

KRIPTOGRAFIJA I SIGURNOST MREŽA

zadaca 3.63

1. Dekriptirajte šifrat

SITIJ EIFAI NHNMJ IORVE IUWOU ORKOD
BLDTE SSNJT LRTIE EIZRJ IATCL TZRFE
KOAZH AAJOA AISAA IJ

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

SBPDIMW
UMJZQWW

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

$$E_1 = 001001, \quad E_1^* = 111101, \quad C'_1 = 0001,$$

$$E_2 = 000010, \quad E_2^* = 110110, \quad C'_2 = 0100.$$