MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

M-138 – Part 1

Author: Klaus Schmeh

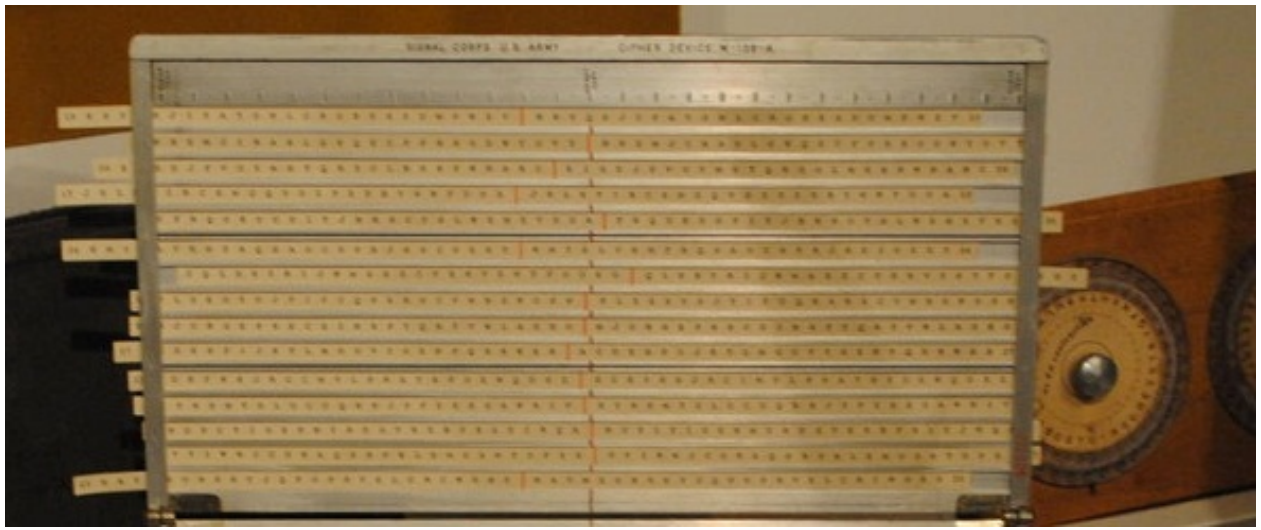
November 2014

Introduction

The M-138 (also known as CSP-845) is a strip cipher used by the US Armed Forces in the first half of the 20th century.

The purpose of the M-138 was to provide reasonable cipher security at low costs. It was not a high security system. It was used when a cipher machine (for instance the M-209 or the SIGABA) was not available. This happened quite often, as cipher machines were by orders of magnitude more expensive than strip ciphers and harder to transport. Before and at the beginning of WW2, a great deal of reliance was placed on the M-138 because of the shortage of cipher machines. Later it remained in use as a backup system. The M-138 was a very cheap tool (consisting only of paper strips and a simple frame) that was easy to carry and to operate, and it provided good security given the circumstances.

We do not know any publications about the cryptanalysis of M-138. It would be interesting to find out how much effort it takes to break an M-138 message, if this effort was realistic for a codebreaking unit in WW2, and whether the M-138 could have been improved significantly without major effort (for instance by putting 30 strips into the frame instead of 25).

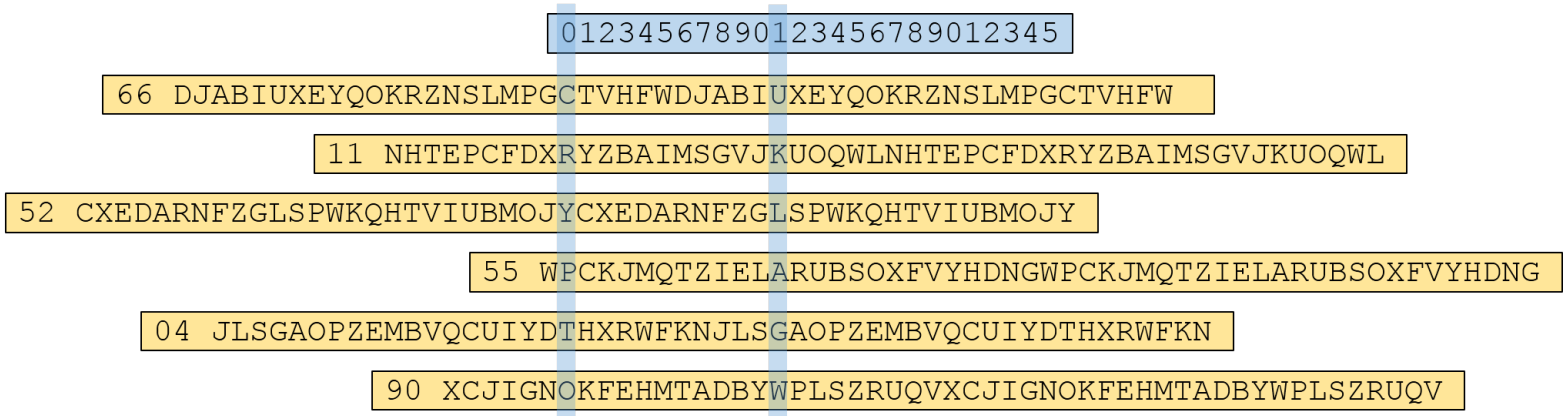


(Picture: Author)

Feel free to discuss these aspects in our forum and to share your research.

Example

In this series of challenges, a fictitious model of the M-138 is used: the used 100 strips are different from the original M-138 device. The strips used are given in the additional file. On each strip the 26 capital letters of the alphabet are printed twice in random order. For encryption, up to 25 strips are chosen from the strip set and placed in the frame. In the following example, the strips 66, 11, 52, 55, 04 and 90 of the fictitious M-138 version have been chosen to encrypt the word CRYPTO.



MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

The key in this example is $(66, 11, 52, 55, 04, 90/11)$. The key consists of the numbers of the used strips followed by the offset between the plaintext column and the ciphertext column. During one encryption process with the M-138 the same offset is used for all strips. In this example the ciphertext is `UKLAGW`. The number of strips used may not exceed 25 (only 25 strips fit into the frame). No strip may be put into the frame twice. This means that a key like $(20, 12, 20, \ldots)$ is not allowed.
If the plaintext is longer than 25 letters, it must be divided into blocks of 25 letters. Each of the blocks is encrypted in the same way as in the smaller example above. The key remains the same for all blocks of the plaintext.

Challenge

The ciphertexts given in this M-138 series have been generated with the fictitious M-138 model. It is your task to break the encryption and find the English plaintext.
Part 1 is the easiest part of the series, as a greater part of the key is known. The key is (46, 59, 09, 13, 08, 90, 30, 34, 62, 83, 51, 55, 49, 88, 27, 92, 69, 40, 74, 17, 21, 71, 45, 79, 96 / xy). So, all strip numbers are known and from the key only the offset (here labeled as xy) has to be found. The plaintext contains 25 characters, thus every selected strip is used once.
As solution, please enter the plaintext in capital letters and without spaces.

Ciphertext:
`SQRXS VNMWZ PZXSX UPSXJ IYBYA`

Annotations – Part 1

- The M-138 is mathematically similar to the well-known Enigma. Both machines use the substitution of single letters. However, the M-138 does not work electro-mechanically and the substitution of one letter depends on only one strip, not on all rotors. There is nothing comparable to the stepping of the rotors.
- The M-138 has been used in two versions: At first with 25 strips, later with 30 strips. The challenge at hand uses 25 strips.

Annotations – Part 2

- The M-138 is a variant of the Vigenère cipher – random "alphabets" are used instead of sorted ones.
- M-138 has remodeled the monoalphabetic substitution in a similar way as Vigenère improved the Caesar cipher.
- In this challenge, the attacker knows all the 100 strips (and which ones have been used in which order). It would be much more difficult, if he did not know the strips.

Sources

This series is based on Klaus Schmeh's blog:
http://scienceblogs.de/klausis-krypto-kolumne/m-138-challenge/

For further information on the original M-138, we recommend:
http://maritime.org/tech/csp845.htm

Information on Venus (M-138-A):
http://www.jproc.ca/crypto/venus.html