Cifrarea prin substituție poligrafică bazată pe algebra liniară

Algoritmul de cifrare Hill este o metodă de substituție poligrafică bazată pe calcule în algebra liniară modulo P.

În acest sistem, delimitatorul de spațiu dintre cuvinte poate fi ignorat ori înlocuit cu caracterul cel mai puțin utilizat (în limba română, acest caracter este „*Q*").

Algoritmul procesează un bloc de date *M* cu *n* caractere (litere); cheia de cifrare este o matrice *K* formată din *n* linii și *n* coloane, inversabilă în mod *P*.

Regula de cifrare este $C = MK$, iar regula descifrării este $M = CK^{-1}$.

Tematică de cercetare:

1. Imaginați un exercițiu de cifrare în care să arătați unde intervine condiția ca matricea K să fie inversabilă (se exclude matricea nulă).

2. Având două căi de criptare, K_1 et K_2, stabiliți legătura între mesajele MK_1, MK_2, MK_1K_2 și MK_2K_1.

3. Realizați un cod secret de criptare bazat pe algoritmul Hill în care să apară patru emotigrame (engl.= emoticons) și cifrați mesajul:

EU LUCREZ CU MARE PLĂCERE LA PROIECTUL MATH EN JEANS

4. Studiați în ce constă metoda transpoziției și cercetați dacă securitatea codificării (confidențialitate, autenticitate, integritate) este îmbunătățită dacă sunt aplicate succesiv mai multe transpoziții.

5. Găsiți o metodă de criptare prin combinarea algoritmului Hill cu metoda transpoziției și studiați dacă aplicarea simultană a celor două metode este comutativă.