

KRIPTOGRAFIJA

Zadaća 3.146 X

Rok za podizanje zadaće je od 15.04.2005. do (uključivo) 29.04.2005. Rok za predaju ove zadaće je 06.05.2005.

1. Dešifrirajte šifrat:

LCINC JALOA NULAR DOJEK OSDEE MOOVL JSPIO FLKIA
OSNLK VRUSR AIONU SEDZT VUTMN GEMOT TNIJJ EMOUU
OOJIA ARCJI EIJRA OUDNA IARIV KARRE FVSVN UOOVL
KIEOI BTANK ECNAO JTAJT PIUM

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca između 4 i 16.

2. Dešifrirajte sljedeća dva šifrata:

GOMRB JSP
VIZUS NAN

ako je poznato da su dobiveni istim ključem po pravilu

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

Oba teksta počinju jednim od slova d, i, n, o, p, s.