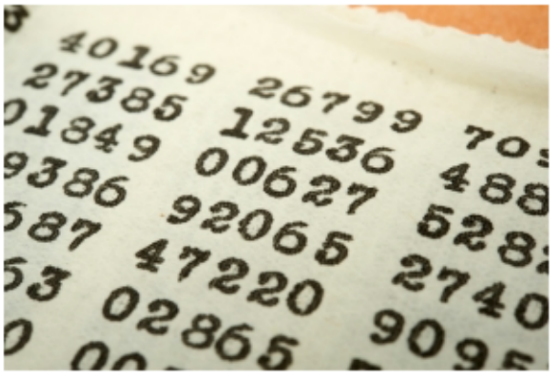
Homepage
Crypto
Index
Glossary
Enigma
Hagelin
Fialka
Rotor
Pin-wheel
TROL
Voice
Data
Hand
OTP
EMU
HSM
Mixers
Phones
Bulk
FILL
Codebooks
Algorithms
Chips
Cryptanalysis
Toys
World War II
Countries
Manufacturers
Spy radio
Burst encoders
Intercept

One-Time Pad OTP

The unbreakable code

The **One-Time Pad**, abbreviated **OTP**, is an encryption technique in which each character of the plaintext is combined with a character from a random *key stream*. Originally described in 1882 by banker Frank Miller (USA), it was re-invented in 1917 by Gilbert Vernam and Joseph Mauborgne. The OTP is named after the sheets of paper (pads) on which the key stream is usually printed. It can only be used once. When applied correctly, the OTP provides a truely unbreakable cipher. An automated form, used in combination with a teleprinter (telex), is known as *One Time Tape* (OTT).



The image on the right shows a page from a typical OTP booklet as it was used during the Cold War by Eastern-Bloc agents and spies, in particular by agents from the Soviet Union (USSR) and East-Germany (DDR). The booklet consists of a stack of very thin sequentially numbered pages, each of which contains a series of random 5-digit numbers. Each page could only be used once and had to be destroyed immediately after use.

OTPs of this type were often used in combination with Eastern-Block spy radio sets, such as the DDR Type 2 and the Russian R-353 (PROTON).

This section shows a selection of OTP systems from various sources and countries. Although the exact operating procedure varies between OTP systems, we will try to provide examples whenever possible. Original OTP booklets are extremely rare as they were normally destroyed after use. The surviving ones are generally held by the intelligence services that either used or confiscated them.

OTP systems on this website


USSR


CZ


OTT

Theory

With a one-time pad (OTP), the encryption key has at least the same length as the actual message (i.e. the plaintext) and consists of truely random numbers or letters. Each letter of the plaintext is 'added' to one element from the OTP using modulo-addition. When the key is unknown, this results in a ciphertext that has no relation with the plaintext. At the receiving end, the same OTP is used to retrieve the original plaintext. For this to work, the following rules are mandatory:

1. The OTP should consist of truely random characters (noise).
2. The OTP (i.e. the key) must have at least the same length as the plaintext.
3. Only two copies of the OTP exist.
4. The OTP can be used only once.
5. Both copies of the OTP are destroyed immediately after use.

When the above rules are strictly obeyed, the OTP is absolutely safe. Combining numbers with the plaintext manually, is a time-consuming task. It is therefore sometimes thought that OTPs are no longer practical. With modern computer technology however, the entire task of enciphering and deciphering can easily be automated, just like it was done in the past on teleprinter systems.

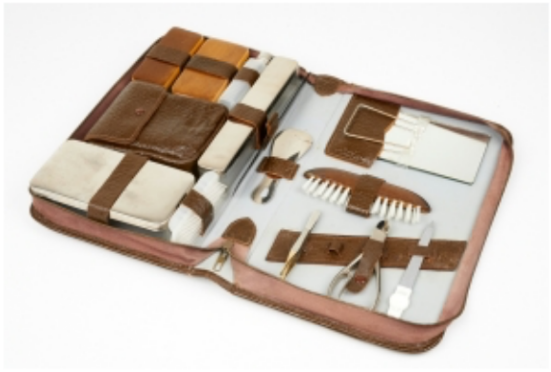
Although it may sound strange, manual OTP ciphers are still being used today (2015) for sending secret

messages to agents (spies) via the Numbers Stations, or One-Way Voice Links (OWVL), that you may have heard on the short-wave radio bands. For a detailed description of the One-Time Pad Cipher and its history, complete with numerous examples, we would like to recommend the excellent paper *Secure Communications with the One Time Pad Cipher*, by Dirk Rijmenants [3].

➤ Read now (off-site)

Distribution

The major disadvantage of the OTP, is the logistical problem of its distribution. A unique pair of OTP booklets must be issued and distributed to each individual agent abroad. As the OTP will be destroyed immediately after use, sufficient and timely supply of new OTPs has to be guaranteed.



During the Cold War, OTPs were often smuggled into a country by means of a concealment, such as the one shown in the image on the right. This regular travel kit was cleverly converted into a concealment device by the East-German Stasi.

➤ More information

Concealment

Another popular method for distributing and hiding OTP booklets, was by printing them at very small size and hiding them inside common objects like ballpoints, photoframes and, as shown in the image on the right, inside a walnut.

For many years, the walnut concealment was very popular with KGB agents in Western Europe, until it was discovered by the West-Germans.

➤ Walnut concealment
➤ Other concealments

Variations

OTP systems come in many forms and flavours, but most of them consist of either **numbers** or **letters**. An OTP based on numbers is also known as a One-Time Figure Pad (OTFP). When sending text, each letter of the plaintext has to be converted into a number before applying the OTP.

An OTP based on letters is also known as a One-Time Latter Pad (OTLP). An example of an OTLP is shown in the image on the right. It consists of a stack of ~ 30 pages that are stapled together. The conver (just visible at the left) holds a folded alphabet that is used in the translation process.

Some OTPs are so small that they can easily be hidden inside a small object. More examples and detailed photographs below. Some OTPs are so small that they can be fitted inside a slide frame.

Compromise

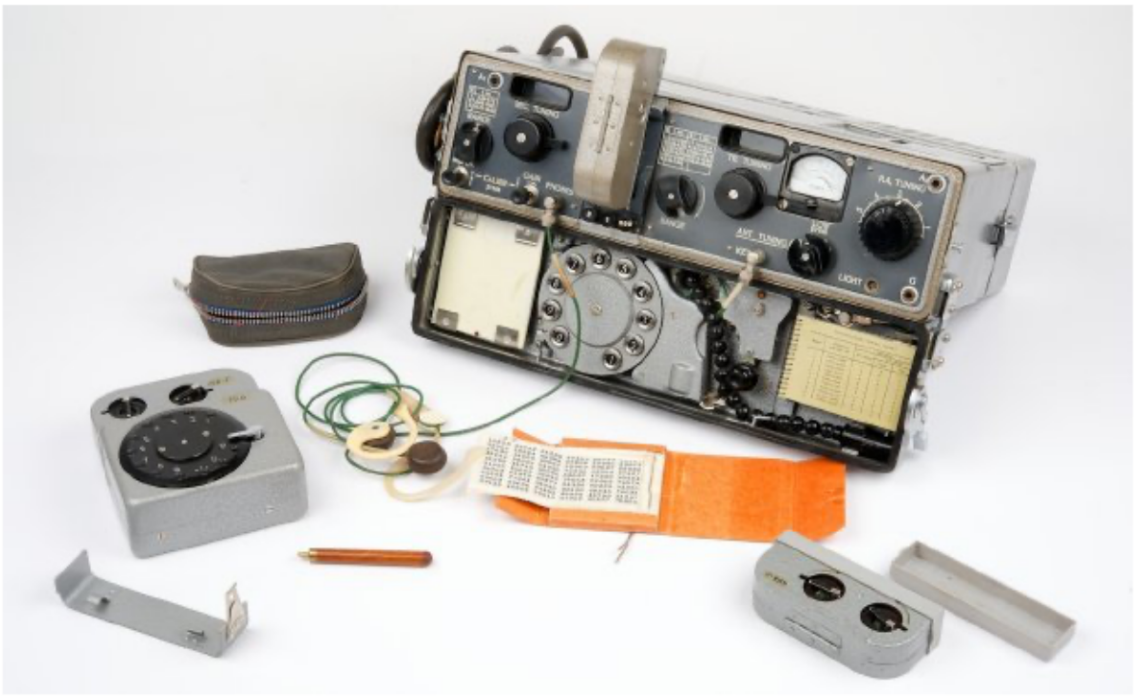
When used properly, OTPs are inherently safe. But when they are used incorrectly, e.g. by reusing them, they can be a cryptologic nightmare. A good example of improper use is described by Matt Blaze in an article about the book *Compromised* by former FBI counterintelligence agent Peter Strzok [4]. He describes how secret OTP-encrypted messages were sent to Russian illegals [1] in the US, via a Numbers Station in Cuba which had a good coverage throughout the US.

The station would broadcast message in morse code and voice 24 hours a day, interleaving real messages with dummy traffic, so that it was not revealed to an interceptor how often and how many real messages were sent. However, the FBI discovered (as did others) that dummy traffic could easily be discriminated from real traffic, as it did not contain the number 9. This was probably caused by a faillure of the random number generator used for the dummy traffic, or a bug in the software that handled it. With this knowledge, the FBI was able to correlate the real messages to the times that messages were decoded by a Russian illegal couple they had under surveillance. It eventually led to the arrest of an several Russian illegals in the US and Canada.

1. In the espionage trade, an **illegal** is a foreign person who lives in a country under a false or assumed identity, also known as a *legend*, for the purpose of spying.

Capture

OTP booklets, such as the one shown above, have been captured during the Cold War by Western intelligence agencies on a number of occassions. One documented example is the capture of a Dutch man, who acted as an East-German agent in The Netherlands, in 1969. When he was finally exposed, the Dutch intelligence service BVD (now: AIVD) found a partly used OTP booklet in his home, along with a fully operational R-353 spy radio set, a burst encoder and cassettes [5].



➤ More about the R-353 radio

References

1. Detlev Vreisleben, *Personal collection of One-Time Pads*
Photographed by Crypto Museum. Köln (Germany), 20 March 2010.

2. Wikipedia, *One-time pad*
Retrieved January 2013.

3. Dirk Rijmenants, *Secure Communications with the One Time Pad Cipher*
Paper (English) 2009-2014. Version 6.2, 18 December 2014.

4. Matt Blaze, *A Cryptologic Mystery*
18 September 2020.

5. AIVD, Short description and image of captured R-353
Website. Retrieved November 2009.

Further information

- Morse code
- The Vernam Cipher
- One-Time-Tape (OTT)
- One-Time Pad on Dirk Rijmenant's website
- One-Time Pad on Wikipedia
- Main Crypto Page