MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

M-138 – Part 4

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.

Challenge

The ciphertexts given in this M-138 series have been generated with a fictitious M-138 model. The strips used are given in the additional file. It is your task to break the encryption and find the English plaintext. The ciphertext of part 4 consists of 75 letters which means that each strip in the frame is used three times. The plaintext is completely unknown.
This part of the series eventually cannot be solved uniquely.
As solution, please enter the plaintext in capital letters and without spaces.

Ciphertext:
PTIJJ HDJPK YTMTK UVEPD HYKLH DEYMG LIJLN WKXVG ZILQN
CJRHW JNBJF UAQHN BJGXW ZBESX NXPZH

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

The template of part 1 of this series also contains some more details and an example of this cipher.