Scientific and Practical Cyber Security Journal (SPCSJ) 4(2): 42-44 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

One-time pad – How breakable it is and How we can use it in the future

Levan Niparishvili, Bachelor in Business Administration, Doing Master in IT Management at Caucasus University of Georgia

ABSTRACT: The article is about to show that One-time pad is unbreakable if all rules are correctly applied. It gives some examples to prove that ciphertext does not leak any information about the plaintext. There are situations when One-time pad can be broken in case it is based on crypto algorithm generator or when it is used more than once. Also, there is analyzed the use of one-time pad in the future.

KEYWORDS: *one-time pad, encryption scheme*

ARTICLE:

The question is: "Is one-time pad really unbreakable" – a simple answer to this question is: "Yes, in case all rules are applied correctly". The scheme is simple and transparent and mathematically one cannot break it. One-time pad is base on the equation of two unknown variables (a plaintext and a key) out of which one is random. Let us consider the example given below:

Ciphertext:	QJKES	QJKES	QJKES
OTP-Key:	XVHEU	FJRAB	DFPAB
	---------	---------	---------
Plain text:	TODAY	LATER	NEVER

Here we have a plaintext "QJKES" encrypted by one-time pad. If an attacker tries to break it, let's say by using a brute force attack, he would find a key "XVHEU" and get a plaintext "TODAY". Unfortunately, he can also find other keys like "FJRAB" or "DFPAB" and get a plaintext "LATER" or "NEVER". He will have no clue which is correct. He can use different keys and produce any plaintext he wants. But the truth is there are many "proper" wrong keys to get a desired plaintext.

Let us give other examples based on digits. In order to encrypt a message, it is subtracted with a key, for decryption, the key is added to the cyphertext. For text-to-digit conversion we will use the following board:

CODE	A	E	I	N	O	T	CT No 1 English		
0	1	2	3	4	5	6			
B	C	D	F	G	H	J	K	L	M
70	71	72	73	74	75	76	77	78	79
P	Q	R	S	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	( )	(+)	(-)	(=)	REQ	SPC
90	91	92	93	94	95	96	97	98	99

Supposing that we have the following Ciphertext: 34818 25667 24857 50594 38586. There are many possible keys to crack it. Some examples are given below:

Ciphertext 34818 25667 24857 50594 38586
Key 1 +58472 33602 88472 58584 86707

Plaincode 82280 58269 02229 08078 14283

82 2 80 5 82 6 90 222 90 80 78 1 4 2 83
R E P O R T fi 222 fi P L A N E S
Recovered plaintext: "REPORT TWO PLANES"

Ciphertext 34818 25667 24857 50594 38586
Key 2 +58472 33602 81702 57464 98606

Plaincode 82280 58269 05559 07958 26182

82 2 80 5 82 6 90 555 90 79 5 82 6 1 82
R E P O R T fi 555 fi M O R T A R
Recovered plaintext: "REPORT FIVE MORTAR"

Ciphertext 34818 25667 24857 50594 38586
Key 3 +58472 33605 28941 36331 20507

Plaincode 82280 58262 42798 86825 58083

82 2 80 5 82 6 2 4 2 79 88 6 82 5 5 80 83
R E P O R T E N E M Y T R O O P S
Recovered plaintext: "REPORT ENEMY TROOPS"

These examples prove that we can produce any plaintext out of any cyphertext, if we apply a "proper" wrong key. That happens because a sequence of truly random digits. Codebreakers have no idea about which one was chosen. There is no mathematical solution to find a plaintext, in this way. But an attacker can think the other way. They can try to break they key and not a cyphertext and then reveal the plaintext. Therefore, it is critical to have a random key[1,2]. If we have a key generated by a deterministic

algorithm, an attacker will find a way to break it. For example, crypto algorithms used for key generation, lowers the security of a one-time pad and it enables an attacker to break it.

There is one important limitation to consider when working with one-time pad. If a key is used more than once, even if it is truly random, simple cryptanalysis can reveal the key. In this case, an attacker will be able to find out the connection between two cyphertexts and it will give information about the key. There can be used heuristic analysis or a known plaintext attack. Simply, there will be a crib, a presumed piece of the first plaintext to be used to reverse-calculate a piece of the key. Then we apply this presumed key to the second cyphertext. If the cribs were correct, it reveals a readable part of the second plaintext and it provides clues that help to expand the cribs.

Regarding the usability of one-time pad, we can say that it is only possible if the sender and the receiver both possess the same key. In this case, we need to ensure its secure exchange process. But we have some more drawbacks regarding the scheme. One-time pad encryption does not provide message authentication and integrity. Even though the sender is authentic and he is assigned to produce a cyphertext, we cannot verify when the message is corrupted by transition errors or by an adversary. Here a solution is to use hash algorithm with the plaintext and send the hash value along with the message [3-5]. An adversary cannot predict neither the effect of his action to the cyphertext, nor the hash value. But the receiver can reveal and compare the hashed value with the message.

As a conclusion, one-time pad is evolving while the computational power grows and the technology advances. It uses new solutions and accepts the challenges. One-time pad encryption will continue in the future securely, as we use it today, and as they were using it in the past.

REFERENCES:

1. M. Iavich, G. Iashvili, A.Gagnidze, S. Gnatyuk, V. Vialkova; Lattice Based Merkle; IVUS2019; CEUR-WS.org; 2019
2. Horstmeyer, R., Judkewitz, B., Vellekoop, I. et al. Physical key-protected one-time pad. Sci Rep 3, 3543 (2013). https://doi.org/10.1038/srep03543
3. Gagnidze A.G., Iavich M.P., Iashvili G.U., Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36.
4. A. Gagnidze, M. Iavich, G. Iashvili// Novel Version of Merkle Cryptosystem// BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017, p. 28-33
5. S. Tang and F. Liu, "A one-time pad encryption algorithm based on one-way hash and conventional block cipher," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 72-74, doi: 10.1109/CECNet.2012.6201917.