## Tema laborator 2

## Criptografie si Securitate

1. De la primul exercitiu avem permutarile ciclice(prima litera cu a patra, a doua litera cu a cincea si a treia litera cu a sasea). Gasesc 2 permutari similare:

|  |  |
| --- | --- |
| Permutarile gasite la exercitiul 1 | |
| AVCMSOJWURKZL | BHIYETFGPDNQX |
| Permutarile similare din tabel | |
| AVRMSTJWUCKZL | BHIPEOFGYDNQX |

1. Avand in vedere permutarile gasite la exercitiul 3, vedem urmatoarele conexiuni intre perechile de permutari:

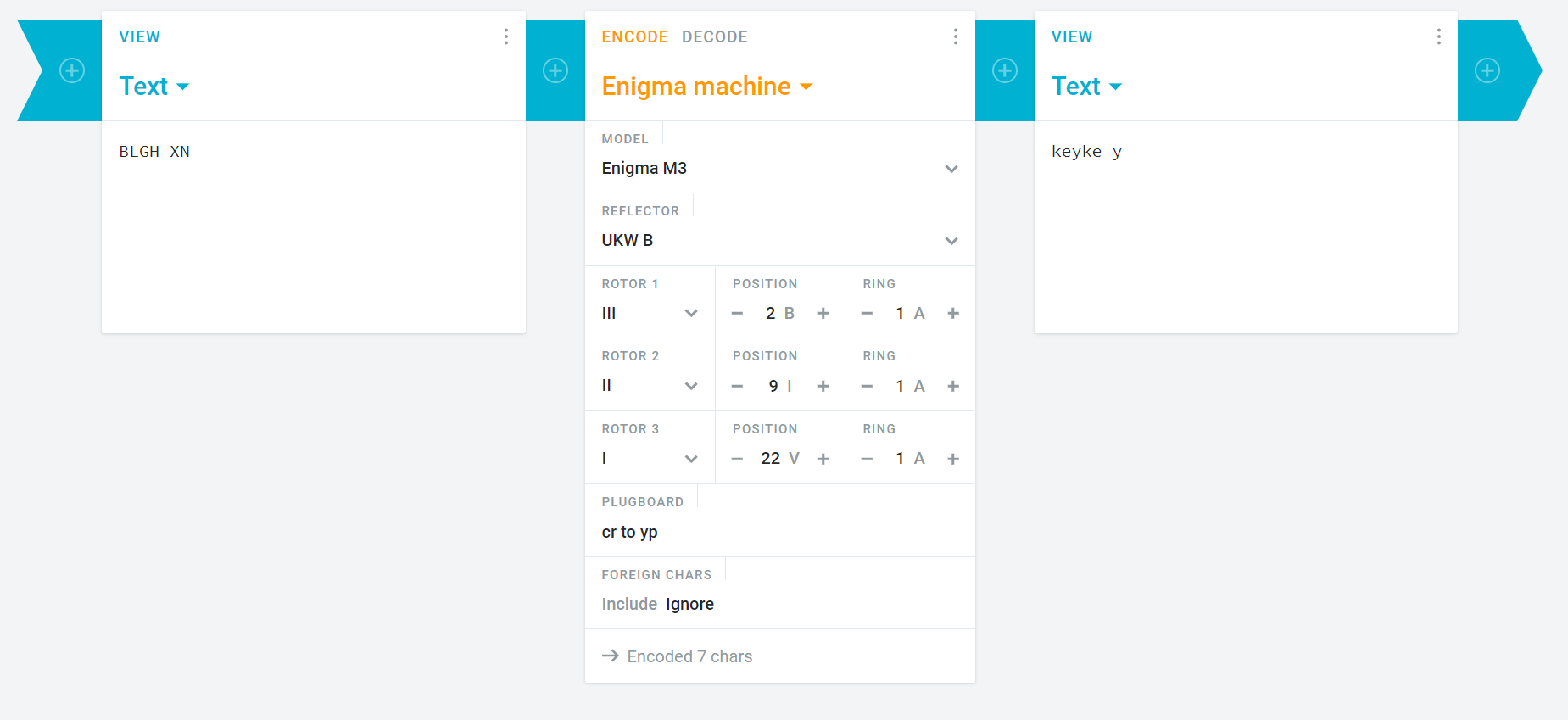
C <-> R si T <-> O pentru prima pereche de permutari

Y <-> P pentru a doua pereche de permutari

* Tabela de conexiuni este CR, TO si YP

1. Mesajul interceptat: ***BLGH XNST PVBX WMUZ P***
   1. Ordinea rotorilor este : III, II, I
   2. 1, 1, 1
   3. Pozitia intiala a rotorilor: Schluessel
   4. Tabela de conexiuni: CR, TO, YP
   5. Reflectorul UKW B

Mai intai aflu cheia: este KEY



Dupa care decriptez mesajul cu KEY si se obtine mesajul clar: NEXT ATTACK