INF247 Mandatory Assignment 1: G-Shcreiber Known Plaintext Attack

Eirik D. Skjerve

2024

1: Known plaintext attack against its internal settings

1. Find cabling and 0-1 distribution on first five wheels:

   - Find positions in ciphertext where ciphertext 5-bit group is "00000" or "11111". Then we know input to the relay box will also be "00000" or "11111" respectively. Since we know plaintext at those positions, we can retrieve the first 5-bit group by xor-ing the relay input ("00000" or "11111") with the plaintext code at that time.
   - Next we find the correct cabling from the 5-bit group to the wheels. For each position in the 5-bit group (1,2,3,4,5), we find a pair of 5-bit groups, and check if the bit is different when their times are congruent modulo period of a wheel. If the bit is different for a period p, then we eliminate the possibility of a cable between that bit position and the wheel with period p. We do this for every wheel/period and every bit position. In the end, if plaintext/ciphertext is long enough, we see that there is only one possible cabling between each bit position and a wheel.
   - When we know the cabling for the first 5-bit group, it is easy to reconstruct the 0-1 distribution on the relevant wheels, by going through the plaintext/ciphertext, and inserting into the wheels the correct bit on the correct position on the wheel. At this point 0-1 distribution on first five wheels should be known.

2. Find control bits for relay box, cabling and 0-1 distribution.

   - We locate times in the ciphertext where the code is a 5-bit group of weight one or weight 4 (e.g. "10000", "01111"). Since we know the bits in the first 5-bit group for those times, we also know the input to the relay box at that time.
   - By constructing a table of possible control-bits for specific 1/4-weight input/output pairs, we can decide some control bits for those moments. For example, a specific input/output pair can yield control bits "101xx". The we can place the bits "1","0" and "1" with certainty, while the remaining bits ("x") are still unknonw.

- Next we test periodicity on these bits aswell, like in the previous step. Then we should know the cabling from the last 5-bit group to the remaining wheels.
- If plaintext/ciphertext is long enough we should be able to retrieve the 0-1 distribution for the last 5 wheels aswell.

2: Attack in practice