

KRIPTOGRAFIJA

zadaća 2.01

1. Šifrirajte otvoreni tekst

CHARLES BABBAGE

pomoću Playfairove šifre s ključnom riječi CRYPTOGRAPHY.

2. Odaberite neku involutornu 2×2 matricu $K = (k_{ij})$ (tj. takvu da je $K^{-1} = K \pmod{26}$) i to takvu da su svi $k_{ij} \neq 0$. Odaberite proizvoljni otvoreni tekst od 6 slova, te ga šifrirajte Hillovom šifrom s ključem K .
3. Odredite ključ K u Hillovoj šifri ako je poznato da je $m = 2$, te da otvorenom tekstu

VERNAM

odgovara šifrat

TNUXCS.