Journal of Computer Science

Original Research Paper

Features of the Security System Development of a Computer Telecommunication Network

Leonid Chervyakov, Tagirbek Aslanov, Dmitry Polezhaev and Viktor Lysenko

World-Class Scientific Center "Digital Biodesign and Personalized Healthcare", Institute for Design-Technological Informatics RAS, Moscow, Russian Federation

Article history
Received: 12-03-2024
Revised: 15-05-2024
Accepted: 17-05-2024

Corresponding Author:
Dmitry Polezhaev
World-Class Scientific Center "Digital Biodesign and Personalized Healthcare", Institute for Design-Technological Informatics RAS, Moscow, Russian Federation
Email: dm.polezhaev@bk.ru

Abstract: Global computer networks have enabled ordinary users, companies, organizations and medical institutions to gain virtually unlimited access to data arrays. Therefore, developing systems capable of ensuring the good performance and secure operation of a standard Computer Telecommunication Network (CTN) has become one of the most pressing tasks demanded in the medical industry. Consequently, this study aims to create an ordered chain of operations that can perform information encryption to enhance data transmission and exchange security. This study examines the existing ordered chains of encryption operations and assesses their strengths and weaknesses. In addition, a framework for implementing cryptographic algorithms is proposed. This algorithm structure enables verification of the existence of the correct key along the specified path, thereby enhancing the overall security of the system. The study results indicate that the optimal variant of encryption is the ordered chains of encoding operations that rely on cryptography. The results of the testing demonstrated that the developed ordered chain of operations exhibited several advantages compared to its analogs, with an efficiency that exceeded that of the analogs by more than fourfold. The implementation of the proposed ordered chain of operations would provide a significantly safer operation of a standard CTN in a typical Medical Institution (MI).

Keywords: Code, Computer Telecommunication Network (CTN), Information Security (IS), Encoding, Ordered Chain of Operations

Introduction

Today, many specialized programs are available to build CTN information and software. However, concerning the Medical Computer Telecommunication Network (MCTN), most available products often do not meet the basic requirements, including the essential requirement of information protection from unauthorized access to MCTN data arrays. An equally important requirement is adapting the functionality of any program purchased for MCTN to minimize the possibility of hacking by intruders, prevent data leakage and increase the product's resistance to viruses, as detailed by Kuklin *et al*. (2023).

Therefore, developing an information and software shell that will consider the list of requirements for modern MCTN and the very specifics of this category of networks operating in most regions is an essential task today. It is worth considering that it is necessary to encrypt only valuable data. For example, secret, private, confidential and others are categorized into several levels of importance. However, the level of data Information Security (IS), which is the subject of trade secrets, should be determined by the company itself, which is the owner of this information, as detailed by Privalov *et al*. (2019); Polezhaev *et al*. (2023); Gürkaynak *et al*. (2014). Using different encryption algorithms yields different encryption keys with different data rates. The fastest data encryption algorithm should be identified and its security optimized by implementing a comprehensive encryption key verification structure. A system of verification of this algorithm should also be developed to ensure the required level of safety.

In order to guarantee the integrity of IS in MCTN, it is proposed that a secure network be developed for the transmission of data, with the essential data being sent in encrypted form. The system will ensure the stable operation of this network and optimize the degree of IS key components. The objective of this study is to create an ordered chain of encryption operations and develop methods for organizing IS in an MCTN.

Today, ISPs organize most connections among medical institutions using existing infrastructure or a private network. Even though an ISP employs an existing network and offers a sufficient range of network services to mobile users, it still takes some time to configure the existing network, deploy the necessary infrastructure components and organize IS, which is usually costly. In addition, sometimes the network is simply absent and its creation will take a long time or, in a particular region, is impossible in the foreseeable future for one reason or another.

Most mobile devices operating in a particular band communicate with each other through a Dynamic Mobile Network (DMN) characterized by high capacity and flexibility. From the IS point of view, the structure of any functioning communication channel is very similar to that of other channels operating in a given region, differing only in the amount of memory and data processing speed. Here, we consider a standard MCTN whose IS level is still insufficient, especially in encryption issues.

Modern medical networks actively use GSM and its versions. Moreover, telemonitoring programs frequently integrate subjective inquiries regarding patients' health and comfort into their operational protocols. These inquiries can be conducted automatically over the GSM line or facilitated by telemonitoring software that facilitates communication between patients and their healthcare providers, as detailed by Lu *et al*. (2010).

The GSM architecture can also be used as a life-saving device by using it with a body sensing sensor and in case of a critical drop in certain parameters to make an ambulance call via SIM, as detailed by Suganthi *et al*. (2022).

However, GSM has certain disadvantages that primarily affect its security issues. However, most operators still use the traditional GSM network. It turns out that GSM and its further improvement should provide the proper level of IS but still apply a standard radio pulse to organize mobile communication between subscribers. This structure of information exchange increases the sensitivity of radio pulses and interested parties can use it by accessing the network through mobile stations. For this purpose, attackers masquerade as a standard subscriber gaining access to the data exchange. Therefore, we can outline two main directions of IS provision regarding the data transmitted through GSM network and its versions, expressed by the following: (1) The public availability of services offered by modern mobile communication; (2) The need to prevent the disclosure of valuable information transmitted through the standard radio channel. Regarding medical CTNs, it is also a question of preventing the possibility of harming patients' health, as discussed in more detail in Yablochnikov *et al*. (2019); Rao *et al*. (2023).

In this study, we propose several technical solutions whose practical realization will improve the IS of existing MCTNs using the GSM standard. Practice shows that today's IS forms the basis of the work of any organization, company and institution, as detailed in Ibragimov *et al*. (2022); Alexandrov *et al*. (2023); Manocha *et al*. (2021).

Materials and Methods

The principles of the GSM IS architecture initially ensure anonymity, identification and the highest possible confidentiality of transmitted data.

Let us enumerate the main tasks faced by GSM IS regarding medical CTNs discussed in Ekwonwune *et al*. (2022); Al-Dujaili and Al-Dulaimi (2023):

- Identify each user of mobile communication by the network
- Ensure the highest possible confidentiality of the data sent and received by subscribers
- Apply SIM as a block responsible for IS

The primary identification key for individual users (K_i) is a randomly selected digit from 128-bit, which acts as a cryptographic key to produce a session code (their sequence). K_i is the base code stored in the user cell on the SIM. Before data exchange, the subscriber enters a sequence of digits, activating one of the three ordered chains of operations: A5/one, A5/two and A5/three. A5/one and A5/two represent streaming codes pre-set by GSM. Note that A5/one is more powerful but is available only in CEPT member states. Meanwhile, A5/two is less powerful and accessible in other states, as detailed by Kuklinski *et al*. (2020).

The application of this category of ordered chains of operations is continuously monitored by the central operator's system, according to the GSM memorandum. The structure of A5/three consists of a block code based on an ordered chain of "Kasumi" operations identified by telephones that support two modes, 2G and 3G.

The SIM also stores all necessary data about the users' accounts. All SIM cards retain the IMSI and K_i base codes. IMSI and K_i codes provide identification codes and sufficient confidentiality of the subscribers' data. Most SIM cards also involve the A3 and A8 coefficients of ordered chains of operations. A3 usually applies for subscribers' identification and A8 for producing cryptographic codes K_c. After subscriber identification, the network may send requests to their mobile device necessary to start encryption using the generated session code K_c. This interaction scheme uses public keys to encode network data. Therefore, the primary attention in fixing the subscriber-specific location is paid to encoding based on public keys (Prajapat *et al*., 2021).

DOI: 10.3844/jcssp.2024.986.996

There are many questions about the organization of GSM IS, for example, the formation by GSM networks of secure ordered chains of operations of identification and encoding. The very principle of this network functioning has disadvantages that make the operation of its main ordered chain of operations less stable and secure. For example, an intruder can create a SIM replica and obtain a base user code to work in the network on his behalf. In addition, attackers can extract K_i codes and IMSI of subscribers even without gaining actual access to the owners' SIM cards, which gives the conditional hacker the opportunity to clone standard SIM cards, as detailed by Voznak *et al*. (2015); Siergiejczyk and Rosiński (2019). The authentication, encryption and session key change processes of the GSM standard are shown in Fig. 1.

Initially, the network sends a request to identify the subscriber, whose mobile device generates an identification response in the form of an output pulse. Figure 2 shows the order of sending a request by the network and receiving a response to the network request. The random number is generated using the AUC algorithm. Initially, the authentication request is sent to the system and the authentication response comes as an output.

Cryptographic complexes functioning on open sequences of codes generally produce two electronic codes for any subscriber: An unprotected code, used to encode the main flow of information and a protected code, used for decoding. The protected code of the subscriber opens the possibility of recovering the session code and further the recognition of files sent within the network using the decoded key, as detailed by He *et al*. (2021); Etemadi Borujeni and Eshghi (2011).

The DES information encoding model (often called ordered chain of encoding operations DEA) eventually formed the DEA-1 model, which today is one of the world standards. In addition, DES performs information encoding using 64-bit modules. DES is a symmetric ordered chain of operations, so one ordered chain of operations working with one code applies to encode and decode data. The code dimensionality is typically 56-bit.

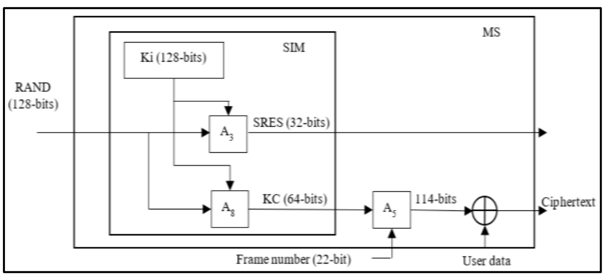

Fig. 1: Identification, key generation (key sequence) of the current session and encoding performed using the GSM scheme

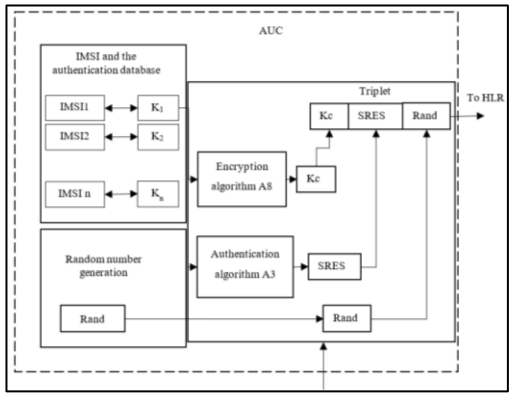

Fig. 2: Scheme for generating triplets using the AUC

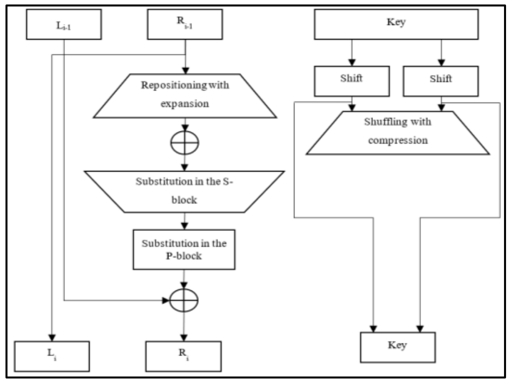

Fig. 3: One stage of DES execution

The code generally uses 64-bit digits, but the system keeps track of every 8th bit to clarify its pairing and can always change the code expressed by any 56-bit digits. However, the standard sequence of digits can be safely classified as a weak code, although only this sequence establishes the security level.

Simply put, the primary ordered chain of operations that ensures the functioning of the GSM network is a combination of core encoding techniques of deviation and variance. For example, if we consider text files, the basic DES module is a single combination of these techniques (input and then move) defined by the base code. Figure 3 shows this module structure called a "stage." In general, DES includes 16 stages, uses identical combinations of input and moves to the plaintexts at least 16 times. The ordered chain of operations uses only the arithmetic of 64-bit digits and several logical operations, providing a simplified order of operations. The presence of many repetitions, the base of an ordered chain of operations, practically transforms it into a reference tool implemented in specialized microcircuits.

DES generally interacts with 64-bit text modules. Thus, upon completion of the initial input and subsequent movement of the chain, the module splits to obtain the left and right segments of 32-bit each. The

16 stages of similar operations, expressed by dependency f, combine fragmented information with the base code. At the end of the final stage, both segments combine and the functioning of the ordered chain of operations ends with the resulting movement. In all stages, the bit of the base code continuously shifts, selecting 48-bit from the 56-bit of the base code.

The right information segment volume increases to 48-bit by moving and expanding, then the segments combine thanks to XOR-48-bit codes passed through 8 S-modules to form the next 32-bit, then performing the permutation again. Subsequently, the dependence f combines with the left segment of the next XOR. The result of the considered operations is the formation of a new right segment, while the former right segment becomes a new left segment. This sequence of actions is repeated at least 16 times, generating 16 stages of DES.

The initial movement is performed for each table of *f*-dependence values, reading the table data by the ordered chain in a standard manner. For example, due to the initial relocation, 58-bits become position No. 1, 50-bit become position No. 2 and 42-bits become position No. 3. The initial and final movements do not affect the security of DES, focusing mainly on simplifying the procedure of obtaining information expressed by an open or encoded file. Next, the resulting code moves. In the first stage, the code dimensionality of the 64-bit DES reduces to 56-bits due to the discarding of 8-bits, which, as we have already discussed, are used by the system solely for pairing tracking. It also checks the integrity and immutability of the structure of the received code. Upon unloading the base code of 56-bits, DES produces another intermediate code of 48-bits. The code of 56-bits is split into two equal segments. Then, the segments cyclically shift to the left by a few bits, given the current stage.

After the shift, every 48th of the 56th-bits is selected. Because the current procedure chooses several intermediate bits sets with a natural change in their order, it has been called "shifting with packing." This procedure results in a conditional list consisting of a sequence of 48-bit segments. For example, a code bit shifted from line 33 occupies a cell in line 35, while the system neglects the 18th bit of this code. Thanks to the shift, the primary sequence of codes uses each successive intermediate code using the next bit in 14 of 16 intermediate codes, but not every intermediate code is used a strictly defined number of times.

In parallel, the process expands the right information segments, e.g., Rt from 32-48-bits and simultaneously, the sequence of certain bits repeats and their order modifies, commonly referred to as "moving with unpacking." This procedure aims to level the dimensionality of the right segment with that of the base code, which is necessary for implementing the XOR procedure and obtaining more voluminous chains for packing during substitution. Therefore, the considered ordered chain of operations does not make it possible to realize the primary function of efficient encoding, as detailed by Belazi *et al*. (2017).

A movement followed by unpacking is called the E-module. Thus, regarding any incoming module containing four bits, the 1st and 4th bits are a single bit of the output module, while the 2nd and 3rd bits are a single bit of the incoming module. For example, the bits stored in the input module of position 2 will move to position 5 of the output module, while the next bit occupying position 22 will move to positions 31 and 33.

The final movement is opposite to the initial one. Here, both segments retain their former positions at the end of the DES extreme stage and the combined module can serve as the input stage of the final movement. This feature applies with the sole purpose of the ordered chain of operation to perform all encoding and decoding stages.

The weakness of DES is the relatively small dimensionality of the base codes. Therefore, other ordered chains of operations are created for more efficient encoding. A simple option to increase the dimensionality of the codes is to use DES repeatedly with different codes. The application of K_1 and K_2 codes to non-encrypted signal P makes it possible to form an encoded signal C:

$$C = E_{k2}[E_{k1}[P]] \tag{1}$$

$$X = E_{k1}[P] = D_{k2}[C] \tag{2}$$

Recall that because of using expression $P = D_{k1}[D_{k2}[C]]$ while decoding the base codes, their final dimensionality is 112-bits.

In creating a closed MCTN project, we considered several optimal protection options that provide high efficiency with relatively low investments, given that we protect patients' health. This problem can be solved by efficient encryption. Let us justify this assumption and propose an optimal encryption method to solve this problem.

It is essential to guarantee the stable distribution of the base code to ensure the proper level of IS. After the analysis and experimental use of the method discussed above, we have created a universal system capable of organizing the protection of electronic document circulation. The system performs document encoding; the formation of an electronic code, "eToken," a separate tool that provides registration and identification of the subscriber; safe memorization of the document configuration; and information integrity, which makes it possible to use EDS, as described in Jo *et al*. (2007).

Table 1: Encoding scheme

Group	Displaying	Form of the provision
DES	An ordered chain of operations that provides encoding: A module including 64-bits and a base code of 64-bits	Design, MI management, subscriber
Triple DES	The 64-bit module uses an encoder that applies DES three times This layout demonstrates a high degree of protection against various types of attacks	Design, MI management, subscriber
Cascade triple DES	Typical triple DESs are equipped with a mechanism that provides flexible feedback and a high level of protection against almost all types of attacks	A representative of MI administration, subscriber
FEAL	Modular encoder is used instead of DES	Design, the subscriber
IDEA	A 64-bit modular encoder, the dimensionality of the base code is 128-bits, 8 actions	Design
Skipjack	A 64-bit modular encoder, base codes of 80-bits are applied at various stages, 32 actions	Design, subscriber
RC2	A 64-bit modular encoder, the dimensionality of the base code may vary	Design, subscriber
RC4	Encoded stream demonstrating a tenfold increase in performance relative to standard DES	Design, a representative of MI administration and subscriber
RC5	The dimensionality of the base module can vary, the dimensionality of the base code can vary from zero to 2048-bits and up to 255 actions can be performed	Design, a representative of MI administration and subscriber
CAST	A 64-bit modular encoder, base codes of dimensionality from 40-64-bits, 8 actions	Design, subscriber
Blowfish	A 64-bit modular encoder, base code, whose dimensionality can change up to 448-bits, 16 actions	be designed, a representative of MI administration and subscriber
System with a set of session codes	The base code has the same dimensionality as the encoded information. This code is an "n" number of bits derived from a set of randomly generated chains of bits stored in the system memory	Design, a representative of MI administration and subscriber

Let us consider popular encoding tools (Table 1). The DES encoding principle was created one of the first by leading specialists of IBM company using their codification, which eventually became universal, as given by Sinha and Singh (2003). DES is a symmetric cipher, which means that the same key is used for both encryption and decryption. DES is a symmetric cipher, which means that the same key is used for both encryption and decryption. For each block of plaintext, encryption is handled in 16 rounds, each of which performs an identical operation. The main disadvantage of this algorithm is its small key space, which entails vulnerability to brute-force hacking techniques.

An alternative to the Advanced Encryption Standard (AES) or the AES finalist algorithms is triple DES, which is often denoted as 3DES. The 3DES algorithm comprises three consecutive DES encryptions. It is considered to be highly resistant to both brute-force attacks and any analytical attack that can be conceived. 3DES is highly efficient in hardware, but less so in software. It is also employed in financial applications and for protecting biometric information in electronic passports, as described by Paar and Pelzl (2010).

Blowfish is one of the symmetric modular codes constructing effective IS in standard CTNs (Fig. 4). In this case, the dimensionality of the base code can vary from 32-448-bits, making this code a reference for system information protection. The algorithm was developed to encrypt 64-bit plaintext into 64-bit ciphertext in a manner that is both powerful and secure. The operations selected for the algorithm were carefully chosen to minimize the time required to encrypt and decrypt data on 32-bit mainframes. These operations included table lookup, modulus, addition and bitwise exclusive-or. Once the algorithm has been initialized, it is capable of encrypting and decrypting data efficiently. Consequently, Blowfish would be a more suitable choice for applications that require the key value to be changed infrequently and for the encryption or decryption of large streams of data. Using the Blowfish cryptographic algorithm, various medical data can be encrypted. Such a system involves collecting data on patient body parameters, processing the data and encrypting and transmitting the data over a wireless network. It also includes decrypting and finally displaying the data on a computer, as described by Kondawar and Gawali (2016).

Rijndael is an Advanced Encryption Standard (AES); in this standard, the cipher key can only be 128, 192, or 256-bits long. At a basic level, the Rijndael algorithm uses several rounds to transform the data for each block. The algorithm can be made public but this does not help an attacker decipher a message, as the encryption key must implement the algorithm. This allows us to define a standard that everybody can follow, as described by Wright (2001).

Ordered chains of operations capable of encryption comprise two large groups formed concerning a particular encryption technique, as detailed by Velan *et al*. (2015); Alrikabi and Tuama Hazim (2021). Such chains can use special keys to make it impossible, as considered, to read the information encrypted in this way without keys (Sikka *et al*., 2020).

The encoding process in mobile CTNs occurs at the second stage (L_2), MAC stage, or RLC stage. Here, the specific location of the main encoding dependency is determined by the specificity of the connections, organizing their control through transparent RLC connections. In the case of data transmission via RLC, encoding is performed at the MAC layer and the base encoding is carried out in a network of isolated channels, as shown in Fig. 5.

Table 2 shows the non-symmetric ordered chains of operations used in non-symmetric coding complexes to secure cyclic codes, as detailed by Li *et al*. (2019). The non-symmetric method uses two codes: Public and secure, as detailed in Lai *et al*. (2010). Table 3 shows the data on the dimensionality of the key.

JCA it serves as a base platform "supplying" the configuration of the API list necessary for encoding information, its certification, generation of base and additional codes and others. We proposed a tested system capable of providing encryption resistant to the unauthorized actions of intruders.

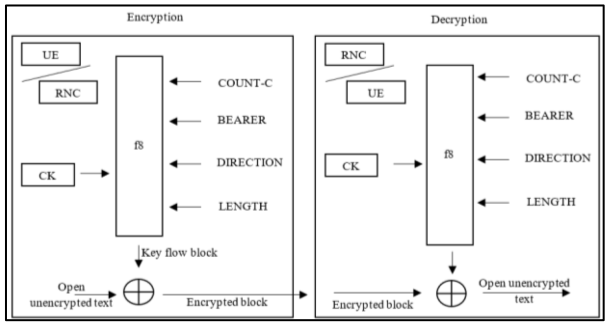

Fig. 4: Encryption/decryption scheme in standard CTN

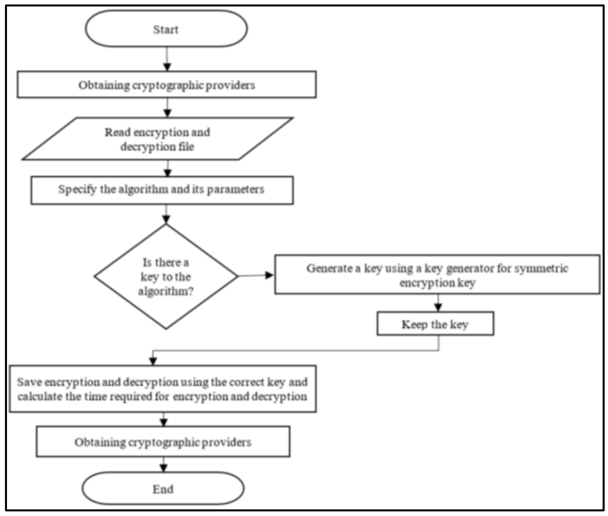

Fig. 5: Symmetric encoding scheme

Table 2: Non-symmetric ordered chains of operations used in non-symmetric coding complexes to secure cyclic code

Group	Tools	Form of the provision	Function
RSA	Ordered chain of decomposition operations	Design	Resistance to malicious attackers is due to the complexity of integer decomposition
ECC	The arithmetic system is involved. The performance is much faster than that of RSA and DSA	Design, subscriber	It is expressed by segments of elliptic dependence necessary for the functioning an asymmetric ordered chain of operations provide encoding
Scheme proposed by El-Gamal	The method proposed by	Subscriber	It is used for encoding and Electronic Digital Signature (EDS) formation

Table 3: Dimensionality of the key

Dimensionality of the symmetric keys (bit)	Dimensionality of the public keys (bit)	Function and form of provision
56	384	Subscriber
64	512	Subscriber
80	768	A representative of MI administration, subscriber
112	1792	A representative of MI administration, subscriber
128	2304	A representative of MI administration, subscriber

Results

We developed an ordered chain of operations that continuously monitors the presence or absence of the base code in the information flow. The administrator knows the path to the generated code located in a memory cell of the system. Before file encoding or decoding, the organized chain of operations generates a command to start the timer.

The cells specified by the system store the output files. Figure 6 shows the results of encoding 64-bit text files.

The encryption time is used to calculate the throughput of the encryption scheme. The experimental results are shown as histograms in Fig. 7 during the encryption stage. The results show the superiority of the Blowfish algorithm over other algorithms in terms of processing time.

The complex solution developed in this study opens up the possibility of unified management of the formation of any Document Structure (DS) by users. The administrator can provide or restrict:

- Accelerated encoding of each document with automatic saving in the Automated system of Data Management (ADMS)
- Accelerated encoding of DS revisions
- Possibility of full-text numbering of the DS and its revisions
- Encoding in the process of DS modification

Ensuring complex control by the administrator of the following:

- The order of opening or closing the rights of users to view specific documents
- Specifying the period of access
- Detailing the authorization of users in fieldwork with documents and others

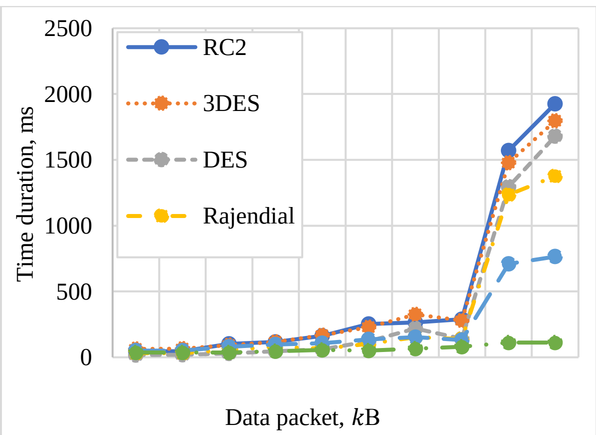

Fig. 6: Duration of an ordered chain of encoding operations functioning

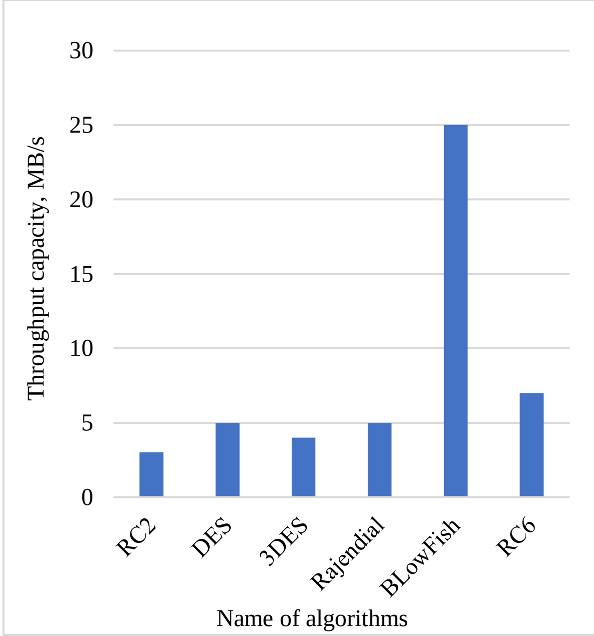

Fig. 7: Performance of core-ordered chains of operations that provide encoding

When a subscriber connects to the network, the system automatically launches a mechanism to verify the identity of the SIM owner, after which the mobile station processor decides to admit or deny the subscriber to a particular network. An ordered chain of operations tracks the number of such requests for subscriber identification, considering the secret code K_i, which the subscriber's mobile device stores in a particular cell of the built-in memory. Then, the encoding and sending of the signed response SRES to the SIM occurs. Note that the index A3 SRES K_i performs a similar process with respect to SRES, comparing its final dimensionality with the received response necessary to verify the authenticity of the base code. When the base code check meets the system requirements, subscriber identification is completed. Then, the base code is overwritten again in the SIM memory. Considering RAND and K_i as the base codes, it is possible to form a new code K_c from them. With its help, it is possible in the automatic mode to make encoding/decoding of sent and received information by the system. Simultaneously, K_i, corresponding to 54-bits, is used by an ordered chain of encoding operations in status A5 stored in the mobile device memory so that coding/decoding, if necessary, can be performed in roaming.

Implementing this functionality will require the following:

- Forming by the system of immediate rejection of an intruder when recognized as an IMSI subscriber
- Establishing a clear MSI

Therefore, the first response of the system should be automatic recognition and identification of the subscriber. For this purpose, the network sends a 128-bit message to the recognized mobile device.

The SIM relies on an ordered chain of A3 operations to produce K_i, which is generally original relative to each registered SIM. Therefore, SRES identification forwards SRES to the master station. Simultaneously, K_i, including the initial invocation to calculate the cyclic code K_c, sends it to the master station. This cyclic key applies in conjunction with the ordered chain of operations A5, which provides information coding.

Subscriber identification is necessary to verify subscriber/device data, determine access rights to the service package and ensure subscriber anonymity. Here, an ordered chain of A3 operations, which requires the IMSI identification code and K_i, will display the SRES response.

Subscriber identification is as follows. The mobile device generates a message to the system and its response with confirmation or denial of identification of a particular subscriber is sent to the SIM. Here, MS identification, relying on the IMSI sequence of digits stored on the MSC server, is sent to the MS, whose algorithm can process random numbers simultaneously with K_i to generate SRES when an ordered chain of A3 operations is applied. Simultaneously, both SRES segments pass the MSC control after the next combination, which is necessary for subscriber identification. In this case, the ordered chain of A8 operations will use the base code K_c together with randomly selected sequences of K_i, which will be its initial data. Thus, K_c will also become the base code for the ordered chain of A5 operations, which encodes voice information.

Figure 8 shows the features of GSM identification. The encryption key K_c is calculated every time authentication is performed.

All activities ensuring IS mode in the GSM standard occur in the 3GPP shell, for which several encoding techniques have been created. The first one covers the information of all subscribers and the signaling of detected violations. The second one encodes only the subscribers' information in roaming, considering the specificity of interaction between different networks. Figure 9 shows the features of IS support in a standard 3G network.

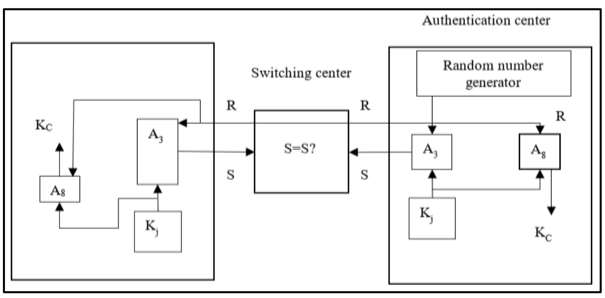

Fig. 8: GSM subscriber identification process

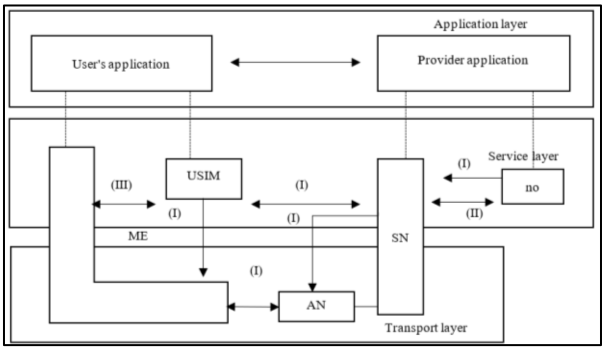

Fig. 9: IS support system in the 3G network

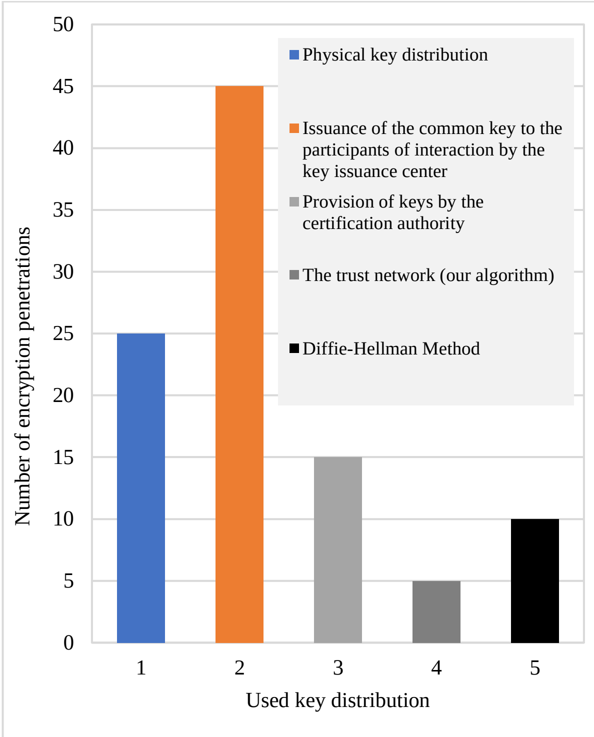

Fig. 10: Description of the number of hacking attempts of the encrypted information in MCTN considering the key distribution variant used

Using an ordered chain of operations in the MCTN will reduce the number of attempts to break or penetrate it fourfold without adding any new technical devices to the existing network structure. Figure 10 describes the advantages of the developed ordered chain of encoding operations.

Discussion

A computer telecommunications network is designed for the transmission, storage and exchange of data between users connected to the network. It is therefore expected that a certain level of security is maintained between users when using such a network. In medicine, such networks are used for structuring data storing patient information and internal system data. Since this is vital information, it is necessary to provide an appropriate level of protection for such information. The system assumes that each subscriber will be identified upon entering the system, and that further coding and decoding will occur automatically. This will ensure that the necessary level of security is maintained. The developed method should be intended for use in medical institutions as a basis for secure information transfer.

Conclusion

The study outlines the necessity for secure telecommunication networks in the field of medicine. The encryption structures analyzed revealed the necessity for cryptographic algorithms, which were subsequently selected. To realize the algorithm, a structure was developed to check the presence of a verifying key, thereby increasing its security.

Practical use of our methods of information encoding in MCTNs opens up the possibility of fourfold minimizing the number of hacking attempts by intruders. These methods do not require the extension of the existing network with any hardware devices. In addition, we have improved the subscriber identification procedure to guarantee an increase in the IS level. The practical application of this organized chain of encoding operations will ensure the possibility of creating, editing, saving and transmitting electronic documents with a high IS level. Our encoding methodology will guarantee the proper level of IS necessary for the normal functioning of MCTN.

Acknowledgment

The authors would like to thank professor Vladimir Kuklin for discussions of this article and useful ideas.

Funding Information

Selected findings of this study were obtained under the grant agreement in the form of subsidies from the federal budget of the Russian federation for state support for the establishment and development of world-class scientific centers performing R and D in priority areas of scientific and technological development No. 075-15-2022-307 dated April 20, 2022.

Author’s Contributions

Leonid Chervyakov: Conducted formal analysis and investigated; prepared the manuscript drafted, contributed to methodology and software.

Tagirbek Aslanov: Carried out validation and visualized, prepared the manuscript drafted and contributed to formal analysis.

Dmitry Polezhaev: Is responsible for conceptualized, reviewed and edited the manuscript drafted, supervised and administrated the project.

Viktor Lysenko: Is in charge of the methodology, software and resources and contributed to reviewed and edited.

Ethics

This article is an original research work. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved. The authors declare no conflicts of interest as there are no financial, personal, or other ties that may influence or may be perceived as affecting their work.

References

Al-Dujaili, M. J., & Al-Dulaimi, M., A. (2023). 5th-generation telecommunications technologies: Features, architecture, challenges and solutions. *Wireless Personal Communications*, *128*(1), 447-469. https://doi.org/10.1007/s11277-022-09962-x

Alexandrov, I. A., Kirichek, A. V., Kuklin, V. Z., Muranov, A. N., & Chervyakov, L. M. (2023). Developing the Concept of Methodological Support for Designing and Assessing the Efficiency of Information Protection Systems of Standard Information Systems Considering Their Vulnerabilities. *Journal of Computer Science*, *19*(11), 1305-1317. https://doi.org/10.3844/jcssp.2023.1305.1317

Alrikabi, H. Th. S., & Tuama Hazim, H. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of Interactive Mobile Technologies (IJIM)*, *15*(16), 144-157. https://doi.org/10.3991/ijim.v15i16.24557

Belazi, A., Khan, M., El-Latif, A. A. A., & Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics*, *87*(1), 337–361. https://doi.org/10.1007/s11071-016-3046-0

Ekwonwune, E. N., Chukwuebuka, U. C., Duroha, A. E., & Duru, A. N. (2022). Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System. *International Journal of Communications, Network and System Sciences*, *15*(10), 167–180. https://doi.org/10.4236/ijcns.2022.1510012

Etemadi Borujeni, S., & Eshghi, M. (2011). Chaotic image encryption system using phase-magnitude transformation and pixel substitution. *Telecommunication Systems*, *52*(2), 525-537. https://doi.org/10.1007/s11235-011-9458-8

Gürkaynak, G., Yilmaz, I., & Taskiran, N. P. (2014). Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer Law and Security Review*, *30*(2), 179-189. https://doi.org/10.1016/j.clsr.2014.01.010

He, Y., Ye, N., & Zhang, R. (2021). Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security. *Wireless Communications and Mobile Computing*, *2021*, 2295130. https://doi.org/10.1155/2021/2295130

Ibragimov, B., Melisova, S., Yernazarova, Z., Isroilov, B., & Usmanalieva, G. (2022). Fundamentals of the Application of the Mathematical Model in Economic Cybernetics. *Review of Economics and Finance, 20*, 1249–1255. https://doi.org/10.55365/1923.x2022.20.137

Jo, J.-G., Seo, J.-W., & Lee, H.-W. (2007). Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint. In F. P. Preparata & Q. Fang (Eds.), *Frontiers in Algorithmics* (1st Ed., Vol. *4613*, pp. 38-49). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-73814-5_4

Kondawar, S. S., & Gawali, D. H. (2016). Blowfish algorithm for patient health monitoring. 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India. *IEEE Xplore*, 1-6. https://doi.org/10.1109/inventive.2016.7830230

Kuklin, V., Alexandrov, I., Polezhaev, D., & Tatarkanov, A. (2023). Prospects for developing digital telecommunication complexes for storing and analyzing media data. *Bulletin of Electrical Engineering and Informatics*, *12*(3), 1536-1549. https://doi.org/10.11591/eei.v12i3.4840

Kuklinski, S., Czerwinski, M., Bieniasz, J., Kaminska, K. H., Paczesny, D., & Szczypiorski, K. (2020). Evaluation of Privacy and Security of GSM Using Low-Cost Methods. 2020 World Conference on Computing and Communication Technologies (WCCCT), Warsaw, Poland. *IEEE Xplore*, 96-105. https://doi.org/10.1109/wccct49810.2020.9170000

Lai, X., Lu, M., Qin, L., Han, J., & Fang, X. (2010). Asymmetric encryption and signature method with DNA technology. *Science China Information Sciences*, *53*(3), 506-514. https://doi.org/10.1007/s11432-010-0063-3

Li, W., Mclernon, D., Wong, K.-K., Wang, S., Lei, J., & Zaidi, S. A. R. (2019). Asymmetric Physical Layer Encryption for Wireless Communications. *IEEE Access*, *7*, 46959-46967. https://doi.org/10.1109/access.2019.2909298

Lu, W.-P., Leung, H., & Estrada, E. (2010). Transforming telemedicine for rural and urban communities Telemedicine 2.0-any doctor, any place, any time. *IEEE Xplore*, 379-385. https://doi.org/10.1109/health.2010.5556538

Manocha, H., Upadhyay, U., & Kumar, D. (2021). Experimental Evaluation of Security and Privacy in GSM Network Using RTL-SDR. In N. Gupta, P. Chatterjee, & T. Choudhury (Eds.), *Smart and Sustainable Intelligent Systems* (pp. 401-412). John Wiley and Sons. https://doi.org/10.1002/9781119752134.ch28

Paar, C., & Pelzl, J. (2010). The Data Encryption Standard (DES) and Alternatives. In *Understanding Cryptography* (1st Ed., pp. 55-86). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04101-3_3

Polezhaev, D. V., Tatarkanov, A. A., & Alexandrov, I. A. (2023). Forming the Architecture of a Multi-Layered Model of Physical Data Storage for Complex Telemedicine Systems. *HighTech and Innovation Journal*, *4*(4), 797-810. https://doi.org/10.28991/hij-2023-04-04-09

Prajapat, R. P., Bhadada, R., & Sharma, G. (2021). Security Enhancement of A5/1 Stream Cipher in GSM Communication and its Randomness Analysis. *IEEE Xplore*, 406-411. https://doi.org/10.1109/rtsi50628.2021.9597348

Privalov, A., Lukicheva, V., Kotenko, I., & Saenko, I. (2019). Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. *Energies*, *12*(24), 4768. https://doi.org/10.3390/en12244768

Rao, S. P., Chen, H.-Y., & Aura, T. (2023). Threat modeling framework for mobile communication systems. *Computers and Security*, *125*, 103047. https://doi.org/10.1016/j.cose.2022.103047

Siergiejczyk, M., & Rosiński, A. (2019). Analysis of Information Transmission Security in the Digital Railway Radio Communication System. In W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, & J. Kacprzyk (Eds.), *Contemporary Complex Systems and Their Dependability* (1st Ed., Vol. *761*, pp. 420-429). Springer International Publishing. https://doi.org/10.1007/978-3-319-91446-6_39

Sikka, P., Asati, A. R., & Shekhar, C. (2020). Speed optimal FPGA implementation of the encryption algorithms for telecom applications. *Microprocessors and Microsystems*, *79*, 103324. https://doi.org/10.1016/j.micpro.2020.103324

Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics Communications*, *218*(4-6), 229-234. https://doi.org/10.1016/s0030-4018(03)01261-6

Suganthi, J., Umareddy, N. V., & Awasthi, N. (2012). Medical alert systems with TeleHealth and telemedicine monitoring using GSM and GPS technology. *IEEE Xplore*, 1-5. https://doi.org/10.1109/icccnt.2012.6396073

Velan, P., Čermák, M., Čeleda, P., & Drašar, M. (2015). A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management*, *25*(5), 355-374. https://doi.org/10.1002/nem.1901

Voznak, M., Prokes, M., Sevcik, L., Frnda, J., Toral-Cruz, H., Jakovlev, S., Fazio, P., Mehic, M., & Mikulec, M. (2015). Vulnerabilities in GSM technology and feasibility of selected attacks. *SPIE Proceedings*, 94560T. https://doi.org/10.1117/12.2177111

Wright, M. A. (2001). The Advanced Encryption Standard. *Network Security*, *2001*(10), 11-13. https://doi.org/10.1016/s1353-4858(01)01018-2

Yablochnikov, S., Kuptsov, M., Vidov, S., & Olisaeva, A. (2019). The aspects of destructive influence of technical means and technologies of telecommunications on the person and society as a whole. *Proceedings of the XI International Scientific Conference Communicative Strategies of the Information Society*, 1-6. https://doi.org/10.1145/3373722.3373766