

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 3.30

1. Dekriptirajte šifrat

OCRAJ ODTJR TREKS REVJN ZAPAJ EDFVS
JAE0E SEOAN RSISI SAINO TISAF KIEVS
DTKEO FJAAT SO

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca veći od 4, a manji od 16.

2. Dekriptirajte sljedeća dva šifrata

RWGJTSH
UQATKUM

ako je poznato da su dobiveni istim ključem po pravilu

$$y_i \equiv x_i + k_i \pmod{26}.$$

Također je poznato da su oba otvorena teksta riječi na hrvatskom jeziku koje počinju jednim od slova S, P, N, D.

3. Odredite skupove $test_1(E_1, E_1^*, C'_1)$ i $test_2(E_2, E_2^*, C'_2)$ ako je

$$E_1 = 000110, \quad E_1^* = 110010, \quad C'_1 = 1000,$$

$$E_2 = 001000, \quad E_2^* = 111100, \quad C'_2 = 1000.$$