MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Purple I

Author: Mark Stamp

October 2010

Purple encryption

The Purple machine was the Japanese counterpart of the German Enigma machine before and during World War 2.
The Purple machine consists of 3 stepping switches named L (left), M (middle) and R (right), which step with different speed and which can be arranged in different sequences.
Each switch permutates the 26 capital letters. There is a 4th switch S (stepping) which is fixed, but all 4 stepping switches do have 26 different initial positions (from 1 for A to 26 for Z).
Furthermore, the Purple machine has two plugboards which perform an initial and a final permutation of the 26 letters of the alphabet. In the former practical case and in this challenge these two permutations are the same.

Challenge

Decrypt the ciphertext (*purpleCipher.txt*) which can be found in the zip archive of this challenge. This ciphertext was encrypted with the Purple machine. Furthermore, there is an implementation of the Purple encryption (*Purple_code.zip*) written in C.

The solution for this challenge consists of the initial permutation, the order of the 3 stepping switches L,M,R and the initial position of each of the 4 switches.

If the initial permutation was the identity, the order of the 3 stepping switches was *LMR* and the initial position of all of the 4 switches was *1*, the solution would be **ABCDEFGHIJKLMNOPQRSTUVWXYZLMR1111**.