# APPLICATION OF THE ONE-TIME PAD (OTP) CIPHER IN BUSINESS COMMUNICATIONS

**Hana Stefanović, PhD[1]; Ana Savić, PhD[2]; Nikola Popović[3]**

[1] Comtrade Information Technology School ITS, Belgrade, SERBIA, hana.stefanovic@its.edu.rs
[2] School of Electrical and Computer Engineering, Belgrade, SERBIA, ana.savic@viser.edu.rs
[3] Alfa BK University, Faculty of Mathematics and Computer Science, Belgrade, SERBIA, nikolap6901@gmail.com

***Abstract:*** *The paper is a demonstration of the application of One-Time pad (OTP) ciphers in business communications. Several simulation models created in the CrypTool software tool are presented, making a mention of the weaknesses if one and the same key is used several times. An improvement of the quality of the created models by using a random sequence generator using data on atmospheric noise is proposed and the performances are significantly better in relation to the random number generator available in the CrypTool tool. How electronic financial transactions are processed by applying a One-Time pad cipher is also shown on a concrete example.*

***Key words:*** *cryptographic algorithms, CrypTool, One-Time pad (OTP), business communications*

## 1. INTRODUCTION

The contemporary business operations that are, first of all, based upon the use of computer systems and electronic data exchange are exposed to different risks which may have unforeseeable consequences. Given the frequent attacks on computer networks, attempts to access data in an unauthorized way, eavesdropping, malicious modifications of data and so on, it is necessary that new ways of communication enabled by technological progress should be applied. The safety issue imposes the need to introduce new mechanisms which should take over the role of classical solutions with the aim of achieving efficient identification, access control and verification [1]. The answer to the majority of challenges like these ones is offered by the application of cryptographic solutions although there are also the problems that cryptography cannot adequately respond to. [2].

Cryptography studies different transferable data transformation techniques in such a way that the meaning of the data is only available to the parties authorized in communication. Simultaneously, transformation should be such that the unauthorized parties in communication that come in possession of a transformed message cannot come to the initial data. There are a large number of cryptographic algorithms, classical and modern, as well as those using the same key for coding and for decoding, and those asymmetrical that use different keys in the coding and decoding processes. The question pertaining to the safety of a cipher is key to each cryptographic cipher, irrespective of whether a symmetrical or asymmetrical cryptographic algorithm is used [3].

The cipher that has the characteristic which makes it impossible to come to a plaintext from a ciphered text without knowing the key, not even through an exhaustive key search, is considered to be an unconditionally safe cipher [4]. It is certain that an exhaustive search (not limiting the search time and the available resources) can lead to the key, but the eavesdropper is not interested in having it done after several tens or hundreds of years.

Should, however, the eavesdropper have the best possible equipment and resources, an unconditionally safe cipher should enable them not to come in possession of a plaintext, even not so in idealized conditions. The basic idea of an unconditionally safe cipher implies that an exhaustive search of the potential keys that generate a large number of messages anyway should make it impossible for the eavesdropper to find a way to determine which one of them is the right one [5], [6]. Full search will enable the eavesdropper to receive a large number of senseless messages which he will reject, but he will surely also receive a certain number of senseful messages; if all those messages are equally probable, then there is no way for the eavesdropper to determine which one of them is the right one.

An example of an unconditionally safe cipher is the One-Time Pad (OTP) cipher [7], which is applied in this paper. The simulation models presenting the basic OTP algorithm principles are implemented in the CrypTool software tool [8], with a special mention of the case of the repeated use of the key intended for one-time use. One example of processing an electronic financial transaction through the application of the OTP is also enclosed.

## 2. OTP ALGORITHM BASIC PRINCIPLES

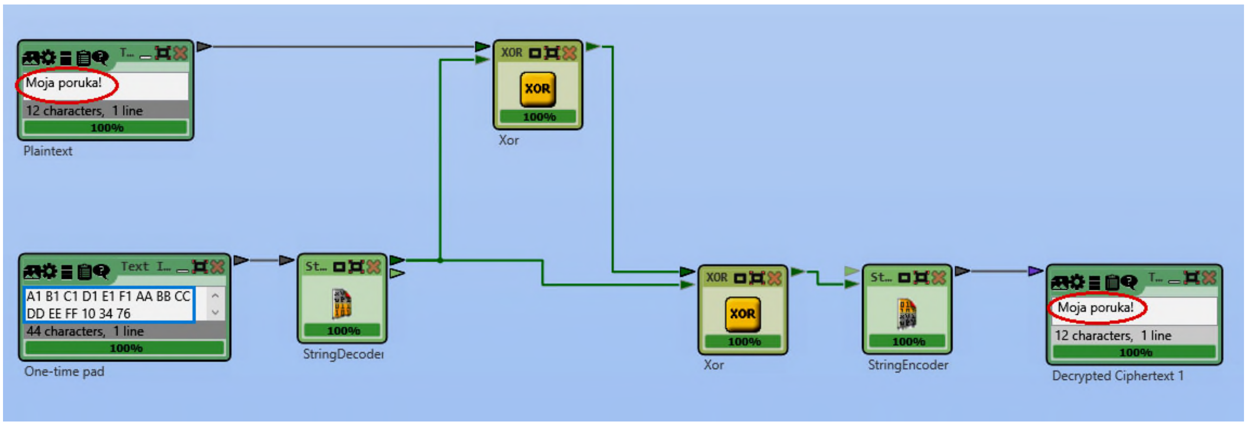
Prior to the encryption, a message first needs to be presented by a binary sequence based on the defined code. Then, another binary sequence of the same length as well as the message, which will represent the key that should have the characteristics of a random sequence, is needed. The encryption implies that every bit of the plaintext $p_i$ is added according to the Module 2 (the XOR operation) with one bit of the *ki* key each so as to obtain an appropriate bit of the ciphered text $c_i$:

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

In the decryption process, each bit of the cipher text is added according to the Module 2 with the same bit of the key used in encryption, which, given the XOR characteristics, provides the original text:

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

The simulation model created in the CrypTool software tool [8] that shows the plaintext encryption and decryption process (the content “My message!”) through the application of the OTP is shown in Figure 1. The key used is recorded in the hexadecimal format in the lower left-hand corner, whereas the decrypted message is shown in the lower right-hand corner in Figure 1.


Moja poruka!

12 characters, 1 line

A1 B1 C1 D1 E1 F1 AA BB CC DD EE FF 10 34 76

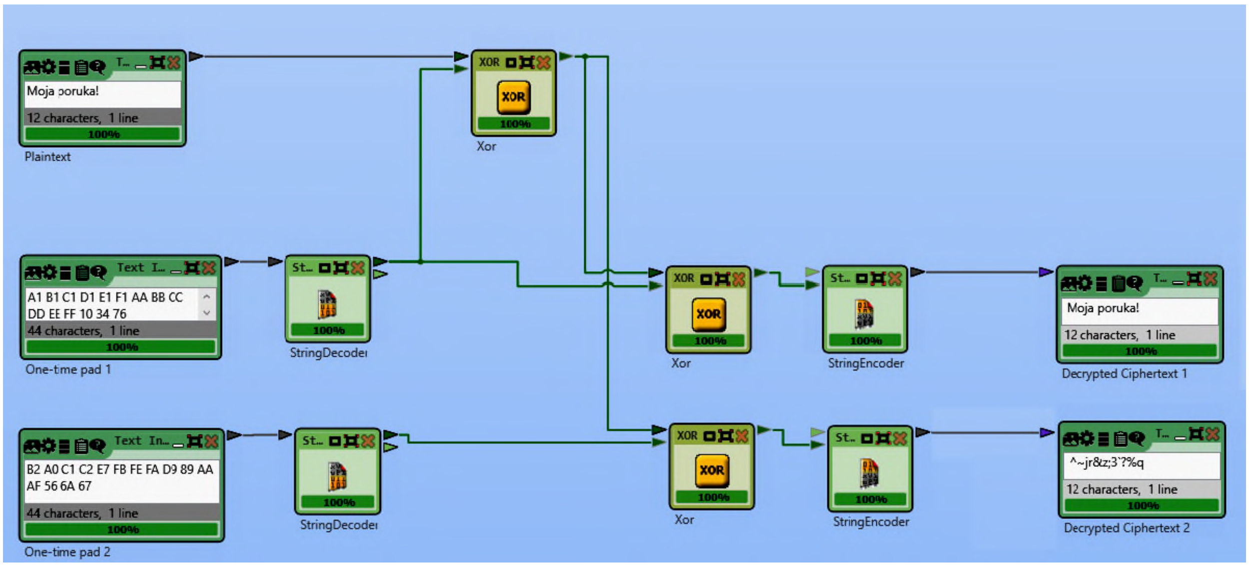
44 characters, 1 line

Moja poruka!

12 characters, 1 line

**Figure 1:** The simulation model showing the plaintext encryption and decryption procedure (the content “My message!”) through the application of the OTP

By searching potential keys, the eavesdropper generates a large number of messages, some of which will be senseless, as is shown in Figure 2. The messages like these will be rejected by the eavesdropper, but a certain number of senseful messages will surely be generated. If all those messages are equally probable, then the eavesdropper can in no way determine which one of them is the right one [7].


Moja poruka!

12 characters, 1 line

A1 B1 C1 D1 E1 F1 AA BB CC DD EE FF 10 34 76

44 characters, 1 line

B2 A0 C1 C2 E7 FB FE FA D9 89 AA AF 56 6A 67

44 characters, 1 line

Moja poruka!

12 characters, 1 line

^~jr&z;3`?%q

12 characters, 1 line

**Figure 2:** The simulation model showing the potential key search procedure

The safety of the OTP algorithm is based on key randomness. There is no exact definition for the term *randomness*, but, from the standpoint of cryptography, there are two basic properties of the binary random key that are required:

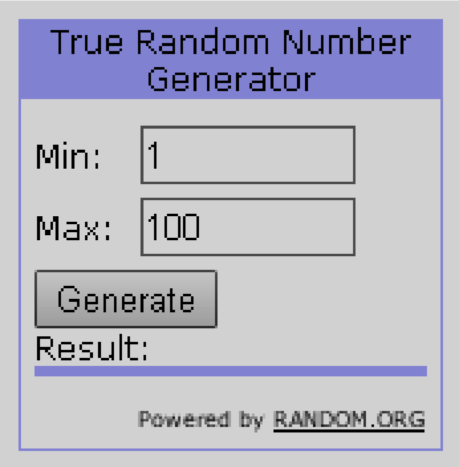
- Unpredictability: Independently of the number of the known key bits, the probability of guessing the next bit is no greater than ½. The probability that the next bit will be 1 or 0 is exactly equal to ½.
- Balance: The numbers “1” and “0” have to be approximately equal in a sequence of a sufficiently big length.

If the key is a random binary sequence, then the probability that any bit of the key whatsoever has the value of the logical one is equal to the probability that that bit has the value of the logical zero and equals ½. Differently from that, the plaintext has certain statistical characteristics and the probability of the appearance of logical ones and zeros is not equal.

## 3. THE IMPROVEMENT OF THE ALGORITHM SAFETY USING THE TRUE NUMBER RANDOM NUMBER GENERATOR

In order to generate a random key with as quality characteristics as possible, some devices have been developed, such as those developed by the company ID Quantique [9]: Cerberis QKD System, Clavis QKD Platform, and Centauris CN8000, which have had a commercial use for a longer time [10], and the random number generator, whose operation is based upon quant mechanics principles (the quantum random number generator) was developed in 2001.

The further improvement of the model simulated in this paper includes the use of the random number generator (the true random number generator) that uses data about atmospheric noise [11] as is shown in Figure 3. A generator like this has much better characteristics [12] than the pseudorandom generator available in the Cryptool tool used in the simulation models shown in Figure 1 and in Figure 2. The user interface of the true random number generator is shown in Figure 3.



True Random Number Generator

Min: 1

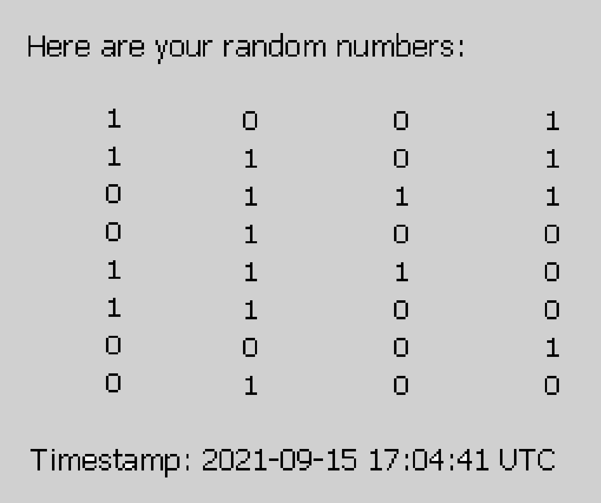
Max: 100

Result:

Powered by RANDOM.ORG

**Figure 3:** The random number generator using data about atmospheric noise

By using a generator like this, a contribution is made to the improvement of the performances of the analyzed model. Appropriate setting enables the generation of the needed number of random bits according to the requirements for the key length, as is illustrated in Figure 4.



```
Here are your random numbers:

    1       0       0       1
    1       1       0       1
    0       1       1       1
    0       1       0       0
    1       1       1       0
    1       1       0       0
    0       0       0       1
    0       1       0       0

Timestamp: 2021-09-15 17:04:41 UTC
```

**Figure 4:** The generation of a sequence of the random value bits using the true random number generator

## 4. DISADVANTAGES OF THE ALGORITHM DUE TO THE MULTIPLE USE OF THE SAME KEY

The simulation model illustrating the application of the same OTP key in the process of encryption two different messages is shown in Figure 5. A digital image was chosen as the plaintext so as to visually as well show the consequences of the multiple application of the same OTP key. Should the XOR operation be performed over the cipher texts $C_A$ and $C_B$, the following result is obtained:

$$C_A \oplus C_B = (A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \oplus 0 = A \oplus B \tag{3}$$

These characteristics has as a consequence the situation in which, after performing the XOR operation over the cipher texts even though the eavesdropper is not knowledgeable of the key $K$, an inventive eavesdropper discovers a lot about the original messages, which is the reason why the multiple use of the same OTP key is not recommendable.

The result shown in the lower left-hand corner in Figure 5 reveals a lot about the original images, which is a consequence of the mentioned characteristics of the XOR operation.

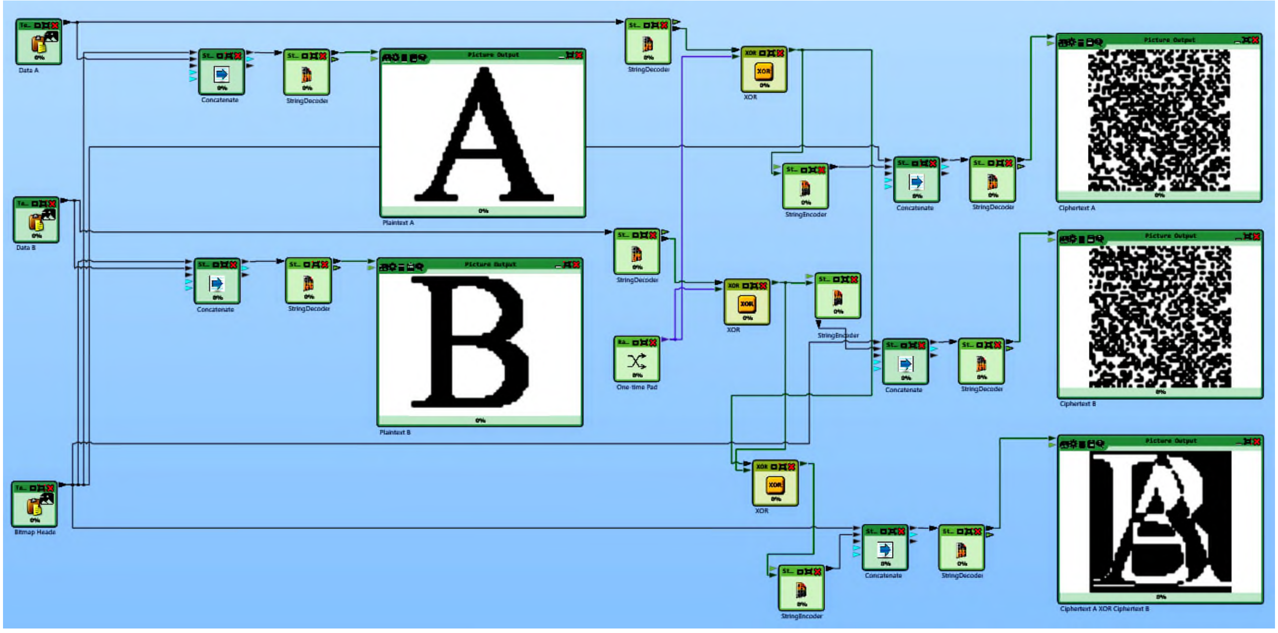


**Figure 5:** The simulation model illustrating the multiple application of the same OTP key

## 5. AN EXAMPLE OF MAKING ELECTRONIC FINANCIAL TRANSACTIONS BY APPLYING THE OTP ALGORITHM

In order to sign in to e-banking applications very frequently used in business and private financial transactions, the serial number of the token or m-token is only needed. The user does not reveal his PIN for the token or m-token to anyone, whereas the implied recommendation reads: keep the PIN with the token or m-token. The bank does not request a one-time password from the user, nor does it request a data for signing a transaction.

The creation of a request for generating a one-time password is shown in the left-hand part in Figure 6, whereas the generated password sent to the user's mobile device is shown in the right-hand part in Figure 6.

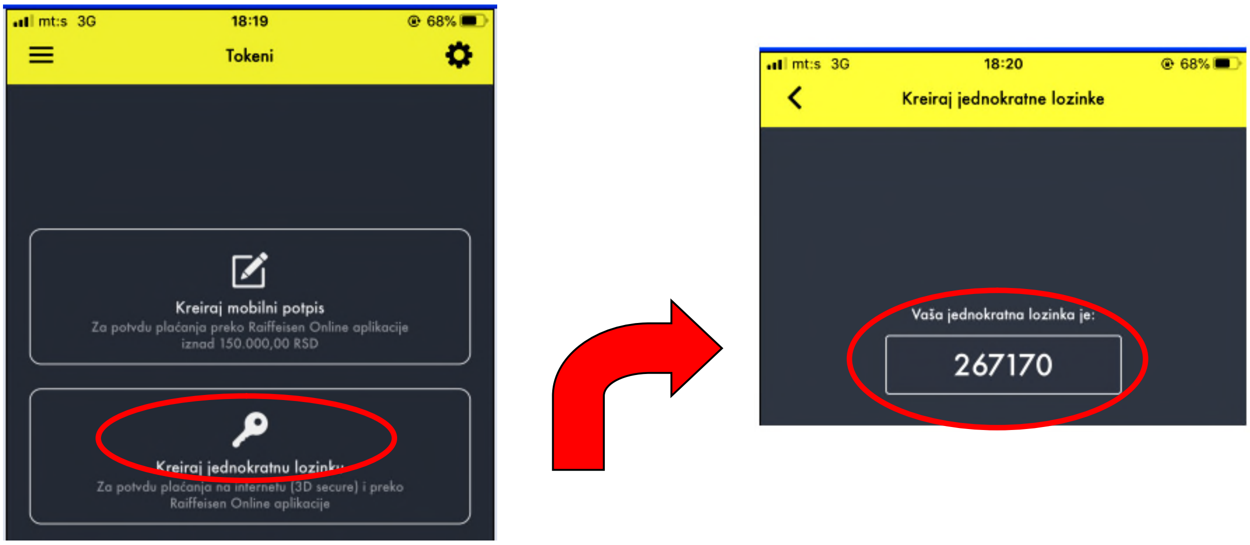
The data about the password time validity is also forwarded to the user, as is shown in Figure 7, also including some additional pieces of information about the token.

The password duration forwarded to the user after the synchronization had been performed with the server time is shown in the left-hand part in Figure 7 and is 5 minutes.

The additional pieces of information about the token (the Token info) showing the serial number and the UTC time are in the right-hand part in Figure 7. The mobile token synchronization is performed to adjust the time on the user application and the server time in order to allow the application to run undisturbedly [13].

An advantage of this kind of password is that since it is randomly generated, the user does not have to make an effort to remember it. The OTP is always provided via authenticator app or physical token.

Randomly-generated passwords are infinitely more secure than user-created passwords. User-created passwords are usually quite weak, with reuse across multiple account further decreasing security.



mt:s 3G 18:19 68%

Tokeni

Kreiraj mobilni potpis

Za potvdu plaćanja preko Raiffeisen Online aplikacije iznad 150.000,00 RSD

Kreiraj jednokratnu lozinku

Za potvdu plaćanja na internetu (3D secure) i preko Raiffeisen Online aplikacije

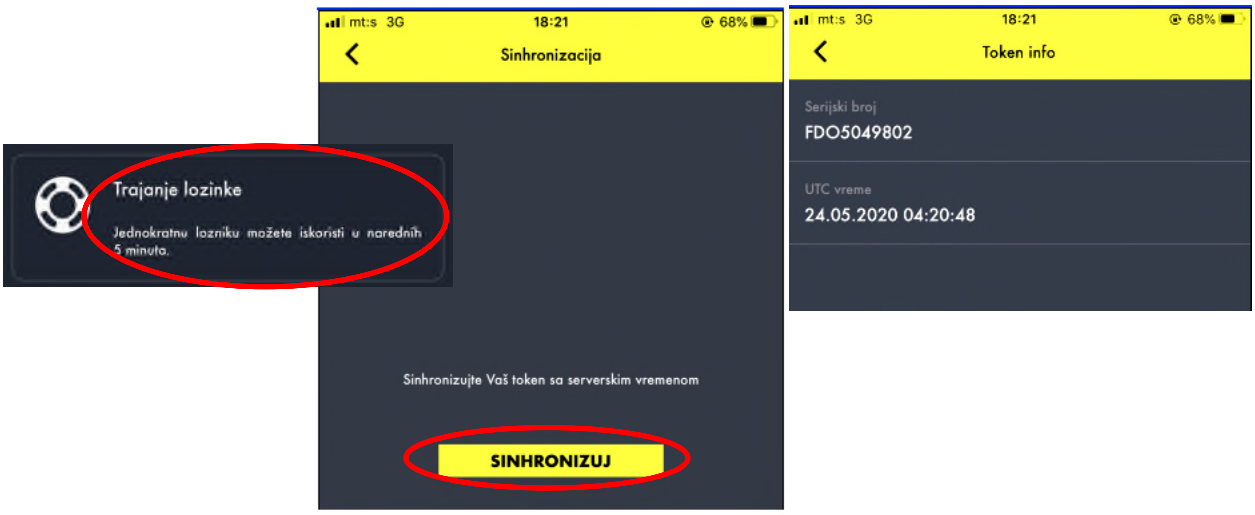
mt:s 3G 18:20 68%

Kreiraj jednokratne lozinke

Vaša jednokratna lozinka je:

267170

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



Trajanje lozinke

Jednokratnu lozniku možete iskoristi u narednih 5 minuta.

mt:s 3G 18:21 68%

Sinhronizacija

Sinhronizujte Vaš token sa serverskim vremenom

SINHRONIZUJ

mt:s 3G 18:21 68%

Token info

Serijski broj

FDO5049802

UTC vreme

24.05.2020 04:20:48

**Figure 7:** The illustration of the data about the password time validity

## 4. CONCLUSION

The paper shows an example of the application of an unconditionally safe cipher, which cannot be broken irrespective of the available resources because the coded message has no sufficient information to uniformly define the appropriate original text. Given the fact that the safety of the OTP algorithm is based on the one-time use and randomness of the key, the paper specially considers the case of the multiple use of the same key, as well as the use of the randomly generated sequence that can qualitatively be verified from the cryptographic aspect, which on its part uses atmospheric noise as the source of randomness. While applying the OTP, the distribution of the generated key to the other party in communication, which is becoming practically impossible to solve in the commercial world, is certainly a major issue.

## REFERENCES

[1] Menez J.A, van Oorschot P.C, Vanstone S.A. A Handbook of Applied Cryptography (5th edition). CRC Press: Series on Discrete Mathematics and Its Applications; 2001.

[2] Stallings W. Cryptography and Network Security: Principles and Practice (3rd edition). Prentice Hall; 2002.

[3] Ramesh G, Urmani R, Thambiraja E. A Survey on Various Most Common Encryption Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2(7), 2012: 226-233.

[4] Bruen, A.A. Cryptography, information theory, and error-correction. San Diego: Willey-INTERSCIENCE; 2005.

[5] Dent, A.W, Mitchell, C.J. User’s Guide to Cryptography and Standards, Computer Security Series. Boston: Artech House; 2005.
[6] Liu Z, Cao Z.F, Huang Q, et al. Fully secure multiauthority ciphertext-policy attribute-based encryption without random oracles. In: Proceedings of 16th European Symposium on Research in Computer Security, Leuven, 2011: 278–297.
[7] Manucom E.M.M, Gerardo B.D, Medina R.P, et al. Analysis of Key Randomness in Improved One-Time Pad Cryptography. In: IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID). Oct. 2019: 11–16.
[8] https://www.cryptool.org/en/
[9] https://www.idquantique.com/
[10] https://www.idquantique.com/random-number-generation/overview/
[11] https://www.random.org/
[12] https://www.random.org/#numbers
[13] https://www.raiffeisenbank.rs/token/