КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.3953
UDC 004.056.5:004.75

Vitalii Chubaievskyi
Doctor of Sciences, associate professor, professor of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Nataliia Lutska
Doctor of Sciences, associate professor, professor of Department of Automation and Computer Technologies of Control Systems
National University of Food Technologies, Kyiv, Ukraine
ORCID 0000-0001-8593-0431
k.khorolska@knute.edu.ua

Tetyana Savchenko
PhD, associate professor, associate professor of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID 0000-0002-8884-5360
sv_t@ukr.net

Lidiia Vlasenko
PhD, associate professor, associate professor of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Kyrylo Synelnyk
Master's Student of Department of Computer Sciences and Information Technologies
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-4083-0255
synelnik@knute.edu.ua

ENHANCED CRYPTOGRAPHIC SECURITY OF AGGREGATED DIGITAL SIGNATURES THROUGH UTILIZATION OF A UNIFIED AUTHENTICATION FRAMEWORK

Abstract. The significance of this research lies in safeguarding user information and data against unauthorized alterations and destruction. Throughout the study, key aspects were explored, including user identification and authen-tication methods, cryptographic authentication protocols, digital signature properties, and strategies to enhance the cryptographic robustness of digital signatures. These strategies involved scrutinizing authentication methods using the Saati technique and the RSA algorithm. The analysis revealed that the attributes employed for digital signature recognition are highly resistant to replication, and the verification process is notably efficient. The height-ened cryptographic resilience of the electronic signature achieved through the RSA algorithm stems from the incorporation of a public key certificate. Consequently, a larger encryption key size corresponds to heightened sys-tem reliability and electronic digital signature security. While the utiliza-tion of the RSA algorithm results in encrypted text that is approximately 10 times larger than the original, its stability is comparatively increased.

Keywords: authentication; identification; user; digital signature; cryptographic security.

ISSN 2663 - 4023

INTRODUCTION

In the modern world, possession of information resources and access control to them are important. Therefore, the matter of information security that must protect infor-mation confidentiality, its accessibility to users, and data security from unsanctioned changes, information destruction is more relevant today than ever. User identification and authentication can be used for ensuring the protection of information and access to its resources, which allows someone to unambiguously identify who can access them, and their permission associated with specific resources [1].

The object of the research is the authentification process of computer systems and users of local networks.

The subject of the research is methods and ways of user authentication in computer systems and local networks [2].

The goal of this study is the research of the common types of dynamic and static authentication methods and the improvement of the cryptographic security of the digital signature at the expense of the RSA algorithm.

Based on the goal, the research has some objectives [3]:

- analysis of modern methods of user identification and authentication;
- definition of a cryptographic authentication protocol;
- study of the digital signature as one of the authentication methods;
- analysis of the cryptographic security of the RSA algorithm for electronic signa-tures.

Research methods. The research conducted in this study is based on modern analytical methods and improved cryptographic stability of digital signatures at the extent of the RSA algorithm.

The practical significance of this study lies in the authors' analysis of authentica-tion methods and the determination of the best one, which improves the cryptograph-ic stability of digital signatures due to the use of the RSA algorithm and the Cryp-Tool 2.0 development environment.

Scientific novelty. The best and most reliable authentication methods have been es-tablished and analyzed. A study of the cryptographic stability of digital signatures has been conducted using the RSA algorithm, which allows quick and reliable user authenticating in the system.

MECHANISMS OF USER IDENTIFICATION AND AUTHENTICATION IN THE SYSTEM

Overview of user identification and authentication properties in the system. Identification as well as authentication serves as the basis of software and technical means of security, reaching the first line of the information space defense, because other servers are designed to serve named subjects [4].

Authentication allows a user or a process acting on behalf of that user, to specify their name. With the help of authentication, which provides "verification of the validity", another user verifies the information provided by the subject.

There is no trusted route in an open network environment between two parties of identification and authentication, therefore, in general, the data that was transmitted by the subject may not match the received data used for verification. So, it is important to protect against active and passive network eavesdropping (interception, reproduction, and modification of data). The protection against transmission of pass-words in the open access and their

encryption does not work here too, so it is necessary to develop more complex authentication protocols [5].

The main reasons for complicating the reliability of identification and authentication are:

- network threats;
- some authentication properties can be found out, forged or stolen;
- a contradiction between the system reliability and the convenience of the system administrator or user; therefore, for security reasons, it is necessary to ask the user to reenter data for authentication because they could be replaced by another person;
- a reliable means of protection is more expensive.

Most modern identification and authentication systems already support the concept of a single sign-on to the network, which is more convenient for the user. For corpo-rate networks that contain many information servers and allow independent circula-tion, multiple identification or authentication is too burdensome [6]. Single sign-on is not the norm, so a compromise must be found between the criteria of reliability, cost, availability, and ease of use as well as administration of identifica-tion/authentication tools.

The identification and authentication service can become the object of cyber-attacks on availability. The configuration of the system is such that after the specified unsuc-cess-ful attempts, the device for entering identification infor-mation (for example, a terminal) is blocked, so an attacker can quickly terminate the work of a legitimate user by pressing a few keys. To prevent such attacks, it is necessary to limit the us-er's availability, that is, to change the user's operation session and access rights (per-mission to perform certain operations on certain objects).

Classification of methods and means of identification and authentication. Currently, there are several basic ways to identify users in the system. The main prob-lem with these methods is that they have their advantages and disadvantages, so software developers need to choose independently which method of identification is suitable for their software product. The subject can confirm its authenticity by pre-senting at least one of the following properties [7]:

- a password is a voice or text message, a combination a lock or a PIN code;
- the subject's item can be a key, a data file, etc. This authentication is often generated in smart cards;
- biometrics — portrait, fingerprint or palm print, voice or iris.

The general procedure for subject identification and au-thentication is presented in Fig.1.

Several basic authentication methods differ in complexity and cost, they are the main indicators. Like any other method, authentication has its advantages and disad-vantages and is divided into types [8]:

- single-factor authentication. When connecting the system, the user confirms his authentication;
- two-factor authentication. After the user is authenticat-ed, the system must also confirm the authenticity;
- three-factor authentification. To confirm the authentication of the subject when transferring or exchanging data, a "notarial authentication service" is used.

ISSN 2663 - 4023

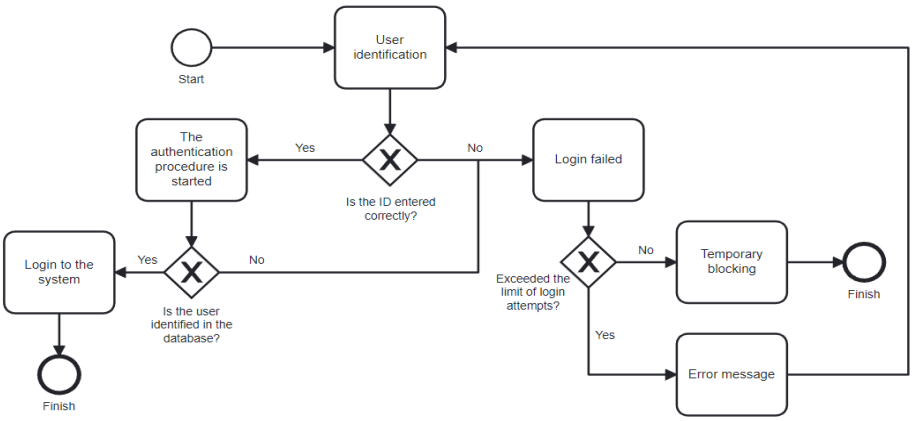

Fig. 1. Identification and authentication procedure

Conventionally, authentication methods are divided into single-factor and multi-factor ones. The classification of authentication methods is presented in Fig. 2.

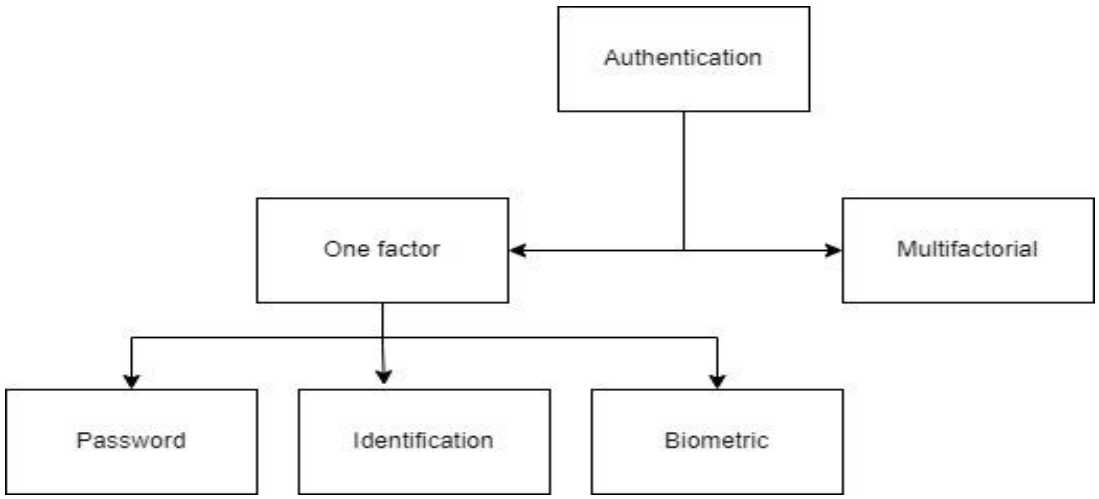

Fig. 2. Classification of authentication methods

One-factor authentication is divided into password, identification, and biometric authentication.

Password authentication is a simple and the most common method of authentication, which is the following: the user enters his password, then the authentication system compares it with the password that is stored in the database in encrypted form or the utility [9].

Identity authentication is based on the use of unique items, which are more reliable than the password method and are divided, in turn, into [10]:

- passive — they store authentication and transfer it to the authentication module when needed or called, such information can also be contained in an open-type object (magnetic cards, electronic devices, etc.);
- active — provided with sufficient computing resources that participate in authentication.

Biometric authentication is based on the use of a device to calculate input data and compare them with a standard set of personal characteristics of the user [11]. Biometrics is a set of automated user authentication tools based on physiological and behavioral characteristics. Physiological features include fingerprints on the hands and feet, the eye retina and cornea, the face geometry, and much more. Behavior includes data about signature dynamics, voice

ISSN 2663 - 4023

recognition, keyboard styles, and more. These features ensure the highest accuracy of user identification based on specific biometric data.

Two-factor authentication is a result of the combination of two different one-factor methods, most often these are identification and logical methods. Each class of methods has its advantages and disadvantages. Most authentication methods have one significant drawback, they are not protected against authenticator compromise, that is, the system authenticates not a specific user, but the fact that the subject's authenticator matches their identifier.

ANALYSIS OF AUTHENTICATION AND IDENTIFICATION METHODS AND PROTOCOLS

Identification using an electronic digital signature. Article 1 of the Law of Ukraine "On Electronic Digital Signature" defines the term an electronic digital signature as a type of electronic signature obtained as a result of the cryptographic transformation of a set of electronic data, which is added to this set or is logically combined with it and allows confirming its integrity and identify the signatory. An electronic digital signature is imposed using a private key and verified using a public key [12].

The signature on the paper of the document author is a handwritten, sometimes drawn name or other graphic sign used to identify the author (the signatory) and indicate their agreement with the document content. This type of signature can be verified by visual comparison with the original or, if necessary, by appropriate inspection. Unlike the paper version of the document, various changes can be made to the electronic version. To ensure the control of the signature authenticity on the electronic document, it is necessary to use the corresponding document so that it is possible to determine whether changes have occurred in the electronic document after the signature [13]. Fig. 3 shows the working model of a digital signature.

A signature, both electronic and paper, must have the following properties:

- authenticity of the signature;
- low probability of forging the signature on the document;
- there is a low probability of not detecting a change in the content of the document;
- indisputability of the signature;
- signature recognition, etc.

Imposing a signature on an electronic document by graphically reproducing a handwritten signature cannot serve as confirmation that the document was generated by the signatory. A complete analog of a handwritten signature on documents is an electronic digital signature, such a signature is carried out using of certain cryptographic transformations, based on which the content of this electronic document is reproduced. According to the legislation of Ukraine, an electronic digital signature has the same legal force as a handwritten signature.

ISSN 2663 - 4023

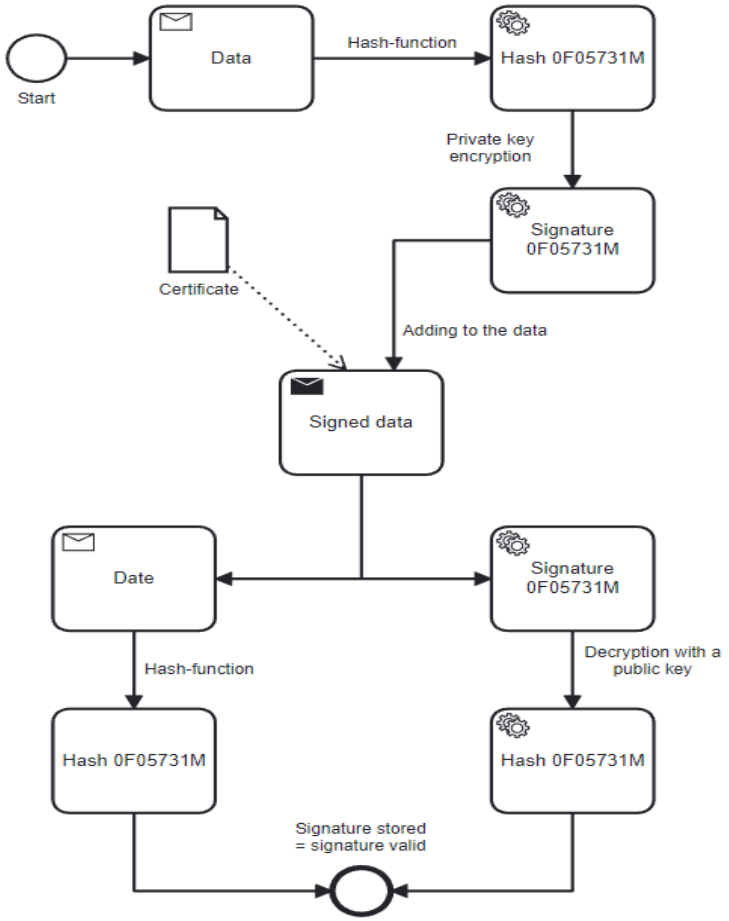

Fig. 3. Modeling of signature and data verification processes [14]

Cryptographic authentication protocols. Cryptographic protocols are a new direction of cryptography that appeared as a result of the successful development of digital signature schemes and open key distribution, the same ideas were also applied to remote subscribers [15].

The classic Shannon model of secret communication has two participants who fully trust each other, they need to share information that is not intended for third parties. It is necessary to protect information from external users. The study object of the theory of cryptographic protocols is remote subscribers who interact, most often, through open communication channels. The purpose of such interaction is to solve a specific secret task. Such a task can be subjected to a cyber-attack, the goal can be a conspiracy of any subscribers. At the same time, the attacker may have various opportunities, for example, to interact with other subscribers, and interfere in the exchange of information between subscribers, and others. Cryptographic protocols must protect users not only from attackers but also from dishonest partners. Differences between cryptographic protocols and cryptosystems:

- users of the protocol do not trust each other;
- there may be more than two users in the agreement;
- the protocol includes multiplex exchange of messages between users.

The basic concepts of cryptographic protocols have not been formulated yet. A protocol is usually understood as a distributed algorithm, which includes:

- a set of algorithms for each participant;
- specification of the format of messages sent between participants;
- specification of synchronization of participants' actions;
- description of actions in case of failure.

ISSN 2663 - 4023

The last item on the list above deserves special attention because it is often ignored, but if used improperly, even a stable cryptographic protocol can completely undermine the security of participants.

All types of cryptographic protocols can be conventionally divided into two groups: application protocols and primitive protocols. Application program protocols solve specific problems that arise in practice. The output protocol is used as a "building block" in the development of the application protocol.

During the last decade, cryptographic protocols have been the main subject of theoretical research in cryptography. One of the main areas of application of cryptographic protocols is banking payment systems, where electronic forms are used instead of paper payment orders. Banks immediately felt the advantages of cryptographic protocols and would not abandon them, despite the technical and cryptographic difficulties, but payment orders are one of the many documents that circulate in the commercial sphere, in particular, with government bodies, public organizations, and others [16].

Justification of stability of asymmetric algorithms in the system. Effective cryptographic protection systems, which are also called public-key cryptosystems, are called asymmetric cryptosystems. The name "asymmetric" comes from the fact that the systems use one key for data encryption and another for decryption. The decryption of the data using the public key is not possible, so the first key is public and can be published for mass use by users who encrypt the data. To decrypt the data, the user has a secret key, this key cannot be determined from the encryption key.

One of the most important achievements of asymmetric encryption is that it allows people who have no prior agreement on security to exchange secret messages. The need to agree on a secret key over a specially protected channel between the sender and the recipient has disappeared.

The stability of most modern asymmetric algorithms is based on two mathematical problems that are difficult to calculate at this stage:

- discrete logarithmization in finite fields;
- divide large numbers into factors.

So far, there is no effective algorithm for solving the above-mentioned problems, or its solution requires the participation of powerful computing systems, resources, and time, and such mathematical problems have found wide application in the construction of asymmetric algorithms.

STUDY OF STABILITY OF AGGREGATED DIGITAL SIGNATURE AT THE EXPENSE OF OTHER AUTHENTICATION METHODS

Analysis of authentication methods and aggregated digital signature. Today, there are two methods of user authentication — one-factor, which, in turn, is divided into password, identification, and biometric, and multi-factor. To analyze the stability of a digital signature, such indicators were introduced [17]:

- recognition by users (degree of human comfort);
- cost (relative economic costs associated with the implementation of the authentication method);
- ease of use (the method of entering information or interacting with the system is taken into account);
- resistance to cyber-attacks and counterfeiting;
- FRR — service failure frequency indicator;

- FAR — false alarm frequency indicator;
- relative time required to serve one user;
- the stability of the method's operation (the indicator of the user's illness and aging is included).

To evaluate authentication methods, eight groups of senior students of the faculty of information technologies with an above-average academic success level was studied. The concordance coefficient for groups was 0.92-0.94. The average age of the interviewees is 23 years old. They have from three to eight years of experience in using various touch devices, for example, a laptop, a tablet, and a smartphone. Survey participants were introduced to single-factor and multi-factor authentication methods.

Due to the situation in the country, the procedure was carried out in compliance with all necessary requirements:

- participants filled out the questionnaire;
- they were familiarized with the purpose and task of the test;
- the time for completing the task for each criterion was limited;
- after completion, participants were interviewed to clarify their opinions on the difference between authentication methods.

Points were distributed within 1–9 for each method and criterion. One point is the worst indicator, nine points is the best indicator. The Saaty method is used to evaluate the best authentication method. The essence of the method is to calculate the Saaty pairwise comparison matrix, the coefficient of priority of alternatives, and the average value of the priority of identified authentication methods for each standard, taking into account all standards at the same time, that is, determining the best method based on multi-criteria analysis. The results of the calculations are given in Table 1 and Fig. 4.

The evaluation results showed that the highest priority coefficient is in the biometric technology of signature recognition, the following indicators, close in value to the best, in fingerprint and iris recognition. Hand geometry recognition has the worst rating.

Different characteristics of the methods have different weights and are perceived differently by the user. Using the Saaty method, the weighting coefficients and the optimal method of authentication were determined taking into account the weighting coefficients. Table 2 shows the numerical value of the priority vector and defines the global priorities.

Fig. 5 shows the authenticity indicators taking into account the weight coeffi-cients.

According to the research results, the dynamic signature method is optimal in terms of the set of criteria based on their significance, the iris and fingerprint authentication methods are close to the optimal value.

Table 1

Analysis of authentication indicators

Alternatives	Recognition by users	Cost	Ease of use	Resistance to cyber-attacks and counterfeiting	FAR	FRR	User recognition time	Stability of the method
Signature dynamics	7	7	8	4	7	8	9	5
Face geometry	8	7	8	4	5	1	8	2
Geometry of the hand	6	4	6	2	6	5	7	4
Voice	9	9	9	3	5	3	4	3
Iris	3	7	4	6	7	7	5	8
Fingerprint	4	6	8	8	5	5	5	8

ISSN 2663 - 4023

Analysis of authentication indicators

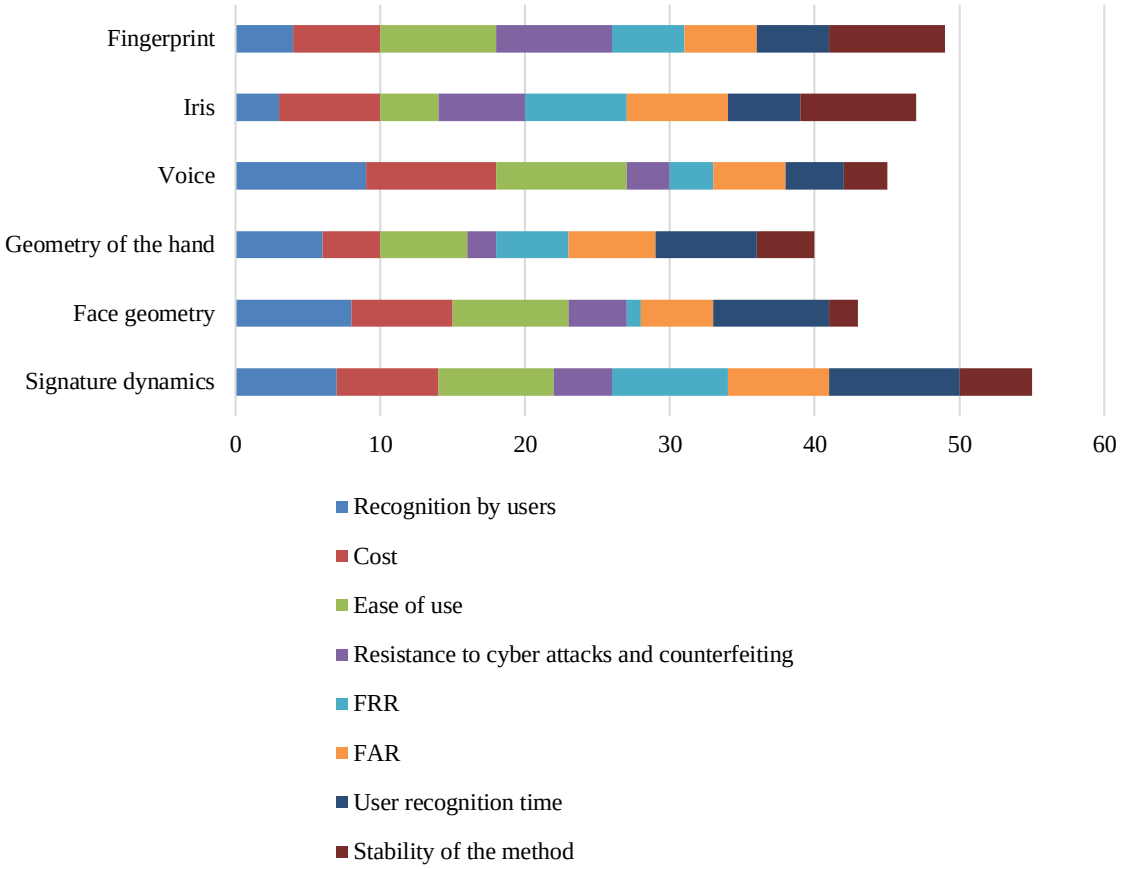

Fig. 4. Analysis of authentication indicators

Table 2

Determination of weighting factors using the Saaty method

Alternatives	Recognition by users	Cost	Ease of use	Resistance to cyber attacks and counterfeiting	FAR	FRR	User recognition time	Stability of the method	Global priorities
	The numeric value of the priority vector								
	0,044	0,086	0,197	0,064	0,055	0,176	0,094	0,047	
Signature dynamics	0,222	0,372	0,266	0,276	0,243	0,230	0,373	0,186	0,21
Face geometry	0,138	0,126	0,246	0,101	0,134	0,219	0,265	0,141	0,15
Geometry of the hand	0,105	0,134	0,111	0,146	0,180	0,240	0,211	0,118	0,13
Voice	0,102	0,135	0,143	0,127	0,639	0,237	0,206	0,169	0,16
Iris	0,234	0,187	0,161	0,133	0,215	0,227	0,286	0,296	0,16
Fingerprint	0,301	0,191	0,216	0,345	0,227	0,238	0,319	0,238	0,19

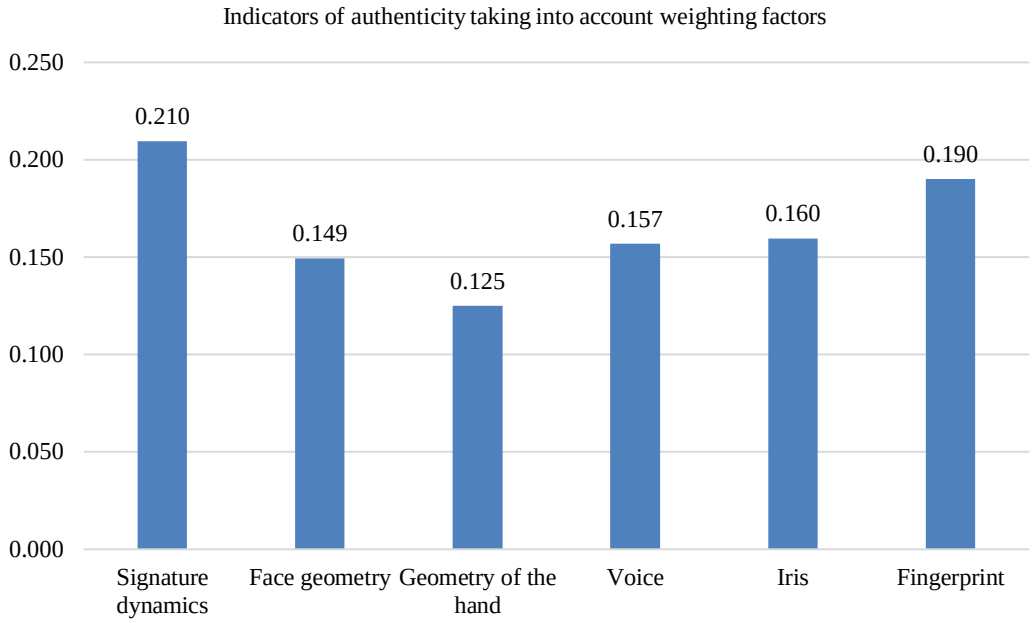

Fig. 5. Indicators of authenticity taking into account weighting factors

Improving the cryptographic stability of the electronic signature to the extent of the RSA algorithm. In the 1970s, people became increasingly interested in cryptography, so it was widely popular and used in cryptosystems. The RSA algorithm has encryption properties typical of symmetric encryption systems.

In symmetric cryptography, one key is used for encryption and decryption. These algorithms are simple and were described as far back as the 1950s, but such algorithms have a major drawback — they require a secure channel to transmit the encryption key. Decryption is the reverse process of encryption, based on which the encrypted text is transformed into the original text [18].

Another encryption method uses a pair of keys: on and off (secret). Public and private keys allow cryptographic algorithms to encrypt and decrypt messages, but you can encrypt with a public key and only decrypt with a private key. The public key is available when the client connects and is published in the owner's certificate, while the private key is stored only by the owner of the certificate. It is impossible to choose a private or public key at random because they are related by mathematical dependencies. With the help of electronic digital signatures, it is possible to check whether the information was not distorted during encryption.

In this case, the text encrypted with the private key is sent to the sender along with the public key. Decryption succeeds if the text matches the unencrypted during encryption with the public key. In practice, the hash function of a document is usually encrypted with a private key. An electronic signature also includes a public key certificate issued by a trusted certification authority that contains all public keys and their user data. Of course, the certificate must also be signed, and the public key of the trusted center must be known in advance, as it can also be forged.

RSA algorithm, which is based on exponentiation using modular arithmetic. The RSA algorithm can be expressed as the following sequence to obtain the encryption key:

$$n = pq, \tag{1}$$

where p and q are two prime numbers.

Let's choose three options for the values of p and q, and calculate the parameters of the locked and unlocked key, respectively (Table 3).

ISSN 2663 - 4023

Table 3

Calculated encryption keys

Calculated encryption keys		
Parameters p and q	**Public key**	**Closed key**
24,65	26,1560	1189,1560
123,186	247,22878	14803,22878
1763,7692	875,13560996	11569145,1356099

The Cryptool 2.0 program currently supports all known encryption models [19]. Functional blocks have modules that input and output information during operation, which, in turn, can connect to other functional blocks and exchange information with each other. Each block has a scene for manipulation and virtualization. This allows you to run a job simulation after developing the entire scenario. Calculated data is entered into the program and encrypted. The obtained results of the research of algorithms are given in Tables 4–6.

Table 4

Encryption for the first set of keys

Values for encryption with the first set of keys (26,1560;1189,1560)	
Hash-function algorithm	**Number of characters**
RSA	209
MD5	92
SHA-1	119
SHA-256	191

Table 5

Encryption for the second set of keys

Values for encryption with the first set of keys (247,22878;14803,22878)	
Hash-function algorithm	**Number of characters**
RSA	210
MD5	95
SHA-1	121
SHA-256	192

Table 6

Encryption for the third set of keys

Values for encryption with the first set of keys (875,13560996;11569145,1356099)	
Hash-function algorithm	**Number of characters**
RSA	161
MD5	71
SHA-1	89
SHA-256	143

Comparing the obtained results shows that the RSA algorithm using SHA-256 re-ceives the biggest changes.

Tables 4, 5, and 6 show that the RSA algorithm using SHA-256 changes mostly with increasing key size. In case of limited computer memory, it is most appropriate to use the RSA + MD5 hash function. When using the RSA algorithm, the resulting encrypted text is 10 times larger than the original but less stable. Electronic signatures contain public key

certificates, which have information about all public keys and their users, that is, with an increase in the size of the encryption key, the validity period of the system and electronic signature increases.

CONCLUSION

So, in the course of the study, the main methods of user identification and authentication in the system were considered. Authentication methods were investigated: single-factor (password, identification, and biometric) and multi-factor ones. An analysis of the properties of a digital signature was carried out (it was established that a digital signature has the same properties as a paper one, namely: authenticity of the signature, low probability of forgery, as well as non-repudiation and recognition of the signature), and cryptographic authentication protocols (conventionally, cryptographic protocols are divided into two types: primitive and applied, applied represent a protocol that solves a specific problem, and primitive protocols are used as "building blocks" in the development of applied protocols).

A multi-criteria analysis of authentication methods was conducted, the results of which showed that the method of dynamic digital signature is better than all traditional methods of authentication and identification of a person. This method has an acceptable level of probability of errors of the first and second kinds. The advantages of this method are that the characteristics used to recognize a digital signature are almost impossible to copy, and verification is quite fast. This method is familiar to a person, as it is the most common and generally recognized way of confirming one's identity.

In addition, a study was conducted on the stability of the electronic signature due to the RSA algorithm. Since the electronic signature contains a public key certificate, we can say that the larger size of the encryption key will ensure greater reliability of the system and the electronic digital signature.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Xuerui, W., et al. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications, 188*. https://doi.org/10.1016/j.jnca.2021.103080
2. Shen, X., Lin, X., & Zhang, K. (2020). User Authentication. *Encyclopedia of Wireless Networks*, 1–4. . https://doi.org/10.1007/978-3-319-78262-1_300683
3. Pant, M., et al. (2021). User Authentication in Big Data. Soft Computing: *Theories and Applications 1053*, 1–9. https://doi.org/10.1007/978-981-15-0751-9_36
4. Murray, H., & Malone, D. (2021). Quantum Multi-factor Authentication. *Emerging Technologies for Authorization and Authentication 13136*, 50–67. https://doi.org/10.1007/978-3-030-93747-8_4
5. Chia, J., Chin, J., & Yip, S. (2021). Pluggable Authentication Module Meets Identity-Based Identification. *Advances in Cyber Security 1487*, 155–175. https://doi.org/10.1007/978-981-16-8059-5_10
6. Tolbert, M., et al. (2022). Exploring Phone-Based Authentication Vulnerabilities in Single Sign-On Systems. *Information and Communications Security 13407*, 184–200. https://doi.org/10.1007/978-3-031-15777-6_11
7. Komarova, A., et al. (2018). Comparison of Authentication Methods on Web Resources. *In: Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry", 679*. https://doi.org/10.1007/978-3-319-68321-8_11
8. Jain, J. (2022). Authentication. *Learn API Testing*, 31–39. https://doi.org/10.1007/978-1-4842-8142-0_3
9. Patel, S., et al. (2021). Survey on Graphical Password Authentication System. *Data Intelligence and Cognitive Informatics. Algorithms for Intelligent Systems*, 699–708. https://doi.org/10.1007/978-981-15-8530-2_55
10. Zaixing, Ch., & Shaofei, W. (2022). Research on Digital Identity Authentication Technology Based On Block Chain. *Journal of Physics: Conference Series, 1802*, 7–9. https://doi.org/10.1088/1742-6596/1802/3/032091

11. Boonkrong, S. (2021). Biometric Authentication. *Authentication and Access Control*, 107–132. https://doi.org/10.1007/978-1-4842-6570-3_5
12. On electronic digital signature, Law of Ukraine No.852-IV (2018) (Ukraine). https://zakon.rada.gov.ua/laws/show/852-15#Text, last accessed 2022/09/23
13. Sagar Hossen, M., (2021). Digital Signature Authentication Using Asymmetric Key Cryptography with Different Byte Number. *Evolutionary Computing and Mobile Sustainable Networks*, *53*. https://doi.org/10.1007/978-981-15-5258-8_78
14. Metyolkin A., & Kardashuk V. (2018). Research methods to improve cryptographic stability. *Bulletin of Volodymyr Dahl East Ukrainian National University, 6(247)*, 90–95.
15. Ravi, P., et al. (2021). Arvind Easwaran Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography. *In: International Symposium on Circuits and Systems (ISCAS)*, 1–5. https://doi.org/10.1109/ISCAS45731.2020.9180847
16. Boyd, C., Mathuria, A., & Stebila, D. (2019). Authentication and Key Transport Using Public Key Cryptography. *Protocols for Authentication and Key*, 135–164. https://doi.org/10.1007/978-3-662-58146-9_4
17. Carminati, B. (2018). Digital Signatures. *Encyclopedia of Database Systems*, 1093–1099. https://doi.org/10.1007/978-1-4614-8265-9_131
18. Thiagarajan, K., et al. (2018). Encryption and decryption algorithm using algebraic matrix approach. *Journal of Physics: Conference Series*, *1000*, 2–3. https://doi.org/10.1088/1742-6596/1000/1/012148

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Чубаєвський Віталій Іванович
доктор економічних наук, доцент, професор кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Луцька Наталія Миколаївна
доктор технічних наук, доцент, професор кафедри автоматизації та комп'ютерних технологій систем управління
Національний університет харчових технологій, Київ, Україна
ORCID 0000-0001-8593-0431
lutskanm2017@gmail.com

Савченко Тетяна Віталіївна
кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0002-8884-5360
sv_t@ukr.net

Власенко Лідія Олександрівна
кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Синельник Кирило Ігорович
здобувач освітнього ступеню магістр кафедри комп'ютерних наук та інформаційних систем
Державний торговельно-економічний університет, Київ, Україна
ORCID 0000-0003-4083-0255
synelnik@knute.edu.ua

ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ АГРЕГОВАНОГО ЦИФРОВОГО ПІДПИСУ ЗА РАХУНОК КОМБІНОВАНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ

Анотація. У цій статті розглянуті механізми, методи ідентифікації та автентифікації користувача; криптографічні протоколи автентифікації; виконаний аналіз за найбільш розповсюдженими показниками автентифікації; визначено найбільш доцільний спосіб автентифікації — за допомогою цифрового підпису; проаналізована криптографічна стійкість цифрового підпису за рахунок RSA алгоритму.

Ключові слова: ідентифікація; автентифікація; користувач; цифровий підпис; криптографічна стійкість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Xuerui, W., et al. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications, 188*. https://doi.org/10.1016/j.jnca.2021.103080
2. Shen, X., Lin, X., & Zhang, K. (2020). User Authentication. *Encyclopedia of Wireless Networks*, 1–4. . https://doi.org/10.1007/978-3-319-78262-1_300683
3. Pant, M., et al. (2021). User Authentication in Big Data. Soft Computing: *Theories and Applications 1053*, 1–9. https://doi.org/10.1007/978-981-15-0751-9_36
4. Murray, H., & Malone, D. (2021). Quantum Multi-factor Authentication. *Emerging Technologies for Authorization and Authentication 13136*, 50–67. https://doi.org/10.1007/978-3-030-93747-8_4
5. Chia, J., Chin, J., & Yip, S. (2021). Pluggable Authentication Module Meets Identity-Based Identification. *Advances in Cyber Security 1487*, 155–175. https://doi.org/10.1007/978-981-16-8059-5_10

6. Tolbert, M., et al. (2022). Exploring Phone-Based Authentication Vulnerabilities in Single Sign-On Systems. *Information and Communications Security 13407*, 184–200. https://doi.org/10.1007/978-3-031-15777-6_11
7. Komarova, A., et al. (2018). Comparison of Authentication Methods on Web Resources. *In: Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry", 679*. https://doi.org/10.1007/978-3-319-68321-8_11
8. Jain, J. (2022). Authentication. *Learn API Testing*, 31–39. https://doi.org/10.1007/978-1-4842-8142-0_3
9. Patel, S., et al. (2021). Survey on Graphical Password Authentication System. *Data Intelligence and Cognitive Informatics. Algorithms for Intelligent Systems*, 699–708. https://doi.org/10.1007/978-981-15-8530-2_55
10. Zaixing, Ch., & Shaofei, W. (2022). Research on Digital Identity Authentication Technology Based On Block Chain. *Journal of Physics: Conference Series, 1802*, 7–9. https://doi.org/10.1088/1742-6596/1802/3/032091
11. Boonkrong, S. (2021). Biometric Authentication. *Authentication and Access Control*, 107–132. https://doi.org/10.1007/978-1-4842-6570-3_5
12. On electronic digital signature, Law of Ukraine No.852-IV (2018) (Ukraine). https://zakon.rada.gov.ua/laws/show/852-15#Text, last accessed 2022/09/23
13. Sagar Hossen, M., (2021). Digital Signature Authentication Using Asymmetric Key Cryptography with Different Byte Number. *Evolutionary Computing and Mobile Sustainable Networks, 53*. https://doi.org/10.1007/978-981-15-5258-8_78
14. Metyolkin A., & Kardashuk V. (2018). Research methods to improve cryptographic stability. *Bulletin of Volodymyr Dahl East Ukrainian National University, 6(247)*, 90–95.
15. Ravi, P., et al. (2021). Arvind Easwaran Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography. *In: International Symposium on Circuits and Systems (ISCAS)*, 1–5. https://doi.org/10.1109/ISCAS45731.2020.9180847
16. Boyd, C., Mathuria, A., & Stebila, D. (2019). Authentication and Key Transport Using Public Key Cryptography. *Protocols for Authentication and Key*, 135–164. https://doi.org/10.1007/978-3-662-58146-9_4
17. Carminati, B. (2018). Digital Signatures. *Encyclopedia of Database Systems*, 1093–1099. https://doi.org/10.1007/978-1-4614-8265-9_131
18. Thiagarajan, K., et al. (2018). Encryption and decryption algorithm using algebraic matrix approach. *Journal of Physics: Conference Series, 1000*, 2–3. https://doi.org/10.1088/1742-6596/1000/1/012148