

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. $KDC \rightarrow A: E_{K_a}[K_s || ID_B || T || E_{K_b}[K_s || ID_A || T]]$
3. $A \rightarrow B: E_{K_b}[K_s || ID_A || T]$
4. $B \rightarrow A: E_{K_s}[N_1]$
5. $A \rightarrow B: E_{K_s}[f(N_1)]$

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.

A	24	26	5	1	9	4	A
B	5	10	16	26	14	24	B
C	15	15	24	18	22	14	C
D	18	5	12	19	16	7	D
E	21	13	4	11	20	16	E
F	6	23	19	2	21	25	F
G	2	1	3	23	1	1	G
H	25	19	18	5	7	26	H
I	1	25	26	12	12	18	I
J	4	3	1	25	26	10	J
K	26	17	7	14	17	2	K
L	13	2	14	3	13	15	L
M	23	8	23	7	2	23	M
N	3	24	25	13	3	19	N
O	20	11	17	20	8	13	O
P	9	4	9	24	15	8	P
Q	11	22	2	16	25	3	Q
R	7	16	6	4	23	12	R
S	12	6	15	21	18	22	S
T	22	21	22	6	4	20	T
U	8	14	21	15	11	17	U
V	17	20	13	8	5	11	V
W	10	7	8	22	10	21	W
X	19	18	10	10	19	5	X
Y	14	9	20	17	6	9	Y
Z	16	12	11	9	24	6	Z

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