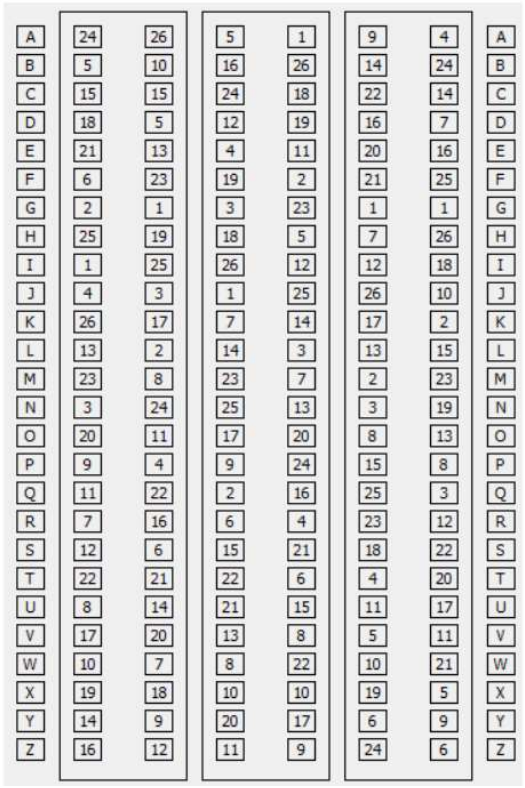
1. (**20p**) Na slici je prikazana trenutna konfiguracija rotor mašine. Prikazati postupak šifrovanja poruke *NEBO JE VEDRO* koja predstavlja deo neke veće poruke, ukoliko se zna da je do ovog trenutka šifrovan 671 karakter.



2. (**15p**) Objasniti šta su i kako se koriste autentikacioni kodovi poruka (MAC). Objasniti koje su osobine MAC i koji su zahtevi za MAC? U čemu su osnovne sličnosti i razlike u odnosu na digitalno potpisivanje?

3. (**15p**) Na slici je prikazano poboljšanje Needham-Schroeder protokola koji je predložila Denning:

1. $A \rightarrow KDC: ID_A || ID_B$
2. $KDC \rightarrow A: E_{Ka}[K_s || ID_B || T || E_{Kb}[K_s || ID_A || T]]$
3. $A \rightarrow B: E_{Kb}[K_s || ID_A || T]$
4. $B \rightarrow A: E_{Ks}[N_1]$
5. $A \rightarrow B: E_{Ks}[f(N_1)]$

a) (10p) Objasniti čemu služi ova šema, koji entiteti komuniciraju, koje su uloge entiteta, kao i koja je svrha svih elemenata poruka koje se razmenjuju?

b) (5p) Objasniti na koji način ova šema sprečava Replay napade i koji tehnički preduslovi treba da budu ispunjeni za to?

4. (**15p**) U SMIME protokolu moguće je korišćenje više različitih algoritama da bi se podržale funkcionalnosti (formiranje hash-a poruke, enkripcija ključa, enkripcija poruke, ...). Objasniti kako se pri slanju poruke za koju su obezbeđene neke od mogućih funkcionalnosti odlučuje koji algoritmi se koriste.

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 150 minuta.*