Chapter 1
One-Time Pad

Thomas Lugrin

1.1 Introduction

The one-time pad is a simple cipher. It ensures a perfect form of confidentiality known as *perfect secrecy* by combining a plaintext and a key of the same length with the exclusive-or (XOR) operator to produce a ciphertext. However, it lacks basic security properties shared by standard ciphers, namely authentication, and integrity. The central issue of the critical exchange between communication partners must be solved by other means. Some modern stream ciphers derive from the one-time pad in that they simulate its mechanism.

1.2 Analysis

The invention of the one-time pad can be attributed to Gilbert S. Vernam, who developed an automated system for teletypewriters using punched paper tapes in 1917 [1]. Together with Joseph O. Mauborgne, he realized that if the keystream, i.e. the distribution of the punches on the tape, was uniformly random and independent such as an infinite non-periodic tape, the cipher would be unbreakable. An earlier mention of the one-time pad can be found in an 1882 publication by Frank Miller [2] and could have been a source of inspiration for Vernam [3]. A famous implementation of the one-time pad is the hotline between the United States and the USSR that was established in 1963 [4].

T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_1

1.2.1 Definition

The one-time pad takes a plaintext message and a random key of the same length as inputs. The message and key are represented in bits in a modern setup. Encryption consists of adding the message to the key using the XOR operator. The result is the ciphertext. The one-time pad decryption process is similar, as the ciphertext is XOR-ed with the same key to recover the plaintext. The simplicity of the encryption and decryption process makes it a very fast cipher, but the length of the key makes it difficult to use in practice.

In 1949, Claude E. Shannon formally showed that the one-time pad has *perfect secrecy* in an information-theoretic sense [5]. Any ciphertext of a given length can be the encryption of any plaintext of the same length with equal probability. Moreover, adversaries with arbitrarily considerable computing power cannot break it, which means it is also quantum-computer resistant.

The one-time pad is, however, not perfect in a broader sense, as it does not provide authentication of the sender, nor does it ensure the integrity of the ciphertext; a malicious intermediary can modify the ciphertext without any of the communicating parties noticing it. Even worse, if parts of the plaintext are known, as is typical in e-mail headers, the corresponding ciphertext parts can be altered to yield precisely any malicious plaintext of the same length. Re-using the key completely breaks the one-time pad security: XOR-ing two ciphertexts gives the XOR-ed plaintexts. If there is enough redundancy in text encoding, e.g., ASCII, one can recover the two plaintexts. More generally, this means that the keystream used by the one-time pad must be free of any dependence patterns, i.e., it must be truly random, see Chap. 7.

1.2.2 Trends

The concept of the one-time pad offers an excellent pedagogical introduction to modern ciphers. However, in practice, its usage is rare and limited to circumstances where perfect secrecy is of utmost importance and integrity and authenticity can be guaranteed by other means.

Most current stream ciphers are simulations of the one-time pad: a random seed, e.g., a 256-bit sequence, is first defined, from which a deterministic pseudo-random keystream is then generated.

1.3 Consequences for Switzerland

The one-time pad should generally not be used, and standardized symmetric encryption algorithms should be preferred and used with the appropriate parameters

and the correct implementation, see Chap. 2. Its usage is costly, and its setup is complicated. Nevertheless, its use could be envisaged in particular government applications where perfect secrecy is a must. The key exchange shall be performed reliably, the keys securely stored until their use and systematically destroyed after encryption. Further measures are required to guarantee the communicating parties' authenticity and the encrypted messages' integrity.

The development of Quantum Key Distribution (QKD, see Chap. 9) renewed interest in the one-time pad [6], as keys could be shared on an interception-aware channel. In practice, however, attacks exist that take advantage of the redundancy of the signal [7], meaning that the one-time pad using QKD would not guarantee perfect secrecy.

1.3.1 Implementation Possibilities

A critical aspect in the application of the one-time pad is the quality of the source of randomness used to feed the keystream. It should be investigated and verified before use. The correctness of its implementation should be verifiable. In particular, the same key should never be re-used. The reliability of the key exchange mechanism should undergo a thorough investigation, and authenticity and integrity should be guaranteed to hold using different mechanisms.

The length of the key is a hindrance to using the one-time pad; if a secure channel exists to communicate a key of the same length as the message to be sent, this same channel could also serve to send that same message. Nevertheless, in the standard one-time pad setup, the secret key exchange would typically happen before the exchange of the message, thus providing a shift of secrecy through time. The one-time pad offers, however, neither authentication nor integrity.

The properties of the one-time pad make it hardly usable in practice, except in particular circumstances, typically in the government, and must be complemented by authentication procedures and integrity protocols.

1.4 Conclusion

The one-time pad is interesting from a theoretical point of view, but it could be more complex and questionable to use in practice. It is very appealing because of its perfect secrecy property. However, it lacks basic security properties shared by standard ciphers, namely authentication, and integrity. It needs to solve the central issue of the critical exchange between communication partners. Some secure stream ciphers simulations of the one-time pad should be preferred.

References

1. D. Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, New York, 2nd edition, 1996.
2. F. Miller. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. Charles M. Cornwell, New York, 1882.
3. Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. *Cryptologia*, 35:203–2222, 2011.
4. Mariusz Borowski and Marek Leśniewicz. Modern usage of "old" one-time pad. In *Military Communications and Information Systems Conference (MCC)*, pages 1–5. IEEE, 2012.
5. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
6. C. H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, 1984.
7. Miloslav Dušek, Ondřej Haderkaab, and Martin Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent state. *Optics Communication*, 169:103–108, 1999.