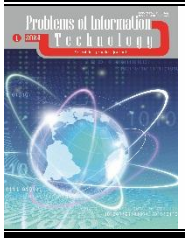

Available online at www.jpit.az

15 (2)
2024

Justification of encryption algorithm for systems monitoring personnel condition of critical informatization objects

Olga Boiprav[a], Oleg Zelmanski[b], Mehman Hasanov[c], Ekaterina Makarenya[d]

[a,b,d] Belarusian State University of Informatics and Radioelectronics, P. Brovki str., 6, 220013 Minsk, Belarus

[c] Azerbaijan Technical University, G. Javid Ave., 25, AZ1073, Baku, Azerbaijan

[a] smu@bsuir.by; [b] 7650772@rambler.ru; [c] mehman.hasanov@aztu.edu.az

[a] https://orcid.org/0000-0002-9987-8109; [b] https://orcid.org/0009-0000-5296-8986; [c] https://orcid.org/0000-0001-5536-9401

ARTICLE INFO

Keywords:

Encryption
Access control
Critical informatization object
Physical condition indicator
Blood alcohol content
Pulse
Saturation

ABSTRACT

The necessity of developing of systems for monitoring the physical condition of personnel at critical informatization objects is substantiated. It is shown that one of the technical problems that must be solved when developing such systems is ensuring the confidentiality and integrity of information processed within these systems. The solution to this problem is based on the selection and implementation of an encryption algorithm characterized by high performance. The encryption algorithm for systems for monitoring the physical condition of personnel at critical informatization objects must be characterized by high performance due to the need to minimize the impact of the functioning of these systems on the processes implemented within these objects. In this regard, the authors of the article conducted research aimed at determining the performance of the encryption algorithms Mars, AES (Rijndel), and Twofish, as well as their RSA add-ons. The dependence of the performance of the listed algorithms on the size and extension of the files encrypted using them, as well as the characteristics of the platform on which the encryption is performed, has been established. Recommendations have been made for the use of the studied algorithms in systems for monitoring the physical condition of personnel at critical informatization objects.

1. Introduction

Critical informatization objects are used to ensure the functioning of environmentally hazardous or socially significant industries. Violation of the normal operating mode of critical information facilities can lead to man-made emergencies. In this regard, in most countries, ensuring the correct functioning of critical informatization objects is one of the tasks to be solved in order to ensure national security. One of the directions in the process of solving this problem is assessing the physical condition of personnel working with critical informatization objects. For this purpose, it seems rational to use special monitoring systems. The purpose of these systems is to assess vital indicators of human physical condition (body temperature, pressure, pulse, saturation) and block access to the hardware and software of the specified objects for those representatives of the personnel of the specified objects in respect of whom it has been established that their physical condition indicators deviate from the norm (Zelmanski, 2024). Monitoring the blood alcohol content of personnel at these facilities deserves special attention, since managing sources of increased danger while intoxicated poses a particular danger. It should be noted that currently in the world, alcohol dependence is one of the most pressing threats to the safety and health of people (Manthey et al., 2021; Stoklosa et al., 2023). Up to

Received 15 March 2024, Received in revised form 13 May 2024, Accepted 27 May 2024
http://doi.org/10.25045/jpit.v15.i2.01

20–30% of healthcare costs are associated with the treatment of diseases caused by alcohol or drug use (Zelmanski, 2023). That is why, in systems for monitoring the physical condition of personnel at critical informatization objects, it is necessary to provide not only mechanisms for automatically obtaining quantitative values of basic indicators of human physical condition but also mechanisms for establishing the facts of a person being in a state of alcohol or drug intoxication. An important task that must be solved during the operation of such systems is the protection of the information they process. The importance of this task is due to the fact that the information provided constitutes personal data. The solution to this problem is based on the use of encryption algorithms (Ryabko, 2018; Khan & Por, 2024). One of the key requirements that must be placed on encryption algorithms for information processed within systems for monitoring the physical condition of personnel at critical informatization objects is high performance. This requirement is due to the need to minimize the impact of the functioning of these systems on the processes implemented within these facilities.

The aim of the present study was to establish the dependence of the performance from the point of view of hardware of complexity the algorithms underlying the operation of modern encryption software objects in information systems on the size and type of these objects and justify, taking into account the established dependence of the algorithm, which is most appropriate to use to protect information in systems for monitoring the physical condition of personnel of critical informatization objects.

To achieve this aim, the following tasks were set:

– review modern software tools for encrypting information in information systems (hereinafter referred to as software tools) and analyze the algorithms underlying the operation of these tools;

– select software for conducting research;

– evaluate the performance of the algorithms underlying the operation of the selected software;

– perform an analysis of the obtained assessment results.

The rest of the paper is organized as follows. Section 2 describes the researched data encryption algorithms. Section 3 presents the obtained experimental results. Section 5 contains the concluding remarks and future research directions.

Recently, the k-means algorithm and its modifications have become the research subject in analysing large volumes of data (Ping et al., 2024; Bagirov et al., 2022; Ahmadov, 2023; Aggarwal & Reddy, 2014). So, (Bahmani et al., 2012) proposed an approach, that is easy to implement, non-trivial, and converges reasonably quickly in a small number of iterations (Boutsidis et al., 2010; Jain, 2010). However, this approach is computationally expensive.

2. Researched data encryption algorithms

Based on the results of a study conducted by the NIST Institute, the following data encryption algorithms were selected as objects of study: Mars, AES (Rijndel), and Twofish, as well as their RSA add-ons (Assa-Agyei & Olajide, 2023; Ghosh, 2020).

The Advanced Encryption Standard (AES) is a specification for electronic data encryption established by the US National Institute of Standards and Technology (NIST) in 2001. AES is a block algorithm that encrypts data in blocks of 128 bits each. The encryption key size can be 128/192/256 bits. AES is based on the substitution-permutation principle, which means that the cipher is executed using a series of related operations, including substitution and shuffling of the input data. The cipher works in several rounds, the number of which depends on the key length:

– 10 rounds if the key length is 128 bits;

– 12 rounds if the key length is 192 bits;

– 14 rounds if the key length is 256 bits.

According to the AES algorithm, each block is treated as a 16-byte grid in a basic columnar arrangement. The AES algorithm is based on the following procedures:

– key extension (KSC);

– replacement of bytes (SubBytes);

– shift rows (ShiftRows);

– mixing columns (MixColums);

– adding and using round keys (9, 11, or 13 times, depending on the length of the encryption key) (Wahid et al., 2018; Xing et al., 2021).

The Twofish algorithm precomputes key-dependent substitution blocks (S-boxes). This distinguishes the Twofish algorithm from other encryption algorithms. The S-box hides the relationship of the encryption key to the ciphertext, despite being dependent on the encryption key. With a 128-bit block size and variable-length encryption key, Twofish is one of the most secure encryption algorithms. It is protected from brute-

force attacks since such an attack requires a lot of computing power.

The following features of the implementation of the steps of the Twofish algorithm can be highlighted:

– in each round of the Twofish algorithm, two 32-bit words serve as input data;

– each word is divided into four bytes (these four bytes are transmitted through four different channels, depending on the key);

– the four output words are concatenated using a maximum distance separable (MDS) matrix and concatenated into a 32-bit word;

– two 32-bit words are combined using the Hadamard pseudo-transform;

– two 32-bit words are added to two round connections;

– two 32-bit words are combined with the right half of the text (Gautam et al., 2019; Saieed & Hattab, 2023).

MARS is a shared key block cipher algorithm. The length of the blocks into which the data must be divided before encrypting it according to this algorithm is 128 bits. The algorithm is a word-oriented Feistel network.

The following features of the implementation of the steps of the MARS algorithm can be highlighted:

– use of addition, subtraction, and "exclusive or" operations to mix data;

– use of single values from 512 32-bit words;

– use of fixed rotations;

– use of data-dependent rotations (data-dependent rotations can lead to differential disadvantages; this problem is solved in MARS by combining these rotations with multiplications);

– use of multiplication operations (all multiplications within the MARS algorithm are performed modulo 232, which is suitable for most modern computer architectures).

The MARS algorithm takes a 128-bit input block as four 32-bit words. First, the input signal goes through a forward mixing stage, which contains keying and eight rounds of keyless forward mixing. It then goes to the cryptographic core (Feistel network), where eight rounds of forward keyed transformation and eight rounds of reverse keyed transformation are performed, and at the end there is another backmixing stage, which contains eight rounds of unkeyed backmixing and key subtraction (Ahmed & Elkamchouchi, 2022; Altigani et al., 2019).

3. Experimental results

During the study, the following was used.

1. Files with extensions *.doc, *.pdf, *.rar, *.ova, *.win, *.bak (8 files with each extension of the following size: 1 MB, 5 MB, 20 MB, 100 MB , 500 MB, 2 GB, 5 GB, 20 GB).

2. Advanced Encryption Package 2021 software tool.

3. Hardware platforms of four types:

1) monoblock Tesla R24VR TU VU 691129503.002-2012 with the following characteristics:

– operating system: Windows 10 21H1;

– storage: SSD 256 GB;

– RAM: DDR4 2666 MHz 8 GB;

– processor: Intel Core i5-12400, 6 cores, frequency 2.5 MHz, cache 7.5 MB;

2) laptop ASUS Vivobook 14 X409FA-BV625 with the following characteristics:

– operating system: Windows 11 22H2;

– storage: SSD 256 GB;

– RAM: DDR4 2400 MHz 8 GB;

– processor: Intel Core i3 10110U, 4 cores, frequency 4100 MHz, 8 MB cache;

3) Acer Aspire E1-531G-B9804G50Mnks laptop with the following characteristics:

– operating system: Windows 7;

– storage: HDD 500 GB;

– RAM: DDR 3 4 GB, 1333 MHz;

– processor: Intel Pentium 3558u, 1.7 MHz, 2 MB cache;

4) desktop computer with the following characteristics:

– operating system: Windows 10 21H1;

– storage: HDD 2TB;

– RAM: DDR4 2667 MHz 16 GB;

– processor: AMD Ryzen 5 Pro 5650G, 6 cores, frequency 3.9 GHz, 16 MB cache.

The research process included the following steps.

Step 1. Encrypt each of the files using a specific algorithm and each of the four hardware platforms above, subject to recording the speed of this process.

Step 2. Repeat step 1 four times.

Step 3. Calculate the average speed of the encryption process for each file based on the results obtained during steps 1and 2.

During the research process, more than 11,000 experiments were performed. The results of the experiments performed are presented in Figures 1–6.

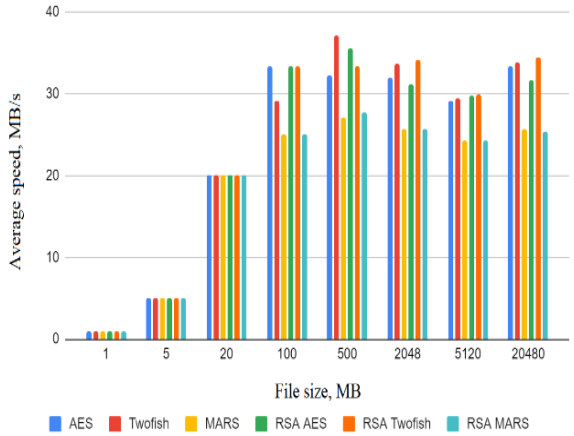

Fig. 1. Diagram showing the encryption speed of *doc files using different algorithms

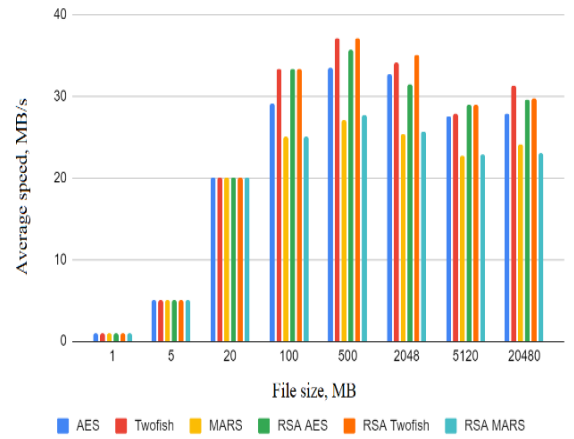

Fig. 2. Diagram showing the encryption speed of *.pdf files using different algorithms

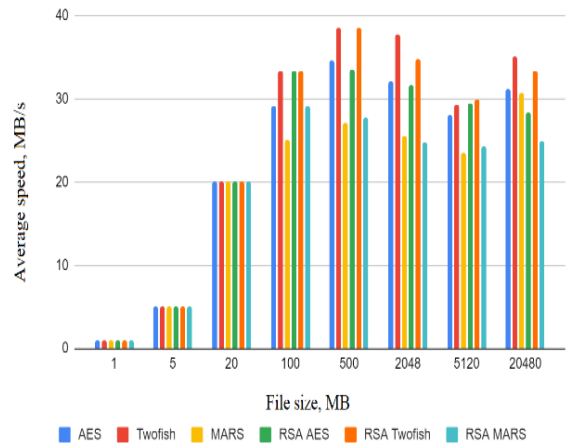

Fig. 3. Diagram showing encryption speed of *.rar files using different algorithms

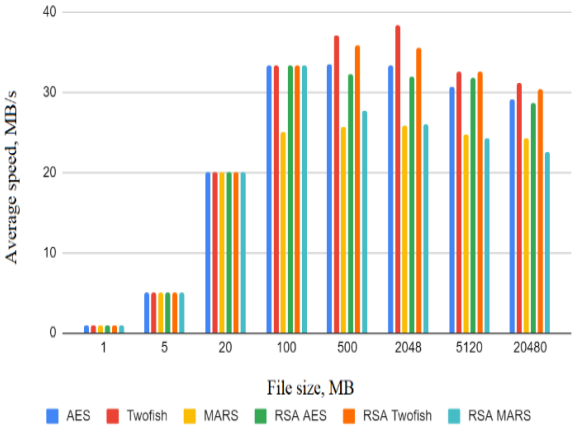

Fig. 4. Diagram showing how fast *.bak files can be encrypted using different algorithms

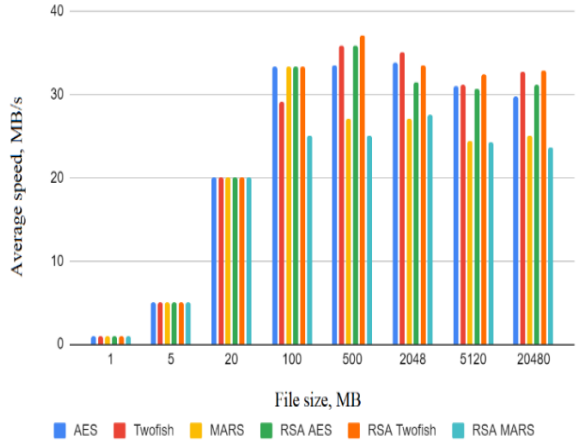

Fig. 5. Diagram showing how fast *.ova files can be encrypted using different algorithms

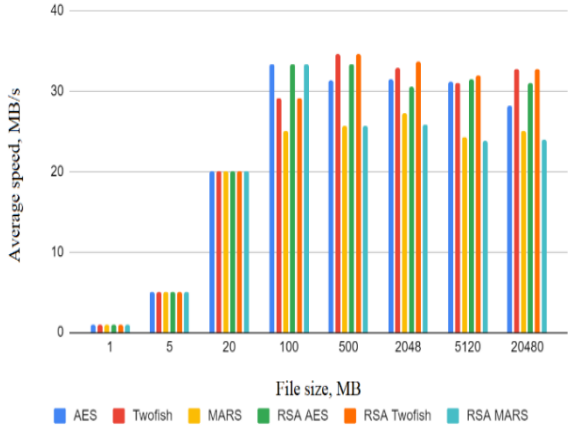

Fig. 6. Diagram showing how fast *.win files can be encrypted using different algorithms

From the presented results, it is clear that the AES algorithm was the fastest in 4 cases, the Twofish algorithm – in 16 cases, the AES (RSA) algorithm – in 7 cases, the Twofish (RSA) algorithm – in 18 cases, the MARS (RSA) algorithm – in 2

cases cases. The MARS algorithm was never found to be the fastest in the study. The results obtained by us are extended compared with the research results, presented in paper (Wahid et al., 2018). They contain the following data which is not contained in the indicated paper:

– the data about the speed of encrypting the files the size of which is more than 3.0 MB;

– the data about the speed of encryption algorithms Twofish and MARS;

– data about encrypting algorithms speed depending on the size of encrypted files.

Tables 1 and 2 systematize information about encryption algorithms that are the fastest when encrypting files with extensions *.doc, *.pdf, *.rar, *.ova, *.win, *.bak of a certain size.

Table 1. The fastest algorithms for encryption files with extensions *.doc, *.pdf, *.rar depending on these files size

File size, MB	Extension *.doc	Extension *.pdf	Extension *.rar
0–250	RSA, AES	Twofish	Twofish
250–1024	Twofish	RSA, Twofish	RSA, Twofish
1024–3072			Twofish
3072–10240	RSA, AES	Twofish	RSA, Twofish
10240–20480	RSA, Twofish	RSA, Twofish	Extension *.rar

Table 2. The fastest algorithms for encryption files with extensions *.bak, *.ova, *.win depending on these files size

File size, MB	Extension *.bak	Extension *.ova	Extension *.win
0–50	AES	AES	AES
50–250	Twofish	Twofish	Twofish
250–1024	RSA, AES	RSA, AES	RSA, Twofish
1024–3072	Twofish	Twofish	Twofish
3072–10240		AES	
10240–20480		Twofish	

4. Conclusion and future work

Based on the results of the research, we can conclude that the Twofish encryption algorithm is most appropriate to use to protect information processed by systems for monitoring the physical condition of personnel at critical informatization objects. This is due to the fact that the process of encrypting both small and large data sets using this algorithm is characterized by higher performance compared to the processes of encrypting data arrays using other algorithms currently recommended by NIST. Further research will be aimed at developing an improved protocol for the exchange of encrypted information between modules of systems for monitoring the physical condition of personnel of critical informatization objects (in particular, between developed module used to assess the quantitative values of basic human physical condition indicators (body temperature, pressure, pulse, saturation (Zelmanski, 2017)), module used to monitor the alcohol content in human blood and module used for monitoring and controlling technological equipment built on the designed integrated circuit for monitoring and control of technological equipment.

References

Altigani, A., Hasan, S., Shamsuddin, S. M., & Barry, B. (2019). A multi-shape hybrid symmetric encryption algorithm to thwart attacks based on the knowledge of the used cryptographic suite. Journal of Information Security and Applications, 46, 210-221. https://doi.org/10.1016/j.jisa.2019.03.013

Ahmed, F., & Elkamchouchi, D. H. (2022). A new modified MARS cryptosystem based on niho exponent with an

enhanced S-box generation. Electronics, 11(15), 2318. https://doi.org/10.3390/electronics11152318.

Assa-Agyei, K., & Olajide, F. (2023). A comparative study of Twofish, Blowfish, and Advanced Encryption Standard for secured data transmission. International Journal of Advanced Computer Science and Applications, 14 (3), 393-398.

Ghosh, A. (2020). Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks. International Research Journal of Engineering and Technology, 07(06), 4656-4659.

Gautam, S., Singh, S., & Singh, H. (2019). A comparative study and analysisof cryptographic algorithms: RSA, DES, AES, Blowfish, 3-DES, and Twofish. International Journal of Research in Electronics and Computer Engineering, 7 (1), 2019.

Khan, A. A., & Por, L. Y. (2024). Special issue on information security and cryptography: the role of advanced digital technology. Applied Sciences, 14(5), 2045. https://doi.org/10.3390/app14052045.

Manthey, J., Hassan, S. A., Carr, S., Kilian, C., Kuitunen-Paul, S., Rehm, J. (2021). What are the economic costs to society attributable to alcohol use? A systematic review and modelling study. Pharmacoeconomics, 39, 809-822. https://doi.org/10.1007/s40273-021-01031-8.

Ryabko, B. Y. (2018). Cryptography in the information world. Moscow, 302 p. (In Russian)

Saieed, A. H., & Hattab, A. A. (2023). Modifications and improvements to the Twofish encryption algorithm: a review. AIP Conference Proceedings, 2834, 050007. https://doi.org/10.1063/5.0161502.

Stoklosa, I., Więckiewicz, G., Stoklosa, M., Piegza, M., Pudlo, R., Gorczyca, P. (2023) Medications for the treatment of alcohol dependence-current state of knowledge and future perspectives from a public health perspective. International Journal of Environmental Research and Public Health, 20(3), 1870. https://doi.org/10.3390/ijerph20031870.

Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. (2018). A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. Journal of Computer Science Applications and Information Technology, 3(2), 1-7.

Xing, B., Wang, D. D., Yang, Y., Wei, Z., Wu, J., & He, C. (2021). Accelerating DES and AES algorithms for a heterogeneous many-core processor. International Journal Parallel Programming, 49 (3), 463-486. https://doi.org/10.1007/s10766-021-00692-4.

Zelmanski, O. B. (2024). System for remote monitoring and management of mobile and stationary objects and controlling of alcohol content in the blood of the personnel of these objects Medicine and High Technologies, 2, 22-29. (In Russian)
https://doi.org/10.34219/2306-3645-2024-14-2-22-29

Zelmanski, O. B. (2023). Technical support for the application of the normoxic therapeutic compression method in drug treatment practice Medicine and High Technologies, 4, 34-39. (In Russian)
https://doi.org/10.34219/2306-3645-2023-13-4-34-39

Zelmanski, O. B. (2017). Device for measuring oxygen saturation of human arterial hemoglobin and heart rate Official Bulletin, 2(115), 174. (In Russian)