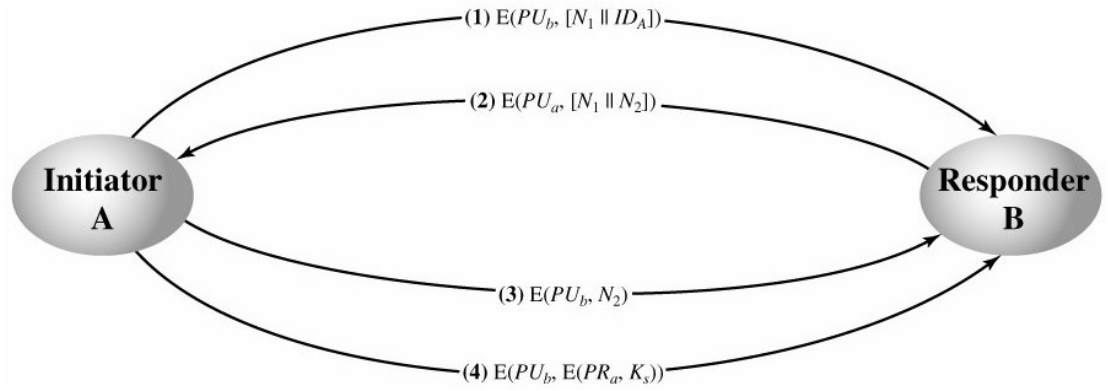
1. Upotrebom *Playfair* algoritma šifrovati poruku VENI VIDI VICI. Za šifrovanje izabrati jedan od ponuđenih ključeva tako da on najviše doprinosi sigurnosti: ANANAS, IRITIRATI, SUNCE. Obrazložiti izbor. Poruka se sastoji isključivo od slova engleskog alfabeta. Uzeti da se I i J mapiraju kao jedno slovo. Prikazati postupak šifrovanja.
2. Za originalnu poruku 24BBh i ključ 1A73h prikazati šifrovanu poruku nakon prve iteracije *S-AES* algoritma. Postupak prikazati po koracima. Parametri algoritma su dati u prilogu.
3. Na koje tipove napada u kriptoanalizi kriptografski algoritam treba da bude otporan da bi se smatrao sigurnim za upotrebu? Koji od tih napada uspeva kod *Hill*-ove šifre i na koji način se izvodi?
4. Na slici je data šema razmene simetričnog sesijskog ključa.



   a) Šta je potrebno da uradi napadač M kako bi izvršio *man-in-the-middle* napad?
   b) Prikazati šemu razmene poruka u ovoj razmeni ključeva između A, B i M u situaciji kada M izvršava *man-in-the-middle* napad.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 90 minuta.

Prilog. Parametri *S-AES* algoritma

	00b	01b	10b	11b
00b	9h	4h	Ah	Bh
01b	Dh	1h	8h	5h
10b	6h	2h	0h	3h
11b	Ch	Eh	Fh	7h

a)

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

b)

Slika 1. Prikaz *S-box* tabele (a) i koeficijenata matrice za operaciju mešanja kolona (b) kod *S-AES* algoritma

Kod operacije mešanja kolona koristi se aritmetika u polju $GF(2^4)$ po modulu x^4+x+1. Kod ekspanzije ključa konstante iteracije koje se koriste u funkciji *g* su: Rcon(1)=80h i Rcon(2)=30h.