International Journal of Business and Technology

Volume 9
Issue 1 *Spring 2021*

Article 13

March 2021

One-Time Pad Cipher (OTP) Use Cases and Simulation Examples for Electronic Financial Transactions

Ana Savic
School of Electrical Engineering and Computer Science Applied Studies, ana.savic@viser.edu.rs

One-Time Pad Cipher (OTP) Use Cases and Simulation Examples for Electronic Financial Transactions

Ana Savic[1], Goran Bjelobaba[2], Nikola Popovic[3], Hana Stefanovic[4]

[1] School of Electrical and Computer Engineering, Academy of Technical and Art Applied Studies, Belgrade, SERBIA, ana.savic@viser.edu.rs

[2] University of Belgrade, Faculty of organizational sciences, Department for e-business, Belgrade, SERBIA, gbjelobaba@gmail.com

[3] Alfa BK University, Faculty of Mathematics and Computer Science, Belgrade, SERBIA, nikolap6901@gmail.com

[4] Comtrade Information Technology School of Applied Studies, Belgrade, SERBIA, hana.stefanovic@its.edu.rs

Abstract. This paper presents some applications of One-Time pad (OTP) cipher in business communications and processing the electronic financial transactions. Several simulation models created in the CrypTool, making a mention of the misuse and weaknesses if the same OTP key is used several times, are also given. Some examples of processing an electronic financial transaction through the application of the OTP are proposed.

Keywords: One-Time pad (OTP) cipher, CrypTool, multiple use of the same key, electronic financial transactions

1 Introduction

An electronic financial transactions and real-world digital 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 (Menez et al., 2001). 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 (Stallings, 2002).

Cryptography examines protecting information in computer systems and 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 (Ramesh et al., 2012).

One-Time pad (OTP), also called Vernam-cipher or the perfect cipher, is a cryptographic algorithm where the plaintext is combined with the random key. It is the only existing mathematically unbreakable encryption (Dent and Mitchell, 2005). 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 (Bruen, 2005). There are some important rules which have to be followed and applied correctly, se the One-Time pad can be proven unbreakable, according to the Claude Shannon's theorem. (Shannon, 1948). Even infinite computational power and infinite time cannot break One-Time pad encryption, simply because it is mathematically impossible. However, if only one of these rules is disregarded, the cipher is no longer unbreakable.

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 (Liu et al., 2011). The exhaustive 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.

In this paper the simulation models presenting the basic OTP algorithm principles are implemented in the CrypTool software tool (https://www.cryptool.org/en/), 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 given.

2 OTP ALGORITHM CHARACTERISTICS

It has been proven that OTP is impossible to crack if it is used correctly. It has the perfect secrecy property and allows very fast encryption and decryption (Manucom et al., 2019). However, the secret key must be at least as long as the message, what makes it quite inconvenient to use while sending large electronic information.

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:

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

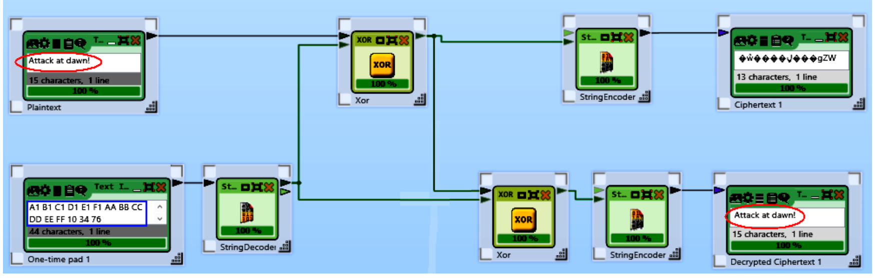
In the decryption process, each bit of the cipher text is added according to the Module 2 with the same bit of the key used in encryption, which, given the XOR characteristics, provides the original text:

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

However, if only one of these rules is disregarded, the cipher is no longer unbreakable:

- The key is at least as long as the message or data that has to be encrypted
- The key is truly random (it is not generated by a simple computer function or such)
- Key and plaintext are calculated modulo 10 (digits), modulo 26 (letters) or modulo 2 (binary)
- Each key is used only once, and both sender and receiver must destroy their key after use
- There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers).

The simulation model created in the CrypTool software tool that shows the plaintext encryption and decryption process (the content "Attack at down!") 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.



Attack at dawn!
15 characters, 1 line

�ŵ�����J����gZW
13 characters, 1 line

A1 B1 C1 D1 E1 F1 AA BB CC DD EE FF 10 34 76
44 characters, 1 line

Attack at dawn!
15 characters, 1 line

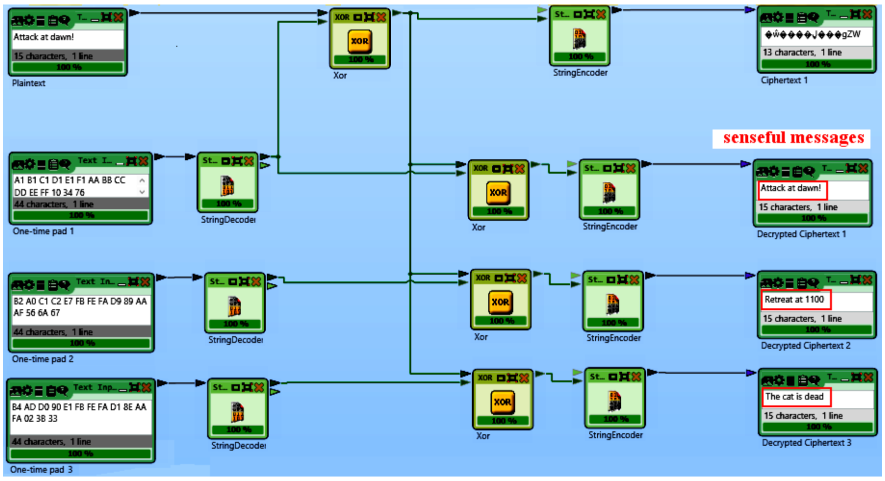
Fig 1. The simulation model showing the plaintext encryption and decryption procedure (the content "My message!") through the application of the OTP

By searching potential keys (Stefanovic et al., 2021), 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.

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.



Plaintext: Attack at dawn!
15 characters, 1 line

Ciphertext 1: ◆ŵ◆◆◆◆J◆◆◆gZW
13 characters, 1 line

One-time pad 1: A1 B1 C1 D1 E1 F1 AA BB CC DD EE FF 10 34 76
44 characters, 1 line

Decrypted Ciphertext 1: Attack at dawn!
15 characters, 1 line

One-time pad 2: B2 A0 C1 C2 E7 FB FE FA D9 89 AA AF 56 6A 67
44 characters, 1 line

Decrypted Ciphertext 2: Retreat at 1100
15 characters, 1 line

One-time pad 3: B4 AD D0 90 E1 FB FE FA D1 8E AA FA 02 3B 33
44 characters, 1 line

Decrypted Ciphertext 3: The cat is dead
15 characters, 1 line

Fig 2. The simulation model showing the potential key search procedure

3. WEAKNESS OF THE ALGORITHM DUE TO THE MULTIPLE USE OF THE SAME OTP KEY

The simulation model illustrating the application of the same OTP key in the process of encryption two different messages is shown in Figure 3. 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:

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

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 3 reveals a lot about the original images, which is a consequence of the mentioned characteristics of the XOR operation.

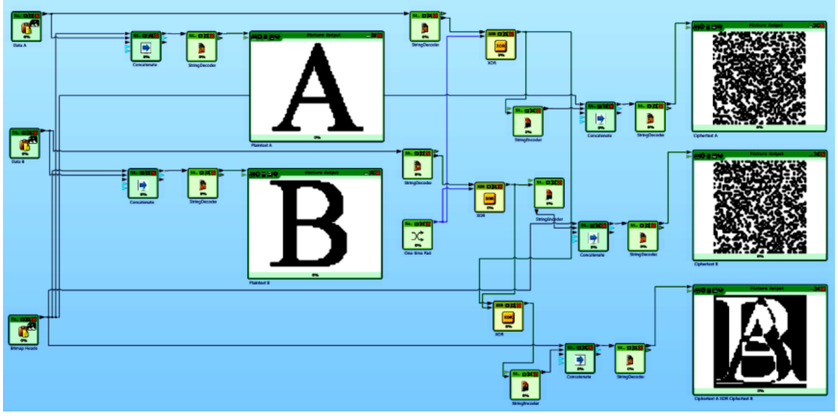
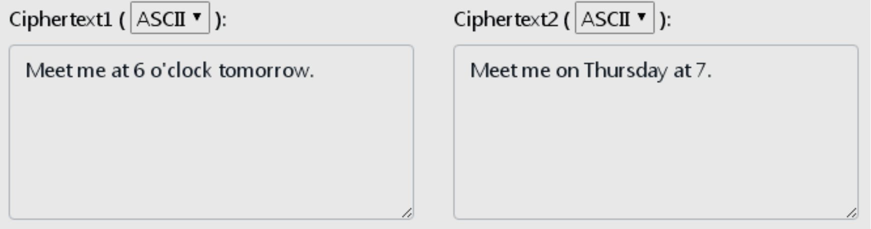


Fig 3. The simulation model illustrating the multiple application of the same OTP key

In the case of text messages, encrypted with the same OTP key, simulation results are given in Figure 4, Figure 5, Figure 6 and Figure 7. Plain text is given in Figure 4, while the cipher text generated using the same OTP key for both messages is given in Figure 5. After performing the XOR operation over the cipher texts given in Figure 5, the obtained result (even though the eavesdropper is not knowledgeable of the OTP key) is illustrated in Figure 6. Some additional analysis of the result is given in Figure 7, showing a lot about the original messages.

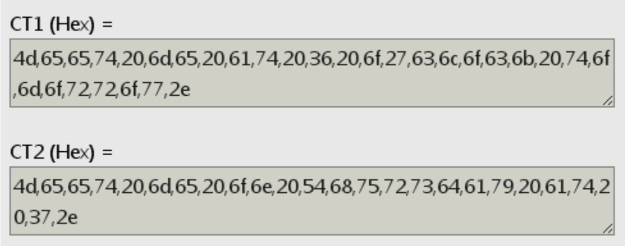

Ciphertext1 (ASCII ▾):

Meet me at 6 o'clock tomorrow.

Ciphertext2 (ASCII ▾):

Meet me on Thursday at 7.

Fig 4. Two messages that are to be encrypted with the same OTP key

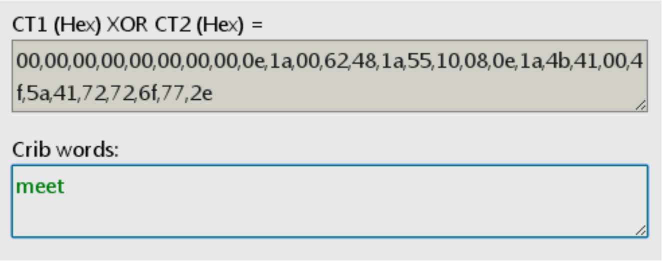

CT1 (Hex) =

4d,65,65,74,20,6d,65,20,61,74,20,36,20,6f,27,63,6c,6f,63,6b,20,74,6f,6d,6f,72,72,6f,77,2e

CT2 (Hex) =

4d,65,65,74,20,6d,65,20,6f,6e,20,54,68,75,72,73,64,61,79,20,61,74,20,37,2e

Fig 5. Cipher text of messages (CT1 and CT2) encrypted with the same OTP key



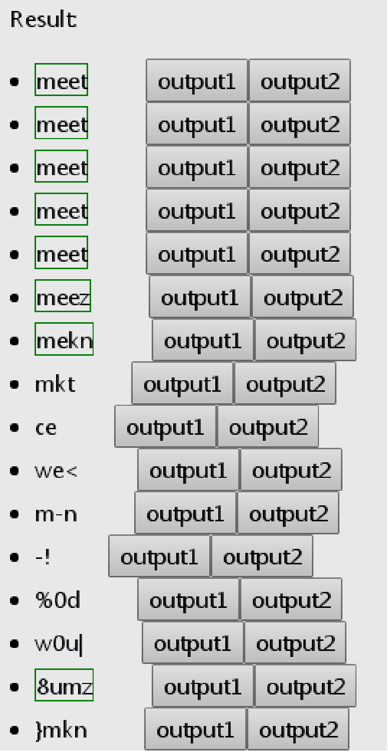
CT1 (Hex) XOR CT2 (Hex) =

```
00,00,00,00,00,00,00,00,0e,1a,00,62,48,1a,55,10,08,0e,1a,4b,41,00,4
f,5a,41,72,72,6f,77,2e
```

Crib words:

```
meet
```

Fig 6. Results after performing the XOR operation over the cipher texts CT1 and CT2



```
Result

• meet    output1 output2
• meet    output1 output2
• meet    output1 output2
• meet    output1 output2
• meet    output1 output2
• meez    output1 output2
• mekn    output1 output2
• mkt     output1 output2
• ce      output1 output2
• we<     output1 output2
• m-n     output1 output2
• -!      output1 output2
• %0d     output1 output2
• w0u|    output1 output2
• 8umz    output1 output2
• }mkn    output1 output2
```

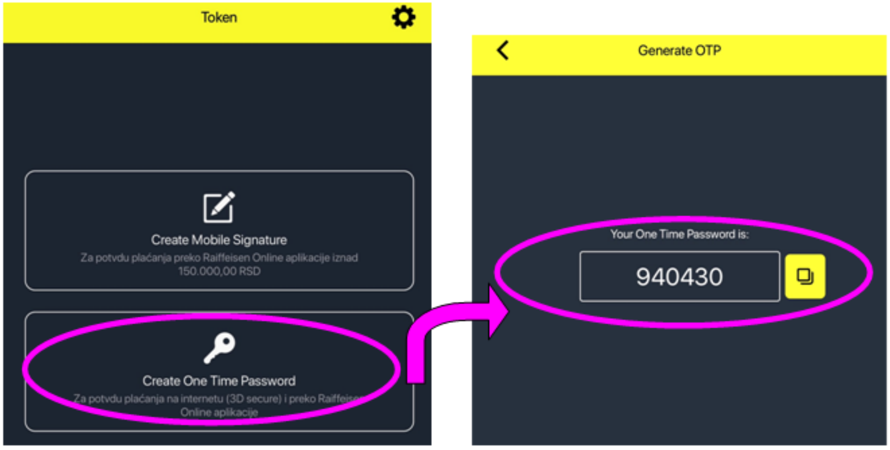
Fig 7. An additional analysis of the results obtained after performing the XOR operation over the cipher texts CT1 and CT2

It can be concluded that each key is used only once, and both sender and receiver must destroy their key after use.

4. SOME EXAMPLES OF MAKING ELECTRONIC FINANCIAL TRANSACTIONS BY APPLYING THE OTP ALGORITHM

Most online transactions require a two-step authentication, and the OTP password sent by SMS is often one of those two steps. The purpose of an OTP is to prevent fraud by confirming that the person making the transaction and the credit card owner are one and the same. To do so, a temporary code is automatically sent by SMS to the phone number associated with the bank account used, as it is illustrated in Figure 8.

Once the OTP SMS is received, the user types it in the transaction interface and he is only then able to finalize his purchase. Regrettably, the mobile device (tablet or smartphone) used to send and receive an SMS is not very innocuous. The time validity of the OTP password is also provided, and it is limited to a couple of minutes, as it is illustrated in Figure 9.

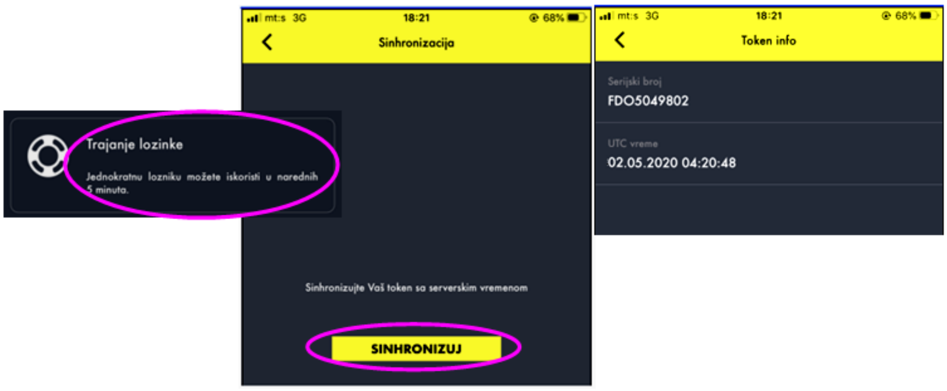


Za potvdu plaćanja preko Raiffeisen Online aplikacije iznad 150.000,00 RSD

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

Your One Time Password is: 940430

Fig 8. 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.

Sinhronizujte Vaš token sa serverskim vremenom

Serijski broj: FDO5049802

UTC vreme: 02.05.2020 04:20:48

Fig 9. The illustration of the data about the password time validity

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 8, whereas the generated password sent to the user's mobile device is shown in the right-hand part in Figure 8. The data about the password time validity is also forwarded to the user, as is shown in Figure 9, 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 9 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 9. 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 (https://www.raiffeisenbank.rs/token/).

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. Another advantage is that the 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.

It can be concluded that one-time passwords are a very good method for increasing security and reducing compromised accounts, fraud, and other cybercrime. Despite the additional effort that is often required to utilize this method, most users strongly agree that this is a small price to pay for the security and peace of mind that comes with using one-time passwords.

5. 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. 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. Bruen, A. A., (2005). Cryptography, information theory, and error-correction, San Diego: Willey-INTERSCIENCE.
2. Dent, A.W., Mitchell, C. J., (2005). User's Guide to Cryptography and Standards, Computer Security Series, Boston: Artech House.

3. https://www.cryptool.org/en/
4. https://www.raiffeisenbank.rs/token/
5. Liu, Z., Cao, Z. F., Huang, Q., et al., (2011). Fully secure multiauthority ciphertext-policy attribute-based encryption without random oracles, In: Proceedings of 16th European Symposium on Research in Computer Security, pp. 278–297.
6. Manucom, E. M. M., Gerardo, B. D., Medina, R. P., et al., (2019). Analysis of Key Randomness in Improved One-Time Pad Cryptography, In: IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp. 11–16.
7. Menez, J. A., van Oorschot, P. C., Vanstone, S. A., (2001). A Handbook of Applied Cryptography, 5th Ed., CRC Press: Series on Discrete Mathematics and Its Applications.
8. Shannon, C. E., (1948). Communication Theory of Secrecy Systems, Bell Systems Technical Journal, Vol. 28, pp. 656–715.
9. Stallings, W., (2002). Cryptography and Network Security: Principles and Practice, 3rd Ed., Prentice Hall.
10. Stefanovic, H., Savic, A., Popovic, N., (2021). Application of the One-Time Pad (OTP) cipher in business communications, In: Proceedings of 12th International scientific conference Science and Higher Education in Function of Sustainable Development – SED 2021 (in press)
11. Ramesh, G., Urmani, R., Thambiraja, E., (2012). A Survey on Various Most Common Encryption Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2(7), pp. 226-233.