*Article*

GSM Encryption

Ardit Abazi 1, Donart Pllashniku 1,\* and Qlirim Hoti 1

1 Master- Faculty of Electrical and Computer Engineering,UP (University of Pristina),Bregu i Diellit, 10000 Prishtinë, Kosovo; ardit.abazi@student.uni-pr.edu, donart.pllashniku1@student.uni-pr.edu, qlirim.hoti1@student.uni-pr.edu

**\*** Correspondence: donart.pllashniku1@student.uni-pr.edu; Tel.: +38345900012

Received: 19.12.2020; Accepted: 10.01.2021; Published: xx.xx.2021

**Abstract:** One of the most used cellular standards in the world is GSM. GSM stands for either "group special mobile" or "general system for mobile communications," a protocol or standard for digital cellular communications. The European Conference of Post and Telecommunications Administrations in 1982, adopted the GSM standard, which in 1987 over 18 nations formalized with the signing of the GSM Memorandum of Understanding [1]. When the media are shared, anyone can listen or transmit also on the media, this means that this type of communication is no longer private. When anyone can see the media that is shared, privacy and authentication are lost. Cryptography provides some method to regain it. GSM encryption is the means by which phone conversations on networks using GSM are scrambled, such that they cannot be descrambled and intercepted by others. Vital to this security is the use of sophisticated encryption algorithms. The A5/x are the encryption algorithms used in order to ensure privacy of conversations on GSM and the most used is the strong version of it the A5/1[2].

**Keywords:** GSM, Encryption, Cryptography, Security, A5/x

1. Introduction

The name GSM first came from a group that was called “Group Special Mobile”, and then became the short term for “Global System for Mobile communication” which was formed in 1982

for European countries. Security has become a crucial topic in current mobile and wireless

networks, and the security procedures for such networks elevates as well as the techniques

used to attack the wirless networks [3]. The first GSM networks began operations in 1991. By the end of the 1990s, some 230 million users worldwide—approximately 65% of the digital wireless market—used digital GSM phones made by companies that included Motorola, Ericsson, and Siemens. The GSM Association estimated in 2011 that technologies defined in the GSM standard served 80% of the mobile market, encompassing more than 5 billion people across more than 212 countries and territories, making GSM the most ubiquitous of the many standards for cellular networks [4]. The wireless-radio medium is open to all .Being a wireless network, GSM is also sensitive to unauthorized use of resources. GSM offers precise security measures some of which maintains privacy and confidentiality of users’ identity and data while others ensure that only registered users access the network.

Some Key features of GSM are:

1. International Roaming
2. High level of security
3. Superior speech quality
4. Digital Convenience
5. Digital Compatibility
6. New services

Some security functions of GSM are:

* Authentication of the registered subscribers only
* Secure data transfer through the use of encryption
* Subscriber identity protection
* Duplicate SIMs are not allowed on the network

GSM is one of the most secured cellular telecommunications systems available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

Temporary identification numbers are assigned to the subscriber’s number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling [5].

The SIM provides the mobile phone with a unique identity through the use of the International Mobile Subscriber Identity (IMSI). The SIM is like a key, without which the mobile phone can’t function and it also is capable of storing personal phone numbers and short messages. It stores also security related information such as the A3 authentication algorithm, the authentication key (KI), IMSI and the A8 ciphering key generating algorithm. The mobile station stores the A5 ciphering algorithm[6].

The SIM is removable, it can be protected with a Personal Identification Number (PIN) chosen by the subscriber. The PIN is stored on the card and if entered incorrectly thrice, the card blocks itself which means you’ll have to contact your cellular provider who can unblocked your mobile phone, by entering an eight digit Personal Unblocking Key (PUK), which is also stored on the card.

2. GSM - Overview

The GSM Memorandum of Understanding in 1987 was perhaps the most important document in mobile phone history. It was the decisive means to secure not only the investment in GSM networks, but to create in fact an entirely new industry almost overnight and there is only one original copy of the GSM Memorandum of Understanding which is held at the HQ of the GSMA. The investment were in every European country on a big scale, scope and time-scale to shock an entire industrial eco-system and finally in 1991 the first GSM networks were ready [7]. GSM (Global System for Mobile communication) 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 code-division multiple access (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 megahertz (MHz) or 1,800 MHz frequency band.

The GSM network has four separate parts (Figure 1) that work together to function as a whole: the mobile device itself, the base station subsystem (BSS), the network switching subsystem (NSS) and the operation and support subsystem (OSS).

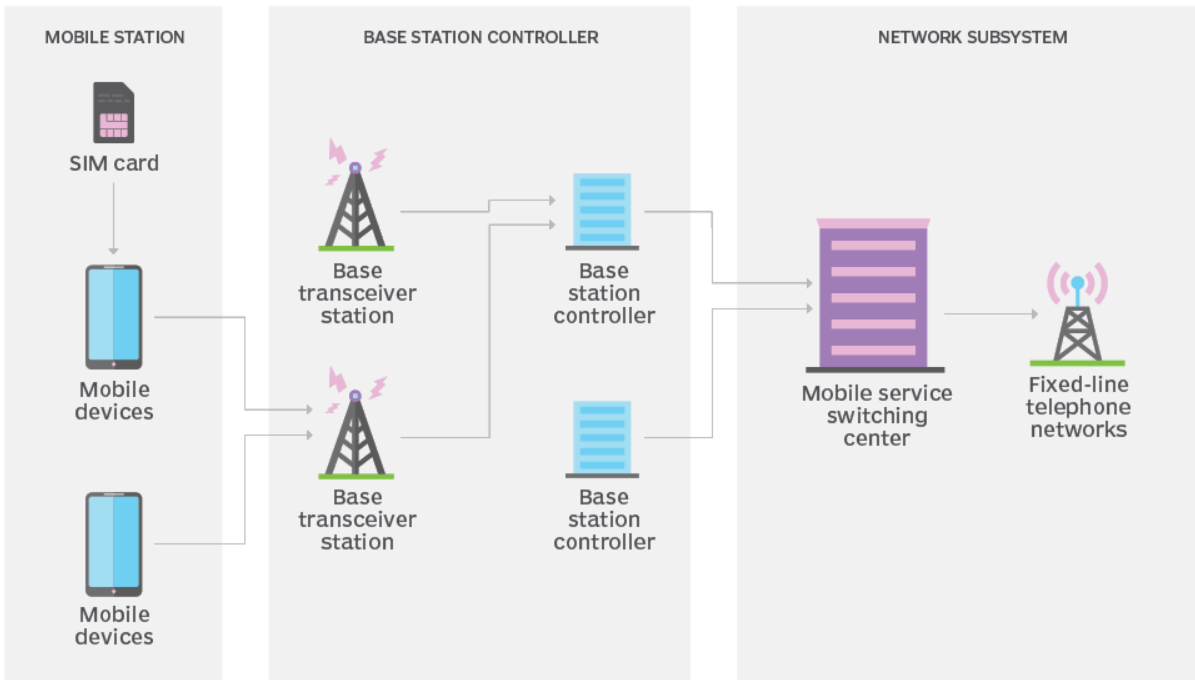


Figure . Global System for Mobile (GSM) Network [8]

The SIM (Subscriber Identity Module) card provides the network with identifying information about the mobile user, after it the base station subsystem handles traffic between the network switching subsystem and the cell phone. There are two main components: the base transceiver station (BTS) and the base station controller (BSC) where the BTS contains the equipment that communicates with the mobile phones, largely the radio transmitter receivers and antennas and the BSC is the intelligence behind it. The BSC communicates with and controls a group of base transceiver stations [9].

The network switching subsystem or also often called the core network tracks the location of callers to enable the delivery of cellular services. The network switching subsystem has a variety of parts, including home location register and mobile switching center. These components perform different functions, some of them are: Authentication, Sorting Caller Accounts information via SIM cards, Routing calls and Short Message Service (SMS).

The OSS (Operation Support System) is responsible for organization and maintenance. Multiple access uses a combination of FDMA (Frequency Division Multiple Access) (with optional frequency hopping) and TDMA (Time Division Multiple Access). FDD (Frequency Division Duplexing) is used for duplexing. The time axis is divided into timeslots, which are grouped into frames, multiframes, and superframes. A combination of frequency band and timeslot index is a physical channel. GSM uses GMSK modulation. Equalization is helped by a training sequence (midamble) in each timeslot. Coding employs unequal error protection, based on convolutional and/or block codes codes for bits created by the speech coder (regular pulse excited – long term prediction RPE-LTE). Interleaving over multiple slots is used. Data transmission in GSM includes circuit-switched transmission for low data rates, e.g., in Short Message Service (SMS) and packet-switched (e.g., General Packet Radio Service GPRS) [10].

Among the digital communication systems, the security process is very easy to be realized for GSM. In GSM systems, the security processes consists of four parts: authentication, encryption, TMSI reallocation, and equipment identification. However, there are some possible vulnerability issues which are a concern among many researchers. Most of them are the weakness in the basic algorithms used for authentication such as COMP128, and the algorithms used for encryption such as A5/1, A5/2. In the past, these algorithms were considered to be secure, but nowadays the advancement of technology has made these algorithms vulnerable to attacks. Recently, countermeasure against these vulnerabilities has been considered and under implementation [11].

A5/1, A5/2 and A5/3 are three stream ciphers that ensure that a user's conversation is private. However, the algorithms for both A5/1 and A5/2 have been broken and published and are therefore susceptible to plaintext attacks. GSM uses GPRS, a packet-based communication service, to transmit data, such as through web browsing. However, the ciphers that GPRS uses, GEA/1 and GEA/2, were broken and published as well in 2011. Researchers published open source software to sniff packets in the GPRS network.

3. GSM - Security and Encryption

As all cellular communications are sent over the air interface, it is less secure than a wired

network, as it opens the door to eavesdroppers with appropriate receivers.

Recently in the last years, the mobile industry has experienced an extreme increment in number of its users. The GSM network with the greatest worldwide number of users succumbs to several security vulnerabilities. Although some of its security problems are addressed in its upper generations, there are still many operators using 2G systems.

The cellular system GSM-2G provides several security functions such as: authentication and anonymity of the subscriber and data confidentiality. However, the most important and well-known shortcoming of GSM security is that, it does not provide a means for subscribers to authenticate the network and this oversight allows for false base station attacks or IMSI catcher attack [12]. The security methods standardized for the GSM System made it the basic standard for the recent generations e.g. 3G-CDMA and 4G-LTE.

Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to-end security. The subscriber’s anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling. Particularly in comparison to the previous analog systems, and hence part of the enhanced security of GSM is due to the fact that it is a digital system utilizing a speech coding algorithm, Gaussian Minimum Shift Keying (GMSK) digital modulation, slow frequency hopping (FH), and Time Division Multiple Access (TDMA) time slot architecture. However, to intercept and reconstruct this signal would require more highly specialized and expensive equipment to perform the reception, synchronization, and decoding of the signal. Nonetheless, there have been many attacks on the GSM system in the last few years [13].

Man-in-the-middle is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signalling and user data messages exchanged between the two parties by modified BTS in conjunction with a modified MS. Therefore, the above reasons make the GSM system needs hard work to balance the communication parameters (bandwidth, data rate, communication overhead, etc.,) with a high security scheme [14, 15][16].

The GSM network has some transport channels: Short Message Service (SMS), Unstructured Supplementary Service Data (USSD), Wireless Application Protocol (WAP), and the voice channel. There are also some newer services such as Enhanced Messaging Service (EMS) and Multimedia Messaging Service (MMS) that have been added in the GSM upgrades. The security flaws described in the previous section are commonly applicable to all the services and transport channels since they aim all the exchanged data and signaling information. However, in addition to such common flaws, some of GSM transport channels have some extra problems and vulnerabilities. The SMS messaging has some extra security vulnerabilities due to its store-and-forward attribute, and the problem of fake SMS that can be conducted via the Internet. When a user is roaming, the SMS content passes through different networks and perhaps the Internet that exposes it to various vulnerabilities and attacks. Another concern is arisen when an adversary gets access to the phone and reads the previous unprotected messages. The USSD that is a session-oriented technology is also vulnerable to attacks since the messages are not encrypted and secured on the GSM backbone. The WAP allows ME to connect to the Internet. The WAP Gateway that resides between MS and Web server in the WAP architecture and acts as an interpreter between the Internet protocols (HTTP, SSL/TLS, and UDP/TCP/IP) and the corresponding WAP protocols (WSP/WTP, WTLS, and WDP), introduces an additional security flaw in some implementations that is referred to as the WAP gap. Other concerns are arisen from security problems of the Internet as a huge uncontrolled network that is in contradiction with assumptions of the GSM security architecture in which the core network is assumed as a secure and controlled environment. The web servers may also download and execute malicious applets at the client (ME) so the safety of applets and other downloaded programs is another concern [25].

**Authentication**

Authentication in the GSM system is achieved by the Base Station sending out a challenge to the mobile station. The Mobile Station uses a key stored on its SIM to send back a response that is then verified. This only authenticates the Mobile Station, not the user. Authentication process is shown in figure 2.

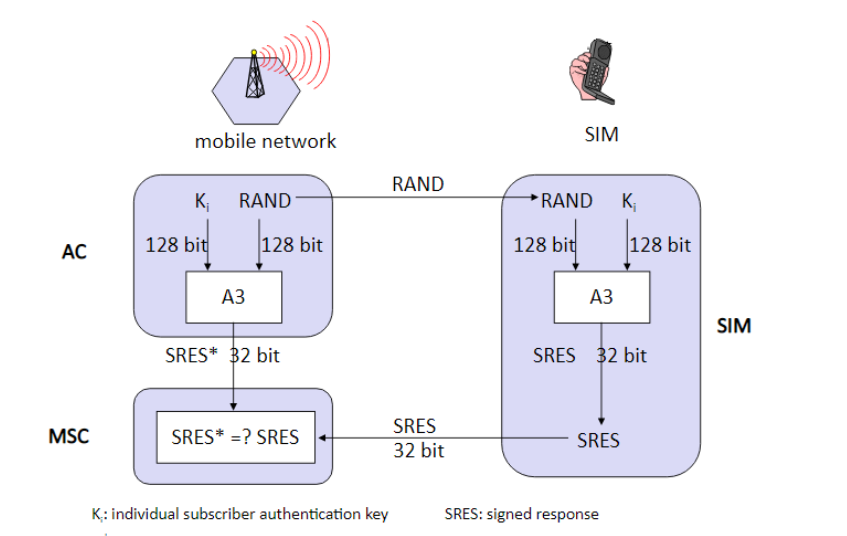


Figure Authentication process in GSM [17]

Steps for a call:

* A unique subscriber authentication key is programmed on every SIM card. The authentication center has a list which maps Ki number with the SIM card. It is a secure database.
* When a SIM card requests for a call, a 128bit random number is instantaneously generated by the authentication center and transmitted to the SIM card.
* The A3 algorithm which is programmed inside the SIM card processes the RAND number and Ki number and generates a 32bit output called the Signed response number (SRES).
* The same process is done on the authentication center side.
* The SIM card transmits this SRES number to the authentication center.
* The authentication center compares the received SRES with the SRES that’s generated on the network side.
* The SIM is authenticated if and only if the two SRES are same.

The authentication center contains a database of identification and authentication information for subscribers including IMSI, TMSI, location area identity (LAI), and authentication key (Ki). It is responsible for generating (RAND), response (RES), and ciphering key (Kc) which are stored in HLR / VLR for authentication and encryption processes. The distribution of security credentials and encryption algorithms provides additional security [18].

Firstly, a 128bit random number is transmitted to the mobile station over the air interface. The random number is passed to the SIM card, where it is sent through the A3 authentication algorithm together with the KI. The output of the A3 algorithm, the signed response is transmitted via the air interface from the mobile station back to the network. On the network, the authentication center compares its value of signed response with the value of signed response it has received from the mobile station.

If the two values of signed response match, authentication is successful and the subscriber joins the

network. The authentication center actually doesn’t store a copy of signed response but queries the HLR or the VLR for it, as needed.

**Anonymity**

When a new user turns on his phone for the first time, its IMSI is transmitted to the Authentication Center on the network. After which, a Temporary Mobile Subscriber Identity is assigned to the subscriber. The IMSI is rarely transmitted after this point that’s what prevents a potential eavesdropper from identifying a GSM user by their IMSI. The user continues to use the same Temporary Mobile Subscriber Identity, depending on the how often location updates are done. Every time a location update is done the network assigns a new Temporary Mobile Subscriber Identity to the mobile phone. The Temporary Mobile Subscriber Identity is stored along with the IMSI in the network. The mobile station uses the Temporary Mobile Subscriber Identity to report to the network or during call initiation and also to communicate with the mobile station. The Visitor Location Register performs the assignment, the administration and the update of the Temporary Mobile Subscriber Identity. When it is switched off, the mobile station stores the Temporary Mobile Subscriber Identity on the SIM card to make sure it is available when it is switched on again. The anonymity in the GSM is provided by replacing the use of IMSI with a 32-bit Temporarily Mobile Subscriber Identity (TMSI). TMSI is typically handled by the VLR, is valid in a particular Location Area (LA), and will be updated at least in every location update procedure. It is also stored on the subscriber's SIM and prevents an eavesdropper to track a particular subscriber [25].

**Encryption and Decryption of Data**

GSM makes use of a ciphering key to protect both user data and signaling on the vulnerable air interface. Once the user is authenticated, the random numbers (delivered from the network) together with the KI (from the SIM) is sent through the A8 ciphering key generating algorithm, to produce a ciphering key. The A8 algorithm is stored on the SIM card. The ciphering key created by the A8 algorithm, is then used with the A5 ciphering algorithm to encipher or decipher the data. The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data on the fly. Therefore mechanisms for encryption need to be performed both at base station and mobile station. The algorithms A5 and A8 are used for encryption (Figure 3).Any encryption algorithm needs a cipher key. This cipher key is not statically available. It is dynamically generated using A8 algorithm. It takes 128 bit key Ki and 128 bit RAND to generate 54 bit cipher key. Then 10 zero bits are appended to the key to make it 64 bit. This is done to reduce the key space from 64 bits to 54 bits.

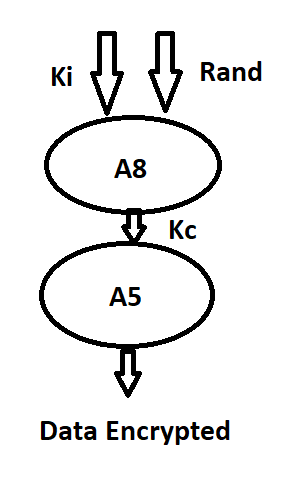


Figure Encryption data using cyphering key

**GSM Encryption Algorithms**

In roaming the exchange of information between providers in different countries must be done. All countries have strict regulations against the export of encryption algorithms and thus GSM works around it. When a user tries to use his phone in another country, the local networks request the Home Location Register of the users home network for the random numbers, Signed Response and Cipher key which is sufficient for authentication and encrypting data. Thus the local network does not need to know anything about the A3 or A8 algorithms stored in the SIM.

GSM uses three different security algorithms called A3, A5, and A8. In practice, A3 and A8 are generally implemented together (known as A3/A8).

Algorithm A3 is used for authentication, A5 is used for encryption, and A8 is used for the generation of a cipher key.

An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4). Development of A3 and A8 algorithms is considered a matter for individual GSM network operators, although example implementations are available.

An A5 encryption algorithm scrambles the user’s voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem.

**Authentication Algorithm A3**

The A3 algorithm is used to authenticate each mobile by verifying the user password within the SIM with the cryptographic key at the Mobile Services Switching Center.

Before a subscriber can use any service provided by the GSM network, the user must be authenticated. This authentication is based on the Subscriber Identity Module, which stores the authentication key Ki, the user identification International Mobile Subscriber Identity, and the algorithm used for this authentication i.e. A3.

The mobile station signs into the network. The access control generates a random number as challenge, and the SIM within the MS answers with the Signed Response as the response. The Authentication Centre generates the random values of random number, the signal response Signed Response and the cipher key. This information is forwarded to the Home Location Register). The Visitor Location Register requests the values of random number, Signed Response and cipher key from the Home Location Register.

The Visitor Location Register sends the random number value generated to the SIM. On both sides, the network and the subscriber module, same operation is performed between the 128 bit random number and 128 bit Ki , called A3. SRES of 32 bit is generated on both the sides. MS sends the SRES generated by the SIM to the Visitor Location Register . Now Visitor Location Register can compare both the Signed Response generated. If both are same, the user or the subscriber is authenticated, otherwise rejected[21].

The A3 algorithm is operator-dependent and is an operator option. The A3 algorithm is a one-way function, which means it is easy to compute the output parameter signed response by using the A3 algorithm but very complex to retrieve the input parameters random numbers and KI from the output parameter. Remember the key to GSM’s security is keeping KI unknown. A3 algorithm is a validation process used in a GSM network for authentication of the mobile user that is requesting service. The A3 algorithm is a mathematical process that combines a secret number (called Ki in documents) stored in the SIM chip and a second number that is transferred between the base station and the mobile station. The numerical result of the A3 algorithm calculation is transmitted back to the base station. It is then compared to a previously internally calculated answer also using the A3 algorithm and the same two input quantities, in the base station controller or in the MSC. When the same matching result occurs for both the mobile supplied information and previously stored information, the customer has granted access[27].

**Ciphering Algorithm A5**

The A5 ciphering algorithm is used for encryption. It provides scrambling for 114 coded bits sent in each TS. The A8 is used for ciphering key.

The most commonly used ones of this algorithm are A5/0, A5/1(Algorithm used in the GSM ciphering process between a MS (Mobile Station) and the GSM network) and A5/2(Encryption Algorithm A5/2 Algorithm used in the GSM ciphering process between a MS (Mobile Station) and the GSM network. This algorithm is simpler than A5/1 and was developed by ETSI (European Telecommunications Standards Institute) for use in Eastern European states that had restrictions to certain Western technologies.). The reason for the different implementations is due to export restrictions of encryption technologies. A5/1 is the strongest version and is used widely in Western Europe and America, while the A5/2 is commonly used in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption [19].

A5 is a family of symmetric stream ciphers most famously used as the encryption schemes in GSM 1 and succeeding technologies. The A5 algorithms are designed for simple commodity hardware with focus on security and speed. The short key length used in A5, along with other vulnerabilities, makes GSM prone to attacks. The architecture and implementation of the algorithms are also flawed and can be abused from not only governments, but adversaries without extensive computational power. The decryption can be done in close to real time. This paper will present the encryption scheme used in the 2G GSM network, the A5/1 algorithm, as well as some of the associated vulnerabilities.

The algorithm takes 228 bits of plain text as input and outputs 228 bits of cipher text. Each block of 228 bits is called a ”frame”, where the first 114 bits represents data sent from unit A to unit B, and the last 114 bits are data received by unit A from unit B. Each frame has a duration of 4.615 ms, allowing 2ˆ8 frames to be sent every second.

Over time, several A5-versions have been developed, but they all share the same main idea. An A5 algorithm takes the session key Kc (symmetric) and a frame counter Fn, and generates 228 pseudo random bits (PRAND), called a key stream. The key stream is then XORed with a 228 bit segment of plain text, yielding 228 bits of ciphertext.

The encryption itself is just a simple XOR operation for each bit. In A5, it is the generation of pseudo random bits (function GEN) that is important. The different A5-versions offer different levels of security by implement GEN differently.

A5/1 is the strongest and most popular of the GSM A5 versions and it is used in both Europe and in the US. A5/1’s pseudo random bits are generated by 3 linear feedback shift registers. An linear feedback shift registers is a shift register whose input is a linear function of its previous state. The register’s state is decided by several tap-bits, and the linear feedback function is an XOR of all the register’s tap bits [20].

**Ciphering Key Generating Algorithm A8**

This algorithm is used in conjunction with Ki, the authentication key, and Random Number to generate Cipher Key. This is used with A5/X to cipher the data stream between the Mobile Station and the GSM network.It is operator-dependent. In most providers the A3 and A8 algorithms are combined into a single hash function known as COMP128. The COMP128 creates ciphering key and signed response, in a single instance. There are three of them: COMP128-1, COMP128-2, COMP128-3.

COMP128-1 uses a compression function with eight rounds which is based on a butterfly structure with five stages. Signed response is filled with the first 32 bits of the output. Ciphering key is filled with the last 54 bits of the output followed by ten zeroes. The COMP128-1 hash function is considered weak because there is insufficient diffusion of small changes in the input. Practical attacks have been demonstrated that can recover the subscriber key from the SIM.

The implementation of COMP128-2 and COMP128-3 is noticeably more complex than COMP128-1. COMP128-2 is identical to COMP128-3 except for the fact that at the end, it clears the 10 rightmost bits of Ciphering Key.

The session keys produced by COMP128-1 and COMP128-2 intentionally have only 54 bits of entropy. This significantly weakens the A5 or A6 encryption.

A5/1 Algorithm

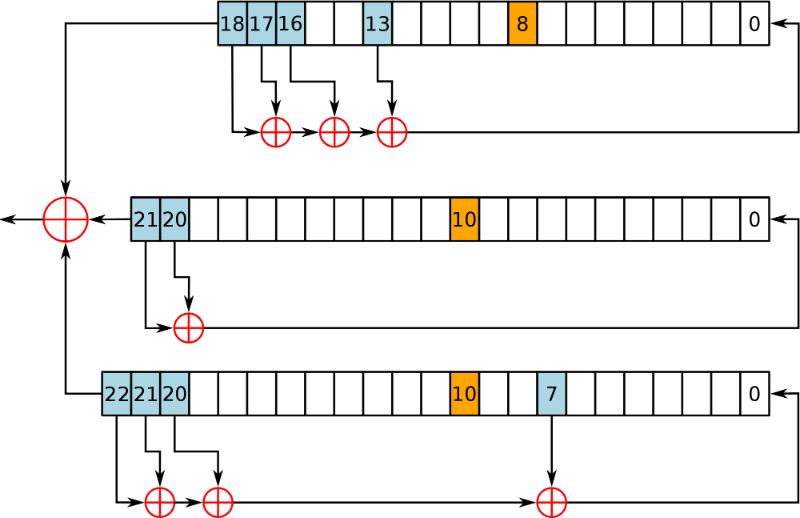
A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It is one of seven algorithms which were specified for GSM use[26]. A GSM transmission is organised as sequences of bursts. In a typical channel and in one direction, one burst is sent every 4.615 milliseconds and contains 114 bits available for information. A5/1 is used to produce for each burst a 114 bit sequence of keystream which is XORed with the 114 bits prior to modulation. A5/1 is initialised using a 64-bit key together with a publicly known 22-bit frame number. Older fielded GSM implementations using Comp128v1 for key generation, had 10 of the key bits fixed at zero, resulting in an effective key length of 54 bits. This weakness was rectified with the introduction of Comp128v3 which yields proper 64 bits keys. When operating in GPRS / EDGE mode, higher bandwidth radio modulation allows for larger 348 bits frames, and A5/3 is then used in a stream cipher mode to maintain confidentiality. A5/1 is based around a combination of three linear feedback shift registers (LFSRs) with irregular clocking. The bits are indexed with the least significant bit (LSB) as 0.

The registers are clocked in a stop/go fashion using a majority rule. Each register has an associated clocking bit. At each cycle, the clocking bit of all three registers is examined and the majority bit is determined. A register is clocked if the clocking bit agrees with the majority bit. Hence at each step at least two or three registers are clocked, and each register steps with probability 3/4. Initially, the registers are set to zero. Then for 64 cycles, the 64-bit secret key K is mixed in according to the following scheme: in cycle {\displaystyle 0\leq {i}<64}0\leq {i}<64, the ith key bit is added to the least significant bit of each register using XOR — R[0]=R[0] K[i]



Each register is then clocked.

Similarly, the 22-bits of the frame number are added in 22 cycles. Then the entire system is clocked using the normal majority clocking mechanism for 100 cycles, with the output discarded. After this is completed, the cipher is ready to produce two 114 bit sequences of output keystream, first 114 for downlink, last 114 for uplink [26]. While we all concentrate on the core IP network, and which has relatively good protection in the transmission over the air, it is the GSM/3G network that could be at risk. The mobile phone network typically uses the A5/1 or A5/2 stream encryption method, but almost on its first day or operation it has been a target for crackers, and the source code to crack A5/2 was released within one month of being made public. While blocked ciphers like AES are robust, the A5/1 stream cipher has been shown to be weak against certain types of attack [24]. There were two main choices for countries with their encryption: A5/1 and A5/2. A5/2 is intentionally weak, so that nation states can easy crack the cipher, but was cracked generally within a month of it being publicly released. A5/1 was meant to be stronger, but, as it has a relatively short key, it can be cracked with powerful computers. There were two main choices for countries with their encryption: A5/1 and A5/2. A5/2 is intentionally weak, so that nation state can easy crack the cipher. A5/1 was meant to be stronger, but it was quickly cracked once the method had been discovered. Currently there are billions of devices around the world using A5/1 for their security, and it is likely that they can be cracked by the NSA. With A5/1 we use three shift registers with feedback (Figure 4). With a stream cipher, we often generate an infinitely long key stream which is then EX-OR'ed with the data stream. In the first shift register the bits at positions 18, 17, 16 and 13 are X-OR'ed together to produce a new bit which is put at the end. This pushes all the bits to move one position to the left. The last bit (the one at Position 18) will then be pushed off and X-OR with the output from the other shift registers. The shift registers are 19, 22 and 23 bits long, thus the key used is 64-bits long (19+22+23). In the diagram the bits 8, 10 and 10 are highlighted, and are the clocking bits. These are examined each cycle. In these are will either be more 1's than 0's or more 0's than 1's. The registers with the most popular bit value will advance their bits, and the other will not advance.



Figure

The algorithm itself was help secret while it was installed in 100 million mobile phones, and was part of the GSM (Global System and Mobile Communications) standard, and has since become a standard with 3G (even though it is seen as weak). The US and Europe adopted the strong A5/1 algorithm, but many selected the weaker one. It was finally made public in August 1999, and within a month the A5/2 method had been cracked. For A5/1 it is thought that the NSA can crack it (as they have the computing power to crack 64-bit keys). The attack typically use known plaintext attacks, but new ones now allow the cipher stream to be decrypted in real-time. When first proposed, in 1982, it is thought that that the A5/1 key would be 128-bits long, but it finalised ended up with a 64-bit key (which can be cracked on expensive hardware using brute force). It is likely that government pressure forced the key to be much shorter. In fact it is thought that the UK wanted just 48 bits, while the West German government of the time pushed for larger key sizes (as they were worried that the East German government would be able to break their ciphers). A stream cipher allows for automatic synchronisation, and where each bit can be decoded as it is received [23].

A5/2 Algorithm

A5/2 algorithm is a kind of stream cipher based on line feedback shift registers. The secret key size of it is 64bit, and the IV size of it is specified to be 22bit frame number. As is shown in Figure 5, A5/2 algorithm is built from four LFSRs of lengths 19,22,23,17 bits denoted by R1, R2, R3 and R4 respectively. Each register is updated by its own primitive feedback polynomial as is shown in Ref. Clocking of R1, R2 and R3 is controlled by R4 which is regularly clocked in each clock cycle. Majority of the bits 3 R4 , 7 R4 and 10 R4 is calculated and a binary result according to majority rule is obtained. If the result is the same as 3 R4 , then R2 is clocked, if the result if the same as 7 R4 , then R3 is clocked and if the result is the same as 10 R4 , then R1 is clocked. After the clocking of R1, R2 and R3, R4 are clocked, the output bit is generated[28].

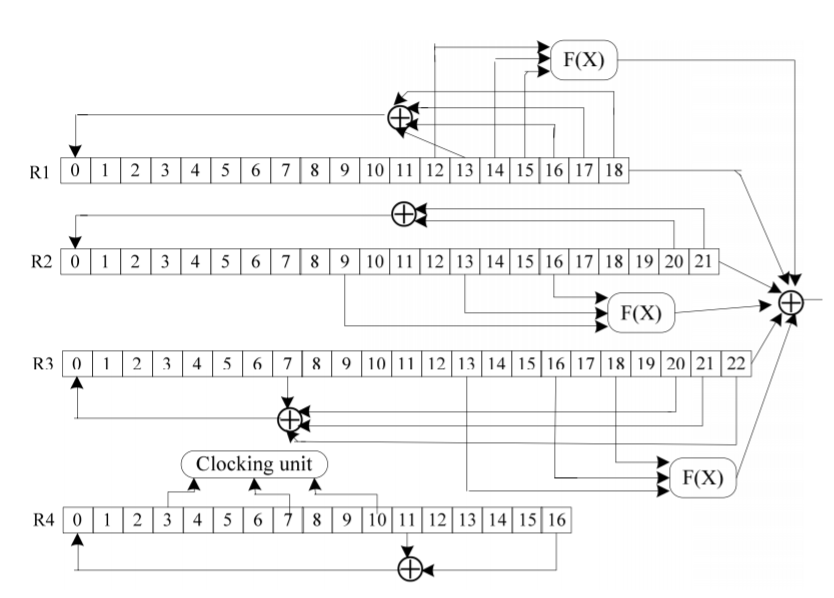


Figure 5

The process flow of A5/2 algorithm can be described as follows. The initialization of the registers loads the bits of secret key and the bits of the frame number, followed by setting 14 R1 , 15 R2 , 17 R3 and 9 R4 to “1”, then 100 output bits. After the initialization, 228 bits of output stream are computed. The former 114 bits are used to encrypt data from the center to the mobile phone, and the latter 114 bits are used to encrypt data from the mobile phone to the other center.

A5/3 Algorithm (KASUMI)

KASUMI is a block cipher used in UMTS, GSM, and GPRS mobile communications systems. In UMTS, KASUMI is used in the confidentiality (f8) and integrity algorithms (f9) with names UEA1 and UIA1, respectively. In GSM, KASUMI is used in the A5/3 key stream generator and in GPRS in the GEA3 key stream generator[29]. KASUMI algorithm is specified in a 3GPP technical specification. KASUMI is a block cipher with 128-bit key and 64-bit input and output[30]. The core of KASUMI is an eight-round Feistel network. The round functions in the main Feistel network are irreversible Feistel-like network transformations. In each round the round function uses a round key which consists of eight 16-bit sub keys derived from the original 128-bit key using a fixed key schedule.

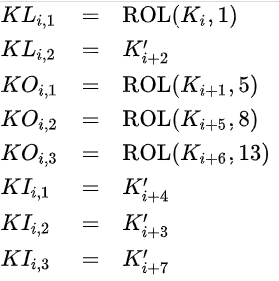
The 128-bit key *K* is divided into eight 16-bit sub keys *Ki*:



Additionally a modified key K', similarly divided into 16-bit sub keys K'i, is used. The modified key is derived from the original key by XORing with 0x123456789ABCDEFFEDCBA9876543210 (chosen as a "nothing up my sleeve" number).

Round keys are either derived from the sub keys by bitwise rotation to left by a given amount and from the modified sub keys (unchanged).

The round keys are as follows:



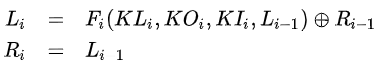
Sub key index additions are cyclic so that if i+j is greater than 8 one has to subtract 8 from the result to get the actual sub key index.

KASUMI algorithm processes the 64-bit word in two 32-bit halves, left (Li) and right (Ri)

The input word is concatenation of the left and right halves of the first round:



In each round the right half is XOR'ed with the output of the round function after which the halves are swapped:



where Kli, Koi, Kli are round keys for the ith round.

The round functions for even and odd rounds are slightly different. In each case the round function is a composition of two functions Fli and Foi. For an odd round



And for an even round



The output is the concatenation of the outputs of the last round.



Both FL and FO functions divide the 32-bit input data to two 16-bit halves. The FL function is an irreversible bit manipulation while the FO function is an irreversible three round Feistel-like network.

4. Discussion

GSM is a globally accepted standard for digital cellular communications.

GSM uses narrowband Time Division Multiple Access (TDMA) for providing voice and text based services over mobile phone networks.

To a large extent, GSM can be said to have been the right system at the right place at the right time. Based on the analysis of this paper, it appears that the essence of the GSM story revolves around the concept of cooperation, and the political and economic environment that facilitated it. A main theme throughout this paper is that investments in the respective IMT-2000 standards are extremely high, and that those sustaining these commitments consist of a number of highly leveraged stakeholders like manufacturers, distributors, and standards consortia – all keen to justify their own paths toward IMT-2000. While European Community policy and Commission leadership were indispensable for GSM, flexibility and adaptability on the national level were vital for success. This is one of the key differentiating factors between the developments of 2nd generation and 3rd generation technologies [22].

Ironically, what is in evidence today in the 3G market, is the growth of consolidation and collaboration between operators that has made 3G unique from GSM. At earlier stages of IMT-2000 development, such collaboration (i.e., in the form of network-sharing) was unthinkable, given the widely divergent stakes in differing types of 2G legacy investments/commitments, and the general emphasis on the necessity for full and free competition in the marketplace. Perhaps this phenomenon of consolidation is reflective of a natural tendency for ‘natural cooperation’ intrinsic to the success of the mobile sector (i.e., the same way that monopolistic tendencies are ‘natural’ for the ‘local-loop’), and that must inevitably emerge in some form as industry experience lead to it again and again. In this case, cooperation is perhaps being spurred by the workings of the spectrum market, despite the fact that the ability of political entities to bring it about was diminished.

In an environment characterized by very rapid change and unmatched dynamism, it is an interesting task to pick and choose those factors that can be drawn in parallel from the past, to explain what is to come in the future. Though the political roots of GSM have transformed significantly into more market-driven ones for IMT-2000, we have seen that certain trends, metrics, and concepts are still relevant, while others fade into the background. One can but hope that past experience – as from the GSM case - breeds the types of institutions and leaders that are willing to learn from their mistakes and improve even further upon their successes as they seek to serve a global market. Above all, the institutions that have shaped these generational transformations have been and continue to be vital for the future of IMT-2000. As a leader among them, the ITU continues to confirm its critical role, not only by helping to map out the evolutionary path toward 3G and recognizing inherent dilemmas in the process, but by serving as a repository for best practices/benchmarked information for IMT-2000, and by helping governments/ operators/regulators alike deal with the foremost concerns of harmonization of standards, roaming and circulation, and globalization.

5. Conclusions

The users and the service providers would never want their resources and services to be

used by unauthorized users. In this work, a technique to provide end-to-end encryption for the GSM system with a little handshaking procedures was demonstrated using Public Key Infrastructure approach PKI, similar to the A5 algorithm. GSM system has been used as a basis for the “next generation” of mobile communication technologies (3G and 4G) in the world. Certificate-less cryptography can be the most suitable scheme for the mobile communication security because its lightweight infrastructure, and it's lack of certificates, and CL-PKC is a promising solution improving several weaknesses of PKI and Identity-Based Cryptography IBC.

The GSM network was the first mobile cellular network with an aim to connect the world. The new requirements for over-air security were not fulfilled by the original 2G implementations. Short encryption keys, flaws in the A5 tap-structure, as well as one-way authentication are some of the vulnerabilities that GSM is faced with. Technologies based on GSM have fixed many of these issues, but there are still ways to downgrade the security preferences in many cases.

GSM being a wireless network is always prone to the unauthorized access to the network and entrustment to the privacy and confidentiality of the users. Therefore, the GSM provides security measures to ensure the privacy and confidentiality of the users to ensure that only registered and authorized users get the access to the network. GSM protection and the algorithms that are mainly used are A3, A5 and A8. Algorithm A3 is used for authentication, A5 is used for encryption, and A8 is used for the generation of a cipher key. The security of the GSM network is evaluated, and a complete and brief review of its security problems is presented. It is proved that the GSM network has many inherent security flaws that can be misused for fraudulent purposes or for deceiving users. Some practical solutions to improve the security of currently available 2G networks are also proposed. Some solutions include the security improvement of the infrastructure while the others tend to provide the end-to-end security. It is also deduced that the end-to-end security or the security at the application layer is the best and most profitable solution for the currently available 2G systems. Even with no encryption, GSM is more secure than analog system by using the speech coding, digital modulation and TDMA. GSM’s security methods (authentication, encryption, and temporary identification number) ensure the privacy and anonymity of the system users, as well as safeguarding against fraudulent use. My experience is that GSM security adds complexity to the system implement. And the current systems have different kinds of defect. With increasing 4G proliferation and 5G already being rolled out in some regions, network operators’ focus has been shifting away from GSM and UMTS networks for quite some time now to free up frequencies for the new technologies.

The move away from legacy technologies will undoubtedly be a significant transition for many IoT and M2M companies, because 2G and 3G connectivity is still the most used technologies for deployed devices. In some European countries it could be the case where 2G may even outlive 3G, UMTS. Norwegian MNO Telenor announced 3G switch-off in 2020 – five years before 2G. Vodafone has announced it is to phase-out 3G networks across Europe in 2020 and 2021 while Deutsche Telekom plans to continue 3G, UMTS until the end of 2020. However, there are no plans by either Vodafone, Deutsche Telekom or Telefonica for 2G switch off.

Table for Europe:

|  |  |  |  |
| --- | --- | --- | --- |
| Switch-Off Date | Network Operator | Country | Technology |
| 01.01.2021 | Swisscom | Lichtenstein | GSM |
| 31.12.2020 | T-Mobile | Netherlands | GSM |
| 31.12.2025 | Telenor | Norway | GSM |
| 31.12.2020 | Telenor | Norway | UMTS |
| 31.12.2021 | Telia | Norway | UMTS |
| 2020 | Telenor | Sweden | UMTS |
| 2025 | Tele2, Telia | Sweden | UMTS |
| End of 2021 End of 2024 | Sunrise | Switzerland | GSM900 UMTS\* |
| 31.12.2020 | Swisscom | Switzerland | GSM |

Table for North America:

|  |  |  |  |
| --- | --- | --- | --- |
| Switch-Off Date | Network Operator | Country | Technology |
| 01.12.2016 | Manitoba Telecom | Canada | CDMA |
| 01.01.2017 | Bell | Canada | CDMA |
| 31.01.2017 | Telus | Canada | CDMA |
| 31.07.2017 | SaskTel | Canada | CDMA |
| 2019 | AT&T | Mexico | GSM |
| 2020 | Movistar | Mexico | GSM |
| 31.12.2016 | AT&T | USA | GSM |
| 31.12.2019 | Verizon Wireless | USA | CDMA |
| 31.12.2020 | T-Mobile | USA | GSM |

\*UMTS900 to remain in operation while UMTS2100 will be gradually wound down until switch-off date. If IoT and M2M companies hope to continue to compete after 2G networks are shut down around the world, they must evolve – and implement hardware that supports modern cellular technologies [31].

It’s important to note that there may be restrictions on 2G network usage even before the actual sunset date. Firstly, carriers will stop activating new 2G devices well in advance of the network shutdown. If you already have a cellular router or phone connected to the network you’ll still be able to use it but new device registration may be impossible. Secondly, carriers will re-farm spectrum ahead of the network shutdown, which means that 2G-only devices may no longer work as well as they used to in these locations.

The only good news is that 4G LTE will be available for at least a decade to come, and will co-exist with 5G networks. In this post, we’ll provide updates on the sunsetting of 2G and 3G networks and the outlook for 4G LTE and 5G networks, to support those who are planning their migration path[32].

References

1. [https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/gsm-encryption#:~:text=GSM%20encryption%20is%20the%20means,inherent%20in%20exporting%20such%20codes](https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/gsm-encryption" \l ":~:text=GSM%20encryption%20is%20the%20means,inherent%20in%20exporting%20such%20codes).
2. <https://www.researchgate.net/publication/50359271_Implementation_of_Cryptographic_Algorithms_for_GSM_Cellular_Standard>
3. M900/M1800 GSM SYSTEM, Training Documents, Huawei Technologies CO. Ltd. Training Center.
4. <https://web.archive.org/web/20100521013451/http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm>
5. <https://www.tutorialspoint.com/gsm/gsm_security.htm>
6. <https://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317>
7. <http://www.gsmhistory.com/rare-gsm-documents/>
8. <https://cdn.ttgtmedia.com/rms/onlineimages/mobile_computing-gsm.png>
9. <https://searchmobilecomputing.techtarget.com/definition/GSM>
10. <https://ieeexplore.ieee.org/document/5635451>
11. <http://article.nadiapub.com/IJSIA/vol10_no6/22.pdf>
12. Jorg Eberspacher, Hans-Jorg Vogel, Christian Bettstetter, “GSM, switching, Services and Protocols”, 2nd edition, (WILEY), 2001.
13. Goswami, Sukalyan, et al. "Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm." Intelligent Systems, 2012 Third International Conference on Modelling and Simulation (ISMS). IEEE, 2012.
14. Petracca, Marco, et al. "Performance evaluation of GSM robustness against smart jamming attacks." Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on. IEEE, 2012.
15. Barkan E, Biham E, Keller N, „Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications“, Journal of Cryptology, 21(3), pp. 392-429. DOI: 10.1007/s00145-007-9001-y, June 2008.
16. <http://article.nadiapub.com/IJSIA/vol10_no6/22.pdf>

1. <https://www.ques10.com/p/48395/gsm-authentication-procedure-1/#:~:text=Authentication%20in%20the%20GSM%20system,the%20MS%2C%20not%20the%20user.&text=To%20request%20for%20a%20call,MS%20has%20to%20get%20authenticated>.
2. <https://web.itu.edu.tr/~korkusuza/Security%20in%20the%20GSM%20Network.pdf?kategori=php>
3. <https://www.mpirical.com/glossary>
4. <https://www.gsma.com/security/security-algorithms/>
5. Jochen Schiller, Mobile Communications Second Edition, 96-122.
6. <https://www.itu.int/osg/spu/imt-2000/technology.html>

1. <https://asecuritysite.com/encryption/a5>
2. Gendrullis, Timo, Martin Novotný, and Andy Rupp. "A real-world attack breaking A5/1 within hours." Cryptographic Hardware and Embedded Systems–CHES 2008. Springer Berlin Heidelberg, 2008. 266-282.

1. <https://arxiv.org/ftp/arxiv/papers/1002/1002.3175.pdf#:~:text=The%20anonymity%20in%20the%20GSM,in%20every%20location%20update%20procedure>.

1. <https://en.wikipedia.org/wiki/A5/1>

1. <http://www.wirelessdictionary.com/Wireless-Dictionary-A3-Algorithm-Definition.html>

1. <https://link.springer.com/chapter/10.1007/978-3-642-02342-2_18>

1. <https://en.wikipedia.org/wiki/KASUMI>
2. "3GPP TS 35.202: Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification". 3GPP. 2009.
3. <https://www.emnify.com/resources/global-2g-phase-out>
4. https://www.digi.com/blog/post/2g-3g-4g-lte-network-shutdown-updates