Type of the Paper: Original scientific paper
Received: 14. 02. 2022
Accepted: 6. 11. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.2
UDK:

Protection and security risk management, a proposal of cryptologic measures and solutions for Vesimpex company

Ivan Jovanović [1], Milosav Majstorović [1] and Hana Stefanović [1*]

[1] Information Technology School – ITS, Belgrade, Serbia; ivan59218@its.edu.rs; milosav.majstorovic@its.edu.rs
[*] hana.stefanovic@its.edu.rs; +381 (0)63/84-97-189

Summary: The subject of this paper comprises the creation of an associative concept network in the realm of security management, and the application of cryptography through secondary research, along with perceiving the importance of security in a concrete organisation through primary research. The objective is to formulate, based on the analysis of a specific company, a proposal regarding security and cryptology measures to advance the security system of a company. The basic principles of information security of small and medium-sized enterprises, along with the application of adequate security algorithms based on a one-time pad (OTP) and visual cryptography (VC) are utilised for the design of a complete solution for the company in question. Alongside its theoretical foundation, the paper contains information about the company itself, collected through observation, note-taking and content analysis, as well as the process of creating the security solution incorporated into the project charter, and the solution itself.

Keywords: small and medium-sized enterprises (SMEs); security solutions; competitive advantage; one-time pad (OTP); visual cryptography (VC)

1. Introduction

The information age and digitalisation have contributed to a considerable advancement of all forms of business, but they have also rendered information easily accessible, which is a potential threat to the security of the business system itself [1]. In a very fierce competitive race on the market, the protection of information has become indispensable [2], as various types of breaches may take place – internal, external or incidental, increasingly perpetrated through the abuse of new technology [3][4]. Reliable security systems considerably lower the risk of information leaks [5] which can be fatal for a company.

Vesimpex is a small enterprise operating in the realm of electrical equipment and solutions, including original solutions in power distribution [6]. The company works with a number of successful companies in different branches of industry, and the issue of information security and reliability is exceedingly important. In such an environment, advanced security can give the company an advantage over its often disloyal competition [7]. To provide security from various attacks, one must analyse the existing state and the level of employees' expertise and, accordingly, formulate a proposal for forming a security system for the small enterprise in question.

The subject of this paper's research is multidisciplinary and has to do with the disciplines of business economics, project management, security and cryptography. The central motive is to formulate a concrete solution on a practical example, by analysing the security characteristics of the company. The purpose of this research is to find adequate ways to realise the formulated goals in order to ensure that the security criteria are realised.

The primary objective of this applied research is to provide a solution to a specific security problem and ensure a competitive advantage for the Vesimpex company [6]. The secondary objective is to study the existing and introduce new cryptologic protection measures to increase the security of the business.

As the modern way of doing business, based primarily on the utilisation of computer systems and the exchange of data in electronic form, is exposed to various risks with potentially catastrophic consequences, it is necessary to analyse and prevent the increasingly frequent attacks on computer networks, attempts at unauthorised data access, tapping, and malicious data exchange [8]. This requires the implementation of new forms of communication, made possible by the advancements in technology. The problem of security necessitates the need for the introduction of new mechanisms that should assume the role formerly played by the traditional solutions for the purposes of efficient identification, access control and verification. Most of these challenges can be resolved through the use of cryptographic solutions [9], although there are problems that cannot be adequately solved by cryptography alone.

Cryptography studies various techniques of transformation of transferred data so that the meaning of the data is accessible only to authorised parties in communication. At the same time, said transformation ought to be such that unauthorised parties in communication who come into possession of the transformed message should be unable to access the initial data.
There are a large number of traditional and modern cryptography algorithms, those that use the same key for encryption and description, as well as the asymmetric ones, which use different keys for encryption and decryption. For any cipher, those with symmetric and asymmetric algorithms alike, the crucial issue is the security of the cipher [10][11].

An unconditionally secure cipher is a cipher that ensures that, without the knowledge of the key, not even a full search of the keys can result in accessing the plaintext from the ciphertext. A comprehensive search (with no limitations regarding time and available resources) can encounter the key, but it is not in the attacker's interest to have it accomplished after several decades or even centuries. However, even assuming that the attacker has the best possible equipment and resources, an unconditionally secure password ought to ensure that the attacker does not come into possession of plaintext, not even in ideal conditions. The basic idea behind an unconditionally secure password is to ensure that a comprehensive search of potential keys, which are sure to generate a large number of messages, should not enable the attacker to determine which one is the right one. Through an exhaustive search, the attacker will get a large number of nonsensical messages, which will be discarded, along with a certain number of messages that make sense, and if the latter messages are equally probable, the attacker should have no way of determining which one is right.

A one-time pad – OTP [12], used in this paper, is an unconditionally secure cipher. Simulation models that illustrate the basic principles of OTP algorithms have been realised in CrypTool software [13], with an emphasis on the case of repeated use of a one-time key. We also include an example of processing an electronic financial transaction using OTP, where confidential information is shared using the visual cryptography technique [14][15].

2. Materials and methods

The work on this paper included the use of a number of scientific and professional methods, techniques and tools, with a research plan that included:

- Defining the subject of the research (through formulating the research problem);
- Defining the research objectives;
- An overview of relevant literature and making a selection of literature for use in the research;
- Determining the theoretical framework of the research (in accordance with the relevant disciplines and the selection of relevant literature);
- Situational analysis;
- Examining the target group through polling;
- Statistical analysis of data from the poll;
- Designing and making the security solution.

The main hypothesis of the study:

H1: The level of information security at Vesimplex is not optimal; it needs to be elevated through a new security solution, considering the elements from the environment and the desired growth and development as an organisational goal.

H2: An adequate advancement of the company's information security would ensure its competitive advantage.

The outcomes of the research, that is, the anticipated results of the research, include analysis of the selected literature and other references, proving the hypotheses and solving the central problem of the research through the selected model. From the professional relevance standpoint, the proposed solution would further advance the business and the security of the observed company, elevating the security of the business, as well as the security of the partners involved (suppliers, and clients). The social justification of this research concerns the awareness of the importance of information security and the optimisation of the level of security of the companies in the country.

3. Results

The results presented in this chapter constitute a concrete solution for the security system of the company, which, although it is already at an acceptable level, still leaves a lot of room for improvement. The major upgrades concern the realm of transactions and the storage of confidential information, such as employees' passwords.

Having provided a secure channel and method of transferring confidential information, we propose that confidential data, such as employees' passwords, should be secured by a random salt value before determining the hash value, to provide additional security in case of an attack.

3.1. Sharing confidential information during transactions

For electronic financial transactions, the technique of expanding the pixels of the original digital image containing a one-time PIN code was used. The encryption and decryption processes are fairly simple, and provide high security, as the proposed visual cryptography technique relies upon a one-time pad algorithm.

Visual cryptography is a cryptology technique that provides the hiding of information, i.e. secret messages so that they can be decrypted at reception without using a computer or performing any other type of calculation [12]. The decryption procedure uses solely human visual perception. This technique was first proposed at the EUROCRYPT conference, by Noni Naor and Adi Shamir. Its encryption and decryption systems are fairly simple and can be used for sharing different types of information, especially in financial transactions over the internet, as well as for verifying ballots, securities, etc.

The algorithm for dividing the original image into layers (share images) was realised in the Visual Studio C# programming environment. Both layers have the same resolution and their overlaying results in the unveiling of the secret message [16]. A simple pixel expansion variant was selected, achieved by random generation on one layer, whereas the second layer with complementary pixels, after visual XORing with the first one (using the exclusive or operation – XOR) provides information (secret message) upon overlaying. Since the values representing pixels on the first layer are randomly generated, this technique can be viewed as a variant of one-time pad encryption, with good security properties.

Transparent images (layer 1 and layer 2) are shown in Fig. 1, with the first layer containing randomly generated expanded values of pixels, and this image constitutes the key. Each pixel is represented by a block which always contains the same number of white and black pixels. If the simpler pixel expansion model is used, a pixel will always be represented by one white pixel and one black pixel, and if the more complex expansion model is used, a pixel will be represented by four new pixels – two white ones and two black ones. A pixel in layer 1 has a certain state, whereas a pixel in layer 2 can have the same state or the opposite state. If the states in layers 1 and layer 2 are the same, the overlaying results in one-half of white and one-half of black pixels, which the human eye will register as a shade of grey, and if the states in layer 1 and layer 2 are opposite, the overlaying yields black pixels, which will be detected by the human eye as the colour black. Overlaying ■□ with an identical block in layer 2 results in a bright pixel (shade of grey), while overlapping ■□ with □■ results in a black pixel. The case with expansion by a four-pixel block for each original pixel is similar: overlaying ■■ with the same block in layer 2 results in a shade of grey, while overlaying ■■ with ■■ results in a black block. Layer 1 contains pixels whose values are determined randomly, which is identical to the procedure for generating a key for a one-time pad cipher, while layer 2 contains fixed blocks that carry information in the overlay phase. The result of overlaying layers is shown in Fig. 1, after layers 1 and 2.

There are also more complex schemes in visual cryptography, and some do not involve the pixel expansion model, in the sense of representing the original pixel by a group of subpixels, while some involve additional techniques for improving the contrast in the decoded image [17][18]. Fig. 2 shows an example of using several generated layers based on which the decoded image is formed.

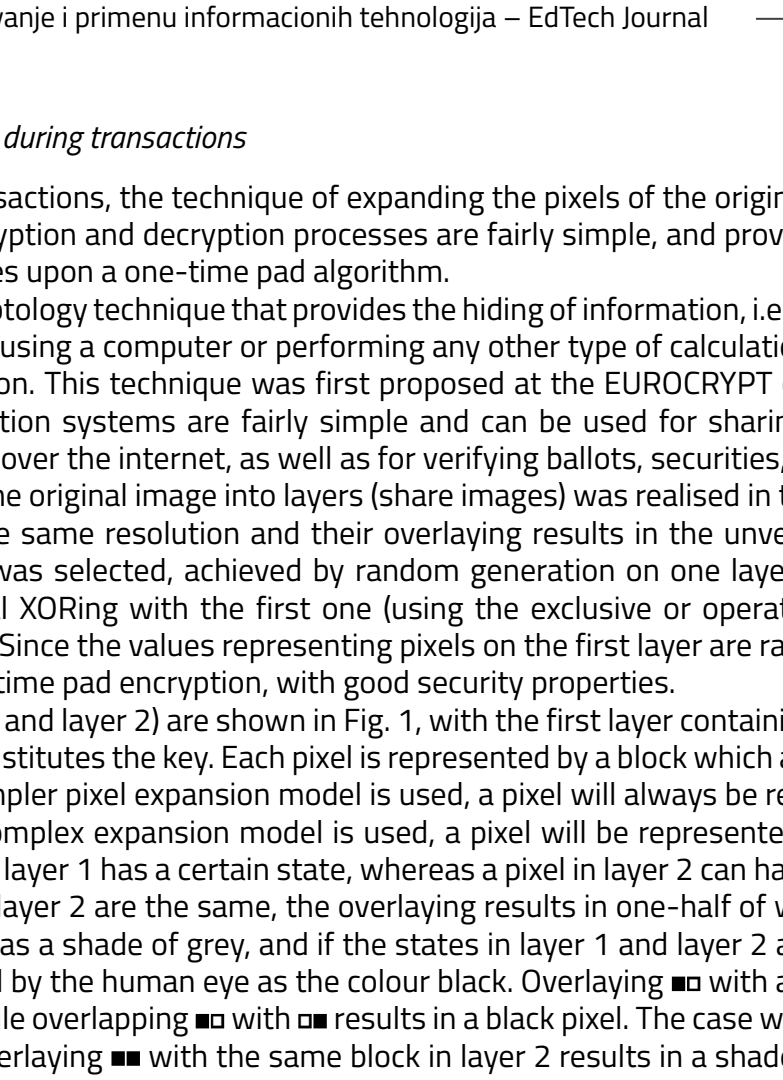

Figure 1. Acquiring the decoded image based on layers 1 and 2

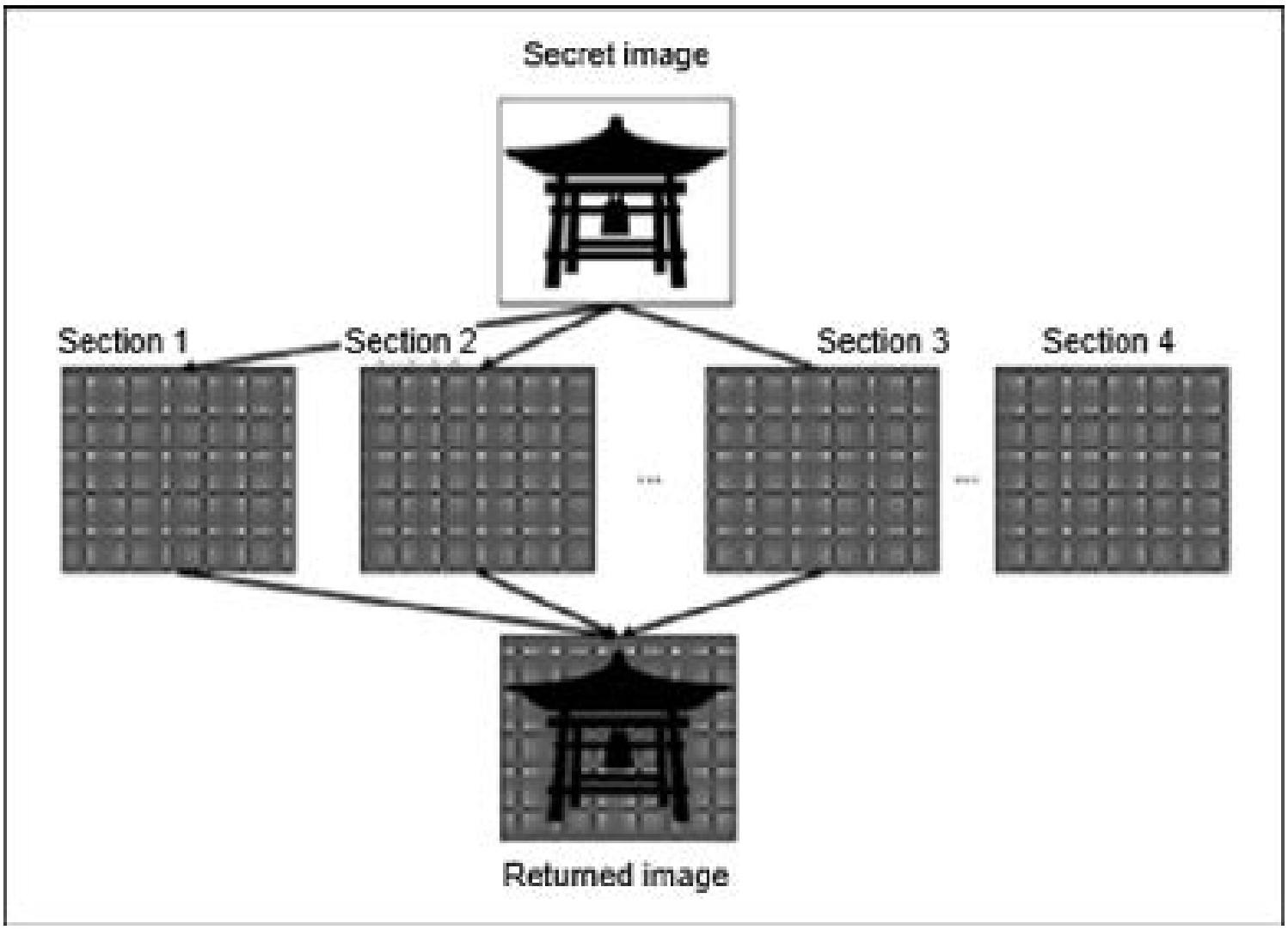

Figure 2. Acquiring the decoded image based on four layers (sections)

3.2. The basic principles of a one-time pad algorithm

Prior to the encoding procedure, the message needs to be represented by a binary sequence based on the defined code. This should be followed by another binary sequence, of the same length as the message itself, which will represent the key. This sequence would have the properties of a random sequence. During the encryption procedure, each bit of the plaintext p_i is added, using modulo 2 (XOR operation), with one bit of the key k_i, to get the relevant bit of the ciphertext c_i [8][19]:

$$c_i = p_i \oplus k_i \tag{1}$$

In the decoding procedure, each bit of the ciphertext is added, using modulo 2, with the same bit of the key which was used for encryption, which, according to the properties of the XOR operation, yields the original text:

$$p_i = c_i \oplus k_i \tag{2}$$

The simulation model, created in CrypTool software, which shows the process of encryption and decryption of the plaintext ("My message!") using OTP, is shown in Fig. 3. The key which was used is written in hexadecimal format in the lower left corner, while the decoded message is shown in the lower right corner.

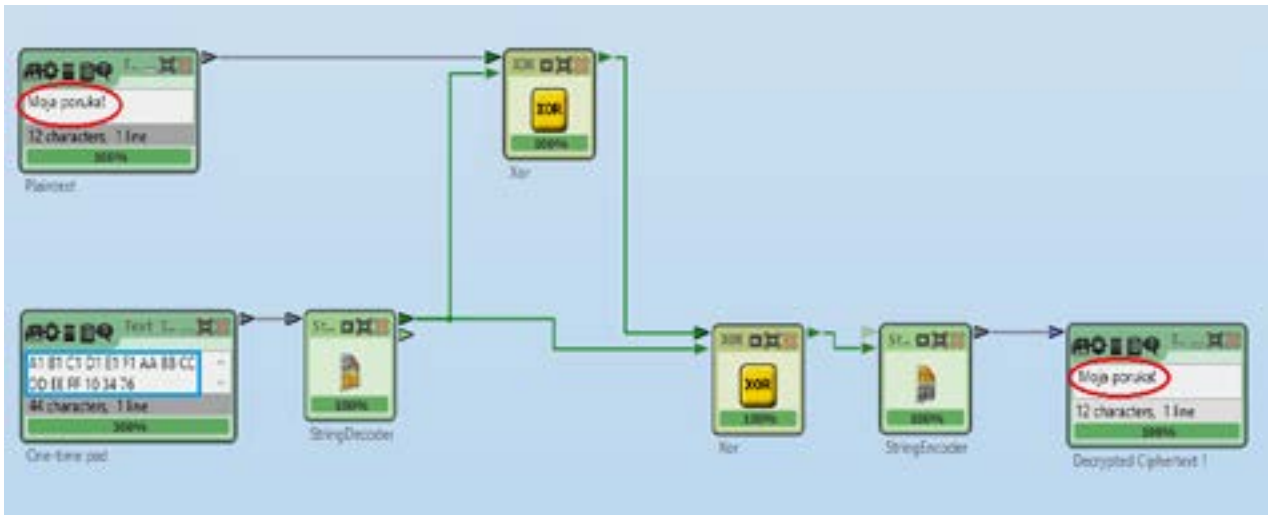

Figure 3. Simulation model illustrating the encryption and decryption procedure for plaintext ("My message!") using OTP

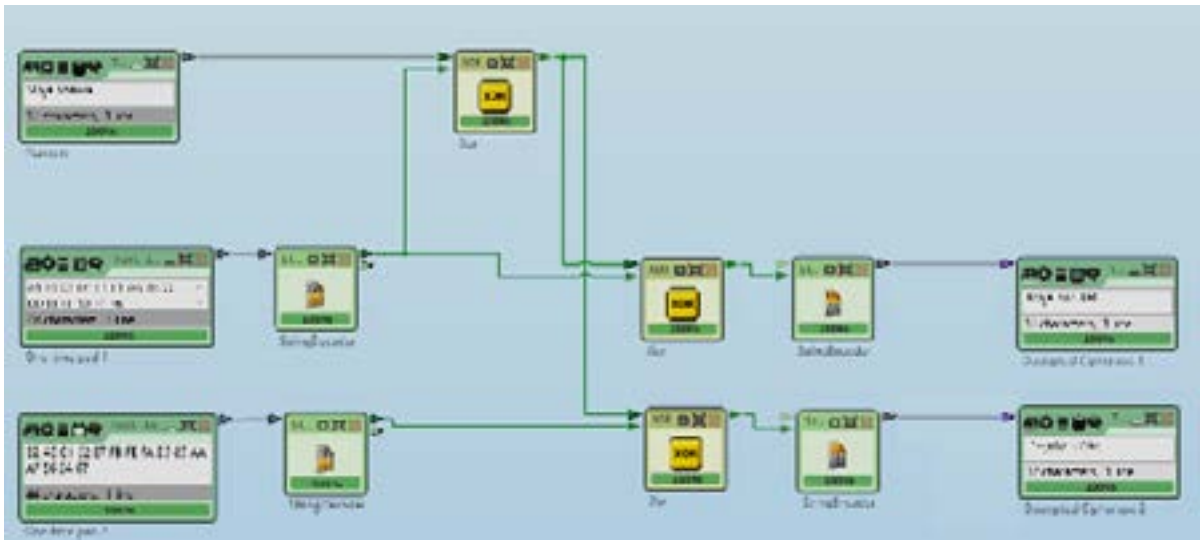

Figure 4. Simulation model showing the procedure of a search for potential keys

Searching the potential keys, the attacker generates a large number of messages, some of which will be nonsensical, as shown in Fig. 4. The attacker will discard such messages, but he will surely also generate a certain number of sensible ones. If all these messages are equally probable, the attacker has no way of ascertaining which one of them is real.

The security of an OTP algorithm is based on the randomness of the key. There is no exact definition for randomness, but from the cryptography standpoint, there are two basic characteristics of a binary random key:

» Unpredictability: Regardless of the number of known bytes of the key, the probability of guessing the next bite must not exceed ½. The chance of the next bit being 1 or 0 is exactly ½.

» Balance: The number of 1s and 0s must be approximately the same, in a sufficiently long sequence.

3.3. Weaknesses of the algorithm due to multiple uses of the same key

If the key is a random binary sequence, the probability of any bit of the key having the value of logic one is the same as the probability of that bit having the value of logic zero: it is ½. However, plaintext has certain statistical properties and the probability of the occurrence of logic ones and zeroes is not the same.

The simulation model that illustrates the use of the same OTP key in the process of encoding two different messages is shown in Fig. 5. To illustrate plaintext, we chose a digital image, to provide a visual representation of multiple uses of the same OTP key. XORing ciphertext CA and CB yields:

$$C_A \oplus C_B = (A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \oplus 0 = A \oplus B \quad (3)$$

The consequence of these properties is that an inventive attacker, after XORing the ciphertext, although unfamiliar with the key K, actually discovers a lot about the original messages, which is the reason why multiple uses of the same OTP key is not recommended. The result shown in the lower right corner of Fig. 5 reveals a lot about the original images, which is a consequence of the aforementioned properties of XOR operation [20].

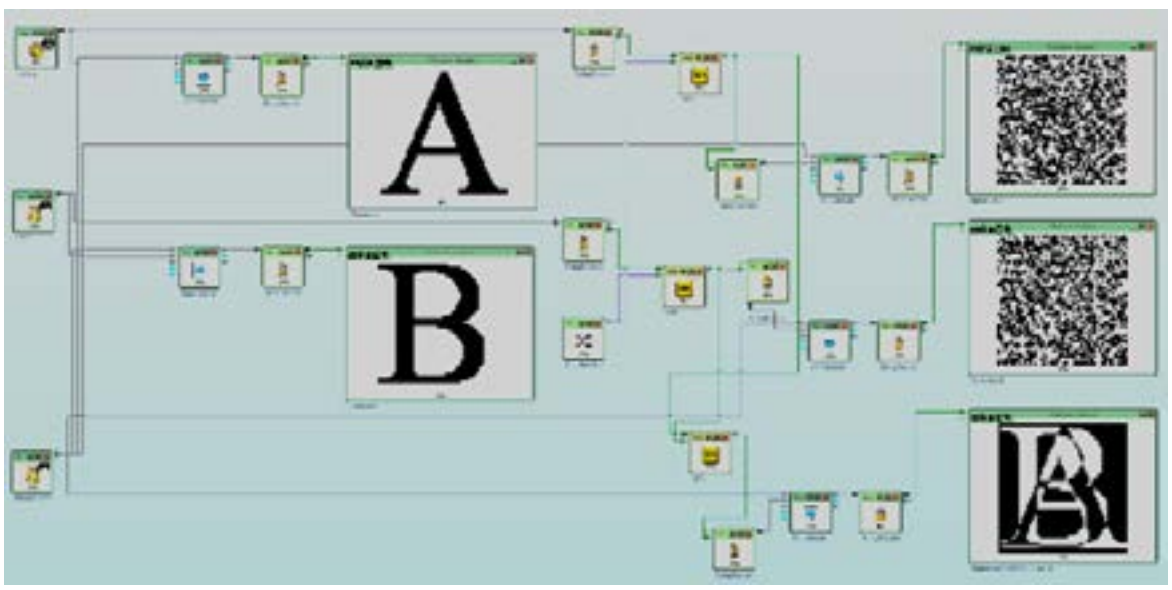

Figure 5. Simulation model illustrating multiple uses of the same OTP key

3.4. An example of an electronic financial transaction using the OTP algorithm

Usually, all it takes to log in to e-banking applications, which are widely used in corporate and private financial transactions, is the serial number of the token or m-token. The user does not reveal the PIN for the token or m-token, and of course, it is recommended that the PIN should be kept separately from the token or m-token.

The bank does not require a one-time password or transaction signing data [21]. The process of creating a request for a one-time password is shown in the upper left part of Fig. 6, while the generated password sent to the user's mobile device is shown on the right.

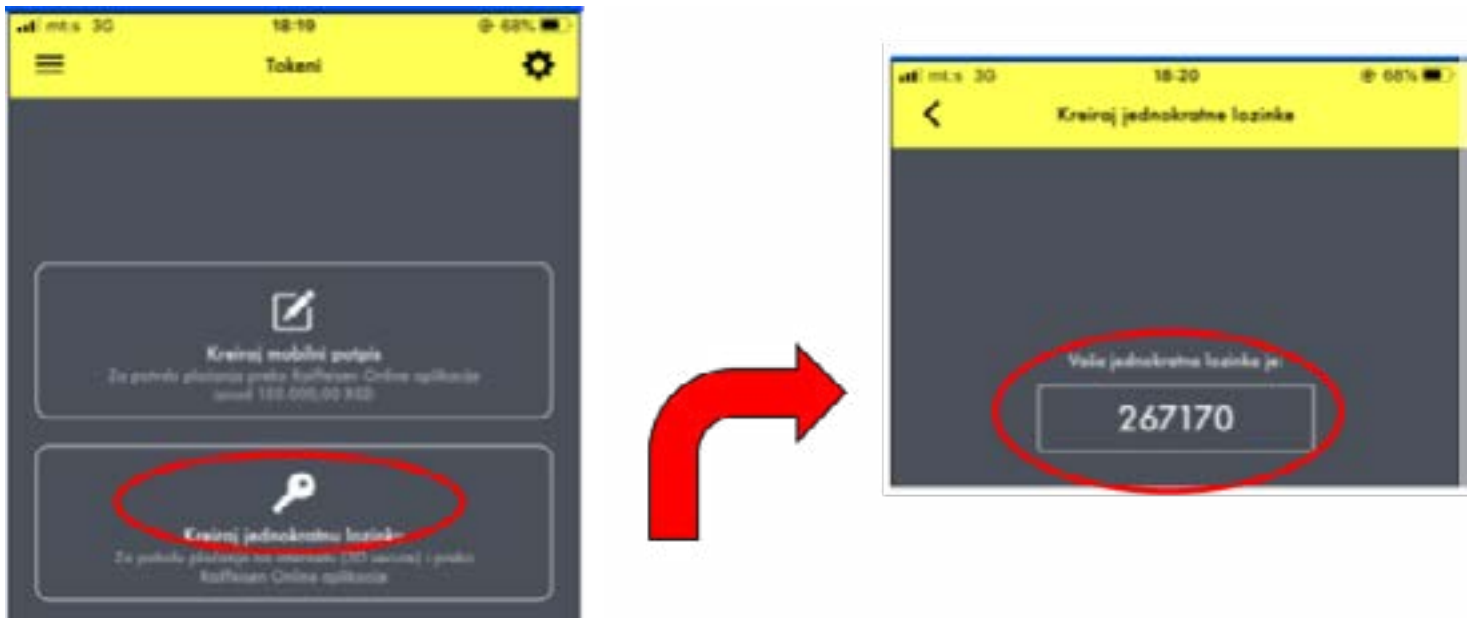

Figure 6. Creating a request for generating a one-time password and sending the password to the user's mobile device

The information about the validity period of the password is also sent to the user, as shown in Fig. 7, along with some additional information about the token. The duration of the password, sent to the user after synchronising with server time, is shown on the left in Fig. 7; it is 5 minutes. Additional information about the token (Token info) showing the serial number and the UTC time is shown on the right in Fig. 7.

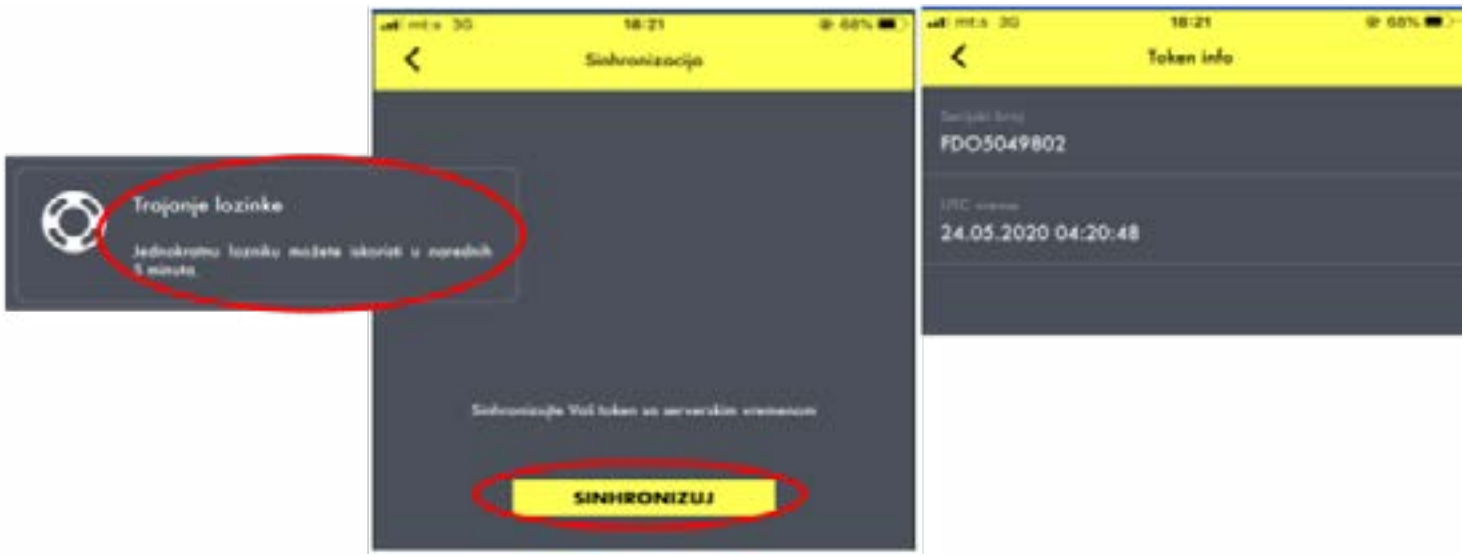

Figure 7. Information about the validity period of the password

3.4. Proposal for storing employees' passwords using hash functions and adding a random salt value

After providing a secure channel and mode of transmission of confidential information, passwords must be kept in a way that prevents the attacker from obtaining them even if the application or the database is compromised. Most modern languages and frameworks provide built-in functionality for the secure storing of passwords.

Hashing and encryption are two different ways of storing sensitive data. In almost any circumstance, it is preferable that passwords should be stored as hash values, not as encrypted data [22]. The hash function is a one-way function, which means that it is practically impossible to obtain the original information based on the hash value.

If the attacker came into possession of a password's hash value, he would be unable to acquire the original data, i.e. the content of the password. Older hash algorithms, such as MD5, have been found to be vulnerable to collisions, and the use of newer generation algorithms (later generation SHA) is recommended.

A cryptographic hash function is a one-way function which, for input data (message, file…) of any final length, returns the same length "hash". Besides providing compression, a hash function must be efficient, one-way and collision-proof.

The application of the SHA algorithm when determining the hash value of the password (content "my secret password") is shown in Fig. 8, while the model that includes the addition of a random salt value is shown in Fig. 9. The models shown in Fig. 8 and Fig. 9 were created in CrypTool software.

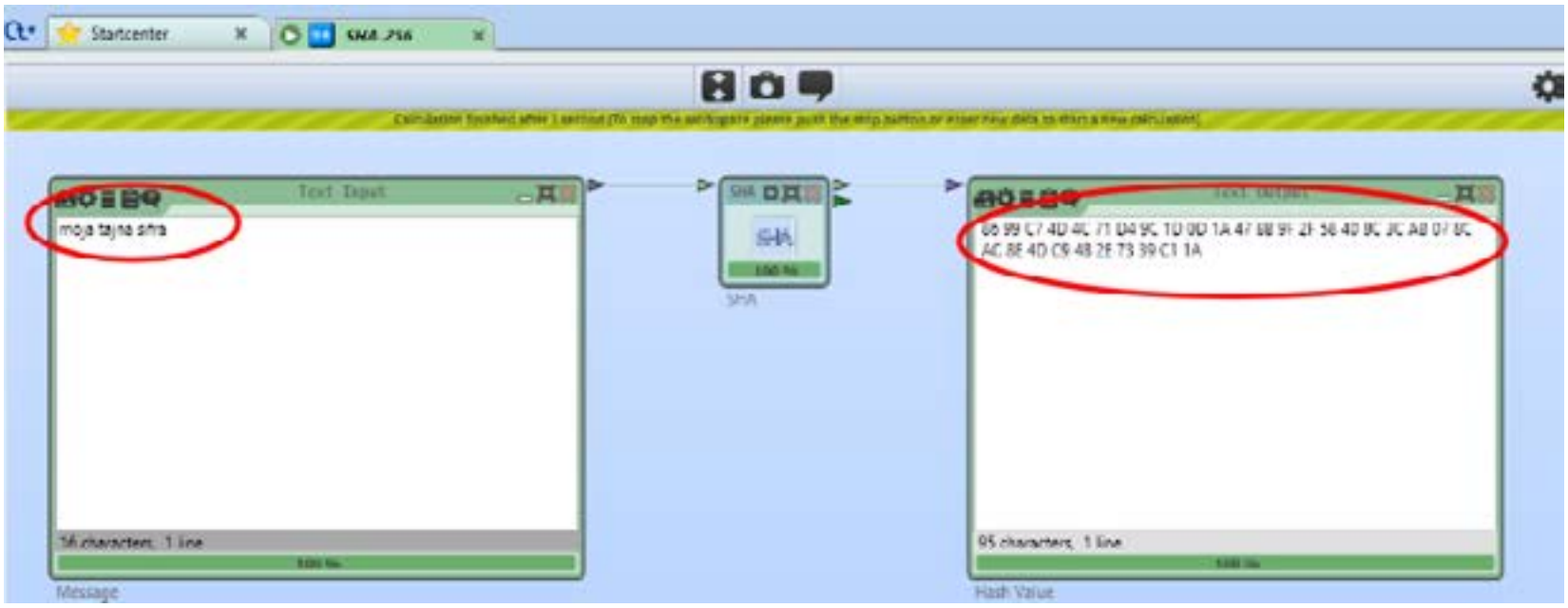

Figure 8. Illustration of a hash value of an employee's password, using SHA algorithm

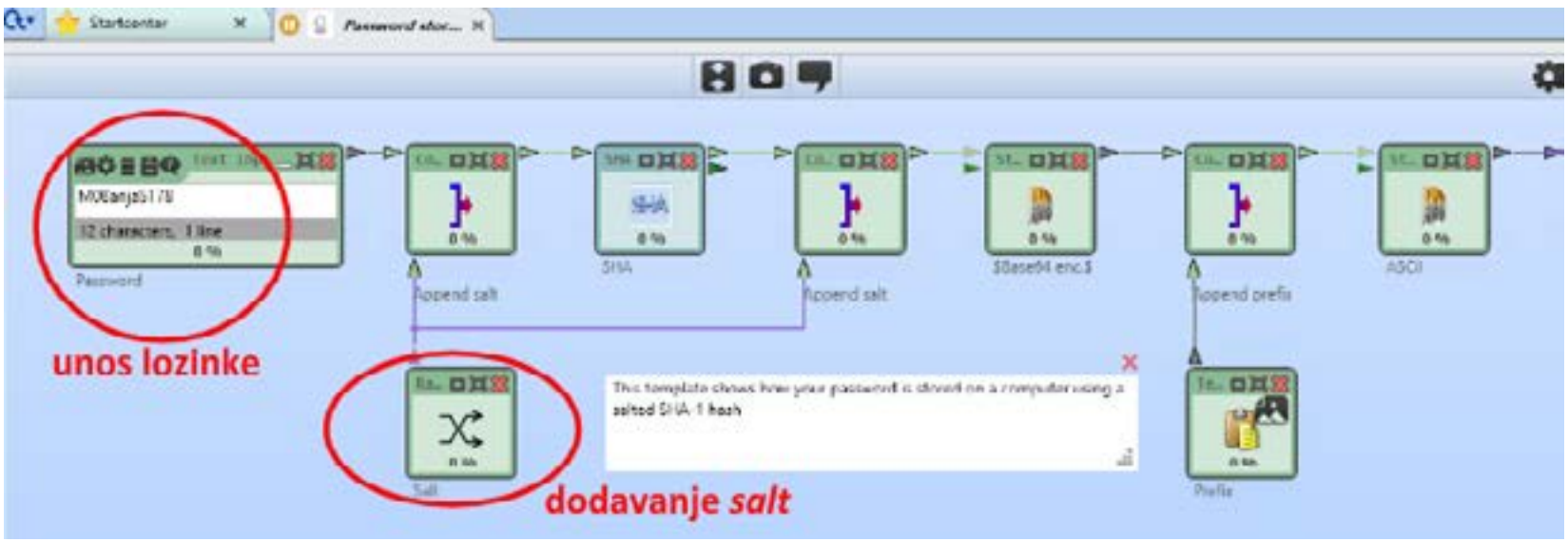

Figure 9. Illustration of a hash value of an employee's password, using the SHA algorithm after adding a salt value

4. Discussion

Improvements in the security of the business of Vesimpex have been proposed for the process of financial transactions and the procedure of storing confidential information, such as employees' passwords.

The transaction implemented the pixel expansion technique for the purpose of assigning tokens when generating a one-time password. The encryption and decryption processes are fairly simple and provide a high level of security because they rely upon the one-time pad technique.

The proposal for storing the login passwords of employees includes adding random salt values before hashing. Salt values are unique randomly generated sequences added to each password, unique for each user.

The purpose of the process described here is to ensure that the potential hacker should find the confidential information entirely incomprehensible and therefore completely useless. This way, most of the responsibility for a data leak risk is conveyed from the human factor to the security system itself, which considerably enhances the security of the company's business.

References

1. Crovini C. Risk management in small and medium enterprises. Routledge; 2019.
2. Hughes P, Ferrett E. Introduction to Health and Safety at Work. 6th ed. New York: Routledge; 2016.
3. Hughes P, Ferrett E. Business Intelligence and Analytics in Small and Medium Enterprises. Melo PN, Machado C, editors. Boca Raton, FL : CRC Press/Taylor & Francis Group, 2020. | Series: Manufacturing design and technology series: CRC Press; 2018.
4. Ranković M, Ilić M. Upravljanje projektima. Beograd: ITS – Beograd; 2018.
5. Seo JH. Information Security and Cryptology – ICISC 2019: 22nd International Conference, Seoul, South Korea, December 4–6, 2019, Revised Selected Papers. In: Seo JH, editor. Cham: Springer International Publishing; 2020 [cited 2022 Feb 14]. Available from: https://link.springer.com/conference/icisc
6. https://www.vesimpex.rs/ [Internet]. [cited 2022 Feb 14]. Available from: https://www.vesimpex.rs/
7. Ilić M. Osnove ekonomije, finansija i računovodstva. Beograd: ITS-Beograd; 2017.
8. Kumar V, Sharma A, Introduction, August IJ-. A Survey on Various Most Common Encryption Techniques. Int J Adv Res Comput Sci Softw Eng [Internet]. 2014 [cited 2022 Feb 14];3:307–12. Available from: https://www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf
9. Menez J., van Oorschot P., Vanstone S. A Handbook of Applied Cryptography. 5th edition. CRC Press Series on Discrete Mathematics and Its Applications; 2001.
10. Klima RE, Sigmon NP. Cryptology Classical and Modern. 2nd ed. Chapman and Hall/CRC; 2019.
11. Stallings W. Cryptography and Network Security: Principles and Practice. 3rd ed. Prentice Hall; 2002.
12. Manucom EMM, Gerardo BD, Medina RP. Analysis of Key Randomness in Improved One-Time Pad Cryptography. 2019 IEEE 13th Int Conf Anti-counterfeiting, Secure Identify [Internet]. IEEE; 2019. p. 11–6. Available from: https://ieeexplore.ieee.org/document/8925173/
13. https://www.cryptool.org/en/ [Internet]. Available from: https://www.cryptool.org/en/
14. Ateniese G, Blundo C, Santis A De, Stinson DR. Extended capabilities for visual cryptography. Theor Comput Sci [Internet]. 2001;250:143–61. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0304397599001279
15. Ibrahim DR, Teh J Sen, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl [Internet]. 2021;80:31927–52. Available from: https://link.springer.com/10.1007/s11042-021-11229-9
16. Gnanaguruparan M, Kak S. Recursive Hiding of Secrets in Visual Cryptography. Cryptologia [Internet]. 2002;26:68–76. Available from: http://www.tandfonline.com/doi/abs/10.1080/0161-110291890768
17. Askari N, Heys HM, Moloney CR. An extended visual cryptography scheme without pixel expansion for halftone images. 2013 26th IEEE Can Conf Electr Comput Eng [Internet]. IEEE; 2013. p. 1–6. Available from: https://ieeexplore.ieee.org/document/6567726
18. Gonzalez RC, Woods RE. Digital Image Processing Third Edition. 3rd ed. New York: Upper Saddle River, NJ: Prentice Hall; 2008.
19. Dent AW, Mitchell CJ. User's guide to cryptography and standards [Internet]. Boston: Artech House; 2005. Available from: https://pure.royalholloway.ac.uk/portal/en/publications/users-guide-to-cryptography-and-standards(2bda27a3-da21-4407-b057-66c80213c16b).html
20. Stefanovic H, Savic A, Veselinovic R, Bjelobaba G. An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images. Int J Eng Invent [Internet]. 2021;10:1–11. Available from: www.ijeijournal.com
21. https://www.raiffeisenbank.rs/token/ [Internet]. Available from: https://www.raiffeisenbank.rs/token/
22. Islam MS. Using ECG signal as an entropy source for efficient generation of long random bit sequences. J King Saud Univ - Comput Inf Sci [Internet]. 2022; Available from: https://linkinghub.elsevier.com/retrieve/pii/S131915782200015