KRIPTOGRAFIJA

Zadaća 3.176 X

Rok za podizanje zadaće je od 05.05.2006. do (uključivo) 12.05.2006.
Rok za predaju ove zadaće je 19.05.2006.

1. Dešifrirajte šifrat:

   ```
   AIDPM NSGDS PUIIU UESOT OSLRM SDEHP EIOOA RMCTO
   SUVVI OABTZ SOMOO RZSCN DVLPO UALET EONDP AIOOK
   INMIL MTNOE ITTNK NFFNL EOADN LNAEE ORIOS HMRZE
   AESVI PEUMU DREBT JDTBA ZSOSA AKOII IELLN FAJEI
   TNIUL DKKOR JETOD EPUOO UP
   ```

   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:

   ```
   JZNVA IMW
   IAIFJ VTB
   ```

   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`.

3. Odredite skupove $test_1\left(E_1, E_1^*, C_1'\right)$ i $test_2\left(E_2, E_2^*, C_2'\right)$ ako je

   $$\begin{aligned} E_1 &= 111110, \quad E_1^* = 101010, \quad C_1' = 1001 \\ E_2 &= 001000, \quad E_2^* = 010100, \quad C_2' = 0001 \end{aligned}$$

4. Izračunajte:

   $$(\texttt{0xe2}, \texttt{0x34}, \texttt{0x56}, \texttt{0x78}) \otimes (\texttt{0x1a}, \texttt{0x2b}, \texttt{0x3c}, \texttt{0x4d}).$$

   Ove vektore pretvaramo u polinome kao na sljedećem primjeru

   $$(\texttt{0x33}, \texttt{0x22}, \texttt{0x11}, \texttt{0x00}) \mapsto \texttt{0x33}x^3 + \texttt{0x22}x^2 + \texttt{0x11}x + \texttt{0x00}.$$

   Koeficijenti ovih polinoma su elementi ranije spomenutog polja $\mathrm{GF}(2^8)$ zapisani heksadecimalno. Npr. $\texttt{0x85} = 1000\,0101_2 \mapsto x^0 + x^2 + x^7 = 1 + x^2 + x^7$.