 AD 39 4E CA
000001d0  5C EB 40 79 D9 8C CA 45  24 D2 64 33 CE 4B 9C 37
000001e0  A9 FC 36 E1 35 21 49 E1  94 E0 8C 2E D5 11 5F C5
```

TABLE 3. DEMONSTRATES A SAMPLE OF SOUND BEFORE ENCODING DIGITALLY

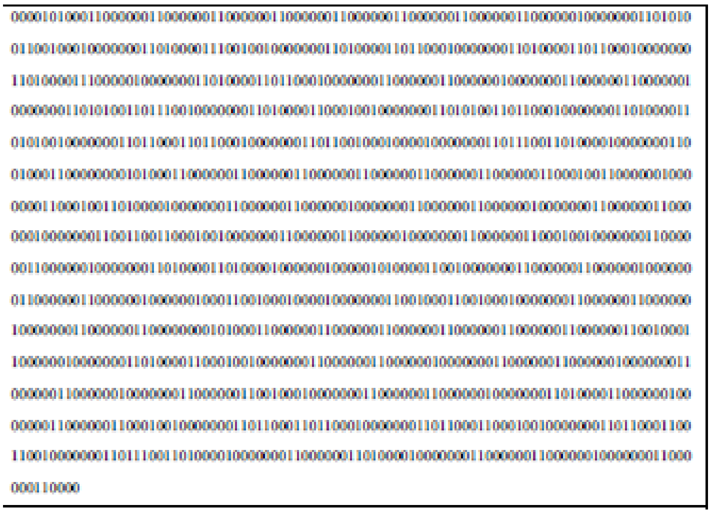
```
001100000011000000110000001100000011000000110000001100000011000000110000001

0000000110101001100100010000000110100001110010010000000110100001101

10000010100011000000110000001100000011000000110000001100000011100010

0110000001000000001100010011010000100000000110000001100000010000000011

00000011000000000101000110000001100000011000000110000001100000011000

00011001000110000001000000011010000110001001000000001100000011000000

100000001100000011000000000101000110000001100000011000000110000000110

0000011000000110011001100000010000000110000001100000010000001000010

0011001000100000000110000001100100000101000110000001100000011000000110000001

100000011000000110000001101000011000000100000000111000001100000001000

0000110010001100100010000000110011001101010000101000110000001100000

011000000011000000110000001100000011010100110000000100000
```

TABLE 4. CLEAR SOUND AFTER SCROLLING TO RC4



```
00000000  52 49 46 46 48 46 00 00  57 41 56 45 66 6D 74 20
00000010  14 00 00 00 31 00 01 00  44 AC 00 00 FD 22 00 00
00000020  41 00 00 00 02 00 40 01  66 61 63 74 04 00 00 00
00000030  00 58 01 00 64 61 74 61  14 46 00 00 51 8D 92 1D
00000040  85 02 98 9D 07 30 DC 48  A3 8F 1D E2 14 6A E8 25
00000050  B0 12 F7 4D 8B 82 C7 DF  DC 4D 2B 6A 14 D9 AC 64
00000060  71 E6 D6 46 5E E9 B6 46  E4 1C C9 88 5C CF 62 A9
00000070  F0 28 32 29 73 70 B4 04  97 14 12 49 BE 52 FD CA
00000080  44 49 5F 94 A5 28 84 6A  E9 C2 90 FC 86 61 ED E6
00000090  8D B0 73 3B 14 54 95 4A  92 A6 99 4D 12 0E D5 A9
000000a0  5C 72 AC DC C8 79 E1 1A  F4 C1 02 C9 C9 DD 17 85
000000b0  5E D5 18 C9 6B 11 1F DE  E0 38 82 AA 95 5E 0E 6D
000000c0  96 D6 C4 EA 6C 10 46 4B  6D 1D 0F 0D 89 02 6D 3A
000000d0  15 CE 91 23 C6 8D 32 39  CF CE 0B 65 48 D1 B9 B0
000000e0  EE 98 71 CB F4 D6 93 82  12 E9 40 11 E5 76 C5 86
000000f0  4D B2 04 47 E7 A3 36 BC  47 0D 75 DE CE D8 64 D1
00000100  0B 4F 01 D7 2D 71 C6 49  D6 44 A0 4A 92 01 B9 7B
00000110  6C F7 4A 13 94 2C B7 1B  B5 3A F4 1C BC 11 EB 3B
00000120  D1 50 50 51 B2 3C 89 4C  6B CC 5E D1 42 3B 1A 9C
00000130  24 92 B1 16 3B 19 8B 44  B7 E0 2E 69 36 40 49 46
00000140  52 CD 02 5E 45 CD F1 BC  88 52 22 4A 56 93 9E 2B
00000150  42 6A 45 4E 72 E5 7A 7D  13 98 4A 50 CA 7E F2 53
00000160  2E BD 11 D9 50 D8 18 91  AC 5C F7 9E 57 31 93 8C
00000170  83 4D D4 B7 5A 8D 4C E4  BA D5 D5 42 39 39 93 86
00000180  8F 51 0C CB 15 F5 6C B5  2E 22 4B 5A 3D 2D 92 5C
00000190  A6 1D 99 1C 4B D0 AA 8E  68 04 FF 52 74 8F C6 8E
000001a0  99 16 BD B0 91 75 2B 5B  BF 71 36 B3 71 44 69 B7
000001b0  89 7F 33 8A 5E 49 23 63  6F E7 41 A9 2C 97 88 2F
000001c0  C3 3D 54 7B 1F 81 B4 4D  94 C0 D8 1E 5E CB 52 98
000001d0  24 46 8A 6D 5B 5F 99 60  34 56 52 19 2B F8 53 27
000001e0  D1 CA 48 AD 16 1A 69 D6  85 FB 96 D3 34 FE BF 86
```

TABLE 5. DEMONSTRATES A SAMPLE OF SOUND AFTER SCROLLING TO THE RC4 ALGORITHM



```
00001010001100000011000000110000001100000011000000110000001100000011000000110000001000000001101010
01100100010000000110100001110010010000000110100001101100010000000110100001101100010000000
11010000111000000100000001101000011011000100000000110000001100000011000000010000000110000001100000001
00000001101010011011100100000001101000011000100100000001101010011011000100000001101000011
0101001000000011011000110110001000000011011001000100010000000110111001101000010000000110
01000110000000101000110000001100000011000000110000001100000011000000110000001100010011000000100
00001100010011010000100000001100000011000000100000001100000011000000110000001000000011000000110000001000
00010000000110011001100010010000000110000001100000010000000110000001100010010000000110000
00110000001000000110100001101000010000000100000101000011001000000011000000110000001000000
01100000011000000100000010001100100010000100000001100100011001000100000001100000011000000
10000000110000001100000000101000110000001100000011000000110000001100000011000000110010001
1000000100000001101000011000100100000001100000011000000100000001100000011000000100000011
000000110000001000000110000001100100010000000110000001100000010000000101000011000000100
0000001100000011000100100000001011000110110001000000011011000110001001000000010110001100
11001000000110111001101000010000000110000001101000010000000110000001100000010000000011000
000110000
```

Through this study, the researcher reached the following results:

- The ability to use the RC4 algorithm with the A5 algorithm to encode audio in telephone networks the car and through its use, we can guarantee the car phone user more security, especially that by using these packages we can deviate from the standard and one of the most important goals the coding is a departure from the usual thing without any increase in the size of the transmitted bits.
- Also it can be allowed for the user to control the encryption keys by himself, so as to ensure more it is reliable in the communication process, especially in the international calls that move between the medium wired and wireless.

The study made the following recommendations:

- Conducting several national studies in this field.
- Working to develop this type of algorithms (stream cypher).
- Create private departments in universities and higher institutes that are only interested in developing security algorithms to meet the steady need with the huge development in information and communication technology in Sudan.

REFERENCES

[1] T. Taraszow, E. Aristodemou, G. Shitta, Y. Laouris, and A. Arsoy, “Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example,” *Int. J. Media Cult. Polit.*, vol. 6, no. 1, pp. 81–101, 2010.

[2] E. Wheeler, *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier, 2011.

[3] A. M. Attia, N. Aziz, B. Friedman, and M. F. Elhusseiny, “Commentary: The impact of social networking tools on political change in Egypt’s ‘Revolution 2.0,’” *Electron. Commer. Res. Appl.*, vol. 10, no. 4, pp. 369–374, 2011.

[4] A. Biryukov, A. Shamir, and D. Wagner, “Real Time Cryptanalysis of A5/1 on a PC,” in *International Workshop on Fast Software Encryption*, 2000, pp. 1–18.

[5] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, “Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAS,” in *22nd International conference on field programmable logic and applications (FPL)*, 2012, pp. 747–753.

[6] N. H. A. A. Ali, “Voice Enery Ption in GSM Network Using RC4 Algorithm.” Sudan University of Science & Technology, 2015.

[7] K. Merit and A. Ouamri, “Securing speech in GSM networks using DES with Random Permutation and Inversion Algorithm,” *arXiv Prepr. arXiv1208.2169*, 2012.

[8] Z. K. Taha *et al.*, “Robust and Secured Image Steganography using Improved LSB and RC4 Cryptography with Preprocessing Operation.”

[9] M. E. Smid and D. K. Branstad, “Data encryption standard: past and future,” *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, 1988.

[10] A. F. Molisch, *Wireless communications*, vol. 34. John Wiley & Sons, 2012.

[11] M. Arner, J. Rodley, and W. W. Graylin, “System and method for developing rich internet applications for remote computing devices.” Google Patents, 25-Dec-2012.

[12] N. Stern, “The economics of development: a survey,” *Econ. J.*, vol. 99, no. 397, pp. 597–685, 1989.

[13] M. k Hussien, “Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES),” *Al-Mustansiriyah J. Sci.*, vol. 28, no. 2, pp. 156–161, 2018.

[14] A. A. Alhijaj and M. K. Hussein, “Stereo Images Encryption by OSA & RSA Algorithms,” in *Journal of Physics: Conference Series*, 2019, vol. 1279, no. 1, p. 12045.

[15] M. K. Haussein, “The optimum encryption method for image compressed by AES,” *GSJ*, vol. 8, no. 4, 2020.

[16] M. K. Hussien, “Encryption of Stereo Images after Estimated the Motion Using Spatially Dependent Algorithms,” 2016.