Short description of the Geheim-schreiber

Johan Håstad

January 23, 2008

The Geheimschreiber had 10 wheels of lengths, 47,53,59,61,64,65,67,69,71, and 73 respectively. Each position on each wheel contained a bit. The plain-text and crypto-text alphabets were given by the string

2T3O4HNM5LRGIPCVEZDBSYFXAWJ6UQK7.

Thus the character '2' corresponded to the integer 0, 'T' corresponded to 1 and so forth with '7' corresponding to 31. Thus, each letter corresponded in a natural way to a 5-bit integer.

Each day a fixed permutation of the wheels was chosen e.g. it could be that the wheel of length 71 was put in position one, the wheel of length 59 was set in position two etc. This remained fixed for the day.

When encrypting a message each wheel was set to a starting position given by a key list. We here assume that the starting position was agreed between the sender and receiver and that it was unique for each message. In some situations some of the positions were transmitted as part of the message but this is not the case for our messages.

Encryption was performed as follows.

1. Read one bit from each of the ten wheels getting bits b_0, b_1, b_2, b_3 b_4, b_5, b_6, b_7 b_8, and b_9.
2. Use the given alphabet to convert the clear-text character to a number between 0 and 31 and let c_0, c_1, c_2, c_3, and c_4 be the bits of this number with c_0 giving the least significant bit.
3. For $i = 0, \ldots 4$ $c_i = c_i \oplus b_i$, i.e. take xor.
4. If b_5 is 1 interchange c_0 and c_4.

5. If b_6 is 1 interchange c_0 and c_1.

6. If b_7 is 1 interchange c_1 and c_2.

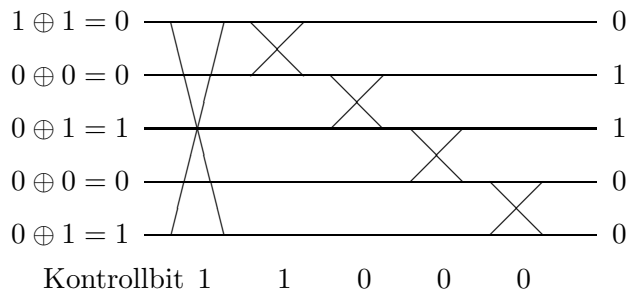
7. If b_8 is 1 interchange c_2 and c_3.

8. If b_9 is 1 interchange c_3 and c_4.

9. Output the character corresponding to the integer with the binary expansion $c_4c_3c_2c_1c_0$ with c_0 being the least significant bit.

Before the next character was encrypted each wheel is stepped one step.

Example: Encrypting "T" (1 = 00001) under the bits 10101 11000 from the wheels gives the following picture.



This prints the letter "N" (6 = 00110) on the output.