

Salausmenetelmät, Harjoitus affinin järjestelmän murtaminen

1. Avaa Caesarin yhteenlaskumenetelmällä laadittu englanninkielinen salakirjoitus

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDL R PD.

2. Tehtäväsi on selvittää affiinilla järjestelmällä tehty salakirjoitus, jossa käytetään 37-kirjaimista aakkostoa, jonka kirjaimet ovat luvut 0–9 (vastaavat lukuja 0–9), englanninkieliset aakkoset A–Z (vastaavat lukuja 10–35) ja väli (=36). Salakirjoitusteksti on

OH7F86BB46R36270266BB9.

Tiedät, että viestin on lähettänyt 007. Mikä on viesti?

3. Avaa Caesarin kertolaskumenetelmällä laadittu suomenkielinen salakirjoitus HMLVLHOKMHFARRGVTA.