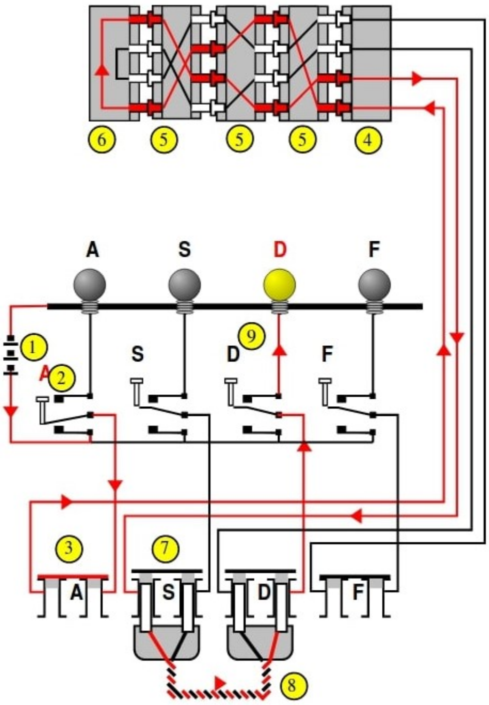
# Problem 5. «An Enigmatic Challenge»

The Enigma machine is a symmetric cipher famous for being during the Second World War by the German military. Its internal structure comprises an 26-letter Latin alphabetic permutation, implemented as rotors. The machine used for this problem consists of 3 **rotors** and a **reflector**.

The figure shows how a simplified Enigma machine works. The key components are the set of input switches (2) – which are reduced to 4 in the example but could have been 26 for the Latin alphabet – an input plugboard (3,7,8), three rotors (5), the reflector (6) and the output board (9).

The components have the following functionality:

- **Rotors:** a rotor (5) is a wheel with the uppercase alphabet in order on the rim and a hole for an axle. On both sides of a rotor are 26 electrical contacts each under a letter. Each contact on one side is wired to a contact on the other side at a different position. The rotor implements an one-to-one and onto function between the upper-case letters, where each letter is mapped to a different one (an irreflexive permutation).
- **Reflector:** the reflector (6) is positioned after the rotors and has contacts for each letter of the alphabet on one side only. The letters are wired up in pairs, so that an input current on a letter is reflected back to a different letter.



**The input message:** is permuted by the rotors, passes through the reflector and then goes back through the rotors in the reverse order (as depicted in the figure). Finally, the light bulb indicates the encrypted letter. The plugboard plays no role in permuting the letter for this challenge, although it could have.

Turn to the next page.

To prevent simple frequency analysis attack the right rotor rotates with every new input. After the right rotor completed a full rotation (after 26 letters were encrypted), the middle rotor rotates once. Similarly, after the middle rotor completes a full rotation (and the right rotor complete 676 rotations), the left rotor rotates once.

**Challenge:** you will play the role of an attacker that knows the source of the plaintext to be encrypted. You are given a ciphertext corresponding to a plaintext taken from this known source which happens to be "Moby Dick" by Herman Melville, and you are asked to recover the plaintext. The plaintext consists only of trimmed capital letters with no punctuation marks and spaces and is contiguous. All letters are from the Latin alphabet. Extra information on the settings of the rotors is provided: the configuration of the first rotor is very close to the one used in the 1930 commercial version: `EKMFLGDQVZNTOWYHXUSPAIBRCJ`.

**Ciphertext:**

```
RHSM ZHXX AOWW ZTWQ QQMB CRZA BARN MLAV MLSX SPBA ZTHG
YLGE VGZG KULJ FLOZ RQAW YGAA DCJB YWBW IYQQ FAAO RAGK
BGSW OARG EYSP IKYE LLUO YCNH HDBV AFKD HETA ONNR HXHE
BBRT ROZD XJCC OMXR PNSW UAZB TNJY BANH FGCS GJWY YTBV
VGLX KUZW PARO NMXP LDLZ ICBK XVSJ NXCF SOTA AQYS YZFX
MZDH MSZI ABAH RFXT FTPU VWMC PEXQ NZVA LMFX BHKG QGYS
BIYE MEUE PJNR AVTL JSUZ PLHQ MOUI IQFD HVXI NOOJ YJAF
 WAVU PVQA FMKP AHLK XJYD GITB QSPK CUZU XPRK MUJJ YRJ
```

**Link to "Moby Dick" text file:** click here.