OTP and AES: A historical transition between two systems of cryptography

Valdemar Thanner
Kantonsschule Zug
supervised by Mr. Bernhard Keller

August 17, 2016

Contents

Chapter 1

OTP: The One Time Pad

1.1 What is a "One Time Pad"?

When speaking about OTP, it is important to distinguish between its two meanings: On the one hand, it is a technique used to encrypt information. This technique requires one single key, used both to encrypt and decrypt the information. This key is also referred to as a one time pad; therefore, it is important to distinguish between the one time pad (a cryptographical technique) and a one time pad (a key which is used to encrypt and decrypt information).

The One Time Pad is largely derived from the Vernam cipher, which is named after Gilbert Vernam. The Vernam cipher utilized a perforated tape (one of the earliest types of data storage) as the secret key[1].

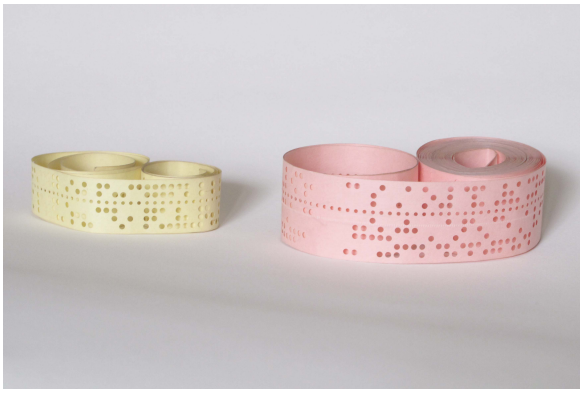

Figure 1.1: Perforated tape, utilized to store bits as punched holes

However, this system had a vulnerability which the One-Time Pad solved: In Vernam's original method, the perforated tape was not exchanged after it had completed one cycle; instead, it was looped around continuously, often being used multiple times on the same information.

1.2 Method used

1.2.1 Generation of the random key

In order to encrypt the plaintext, a key must first be generated. This key will be utilized to encrypt the plaintext through the usage of modular addition, turning it into the ciphertext.

This key must fulfil some crucial criteria. Foremost, the length of the key (the amount of characters contained within it) must be equivalent to or greater than the length of the plaintext; otherwise, it is not possible to perform any encryption (using the OTP). Secondly, the key must be generated randomly. This is mainly due to the fact that a randomly generated key makes frequency analysis[2], the form of cryptanalysis most commonly used to break classical ciphers, impossible.

1.2.2 Modular addition of the key and plaintext

Next, the ciphertext is created through modular addition of the key and the plaintext. This can be applied not only to a message consisting of alphabetical characters, but also to any sequence of bits. If the plaintext consists of a message made up of alphabetical characters, the plaintext and the key are added using arithmetic reffered to as *"addition modulo 26"*.

First, each character is assigned a number, in this case corresponding to it's position in the Latin alphabet:

1.2.3 decoding of the ciphertext using the key

1.3 Perfect secrecy: Information-theoretical security

1.3.1 definition

1.3.2 Why can only OTP achieve perfect secrecy?

1.4 Issues with OTP

1.4.1 True randomness in generating the key

1.4.2 Secure distribution of the key itself

1.4.3 Secure disposal of a utilized key

Bibliography

[1] G.S Vernam. "Secret Signaling system". Pat. U.S. Patent 1,310,719. 1919.

[2] learncryptography.com. *Frequency Analysis*. 2014. URL: `https://learncryptography.com/cryptanalysis/frequency-analysis`.