CZU: 004.056.55:512.64

APLICAȚIILE ALGEBREI LINIARE ÎN SISTEMUL DE CRIPTARE HILL ȘI ÎN CEL DE PERMUTARE

Dorin AFANAS, dr., conf. univ.
Vasile NICHIFOROV, masterand, anul II
Universitatea de Stat din Tiraspol

Rezumat. Algebra liniară are aplicații în diverse domenii: geometria analitică, analiza funcțională, științele naturale, științele sociale, economie, etc. În prezentul articol sunt cercetate aplicațiile algebrei liniare în sistemul de criptare Hill și în cel de permutare. Sunt prezentate metode de criptare și metode de decriptare a mesajelor. La baza metodelor prezentate se află noțiunile de *modulo p* și *matrice*.

Abstract. Linear algebra has applications in various fields: analytical geometry, functional analysis, natural sciences, social sciences, economics, etc. This paper investigates the applications of linear algebra in Hill encryption and permutation. Encryption methods and message decryption methods are presented. At the base of the presented methods are the notions of *p-module p* and *matrix*.

Cuvinte cheie: criptare, decriptare, modulo p, matrice, cifru, criptotext.
Keywords: encryption, decryption, p-module, matrix, cipher, cryptotext.

Algebra liniară este ramura matematicii care studiază vectorii, spațiile vectoriale (numite și spații liniare), transformările liniare și sistemele de ecuații liniare. Spațiile vectoriale sunt o temă centrală în matematica modernă. Astfel, algebra liniară este utilizată pe scară largă atât în algebra abstractă cât și în analiza funcțională. Algebra liniară are de asemenea o reprezentare concretă în geometria analitică. Are aplicații numeroase în științele naturale și științele sociale, întrucât sistemele și fenomenele neliniare pot fi adesea aproximate printr-un model liniar.

Dacă spațiul vectorial are fixată o bază, atunci fiecare transformare liniară poate fi reprezentată printr-o tabelă de numere denumită matrice. Studiul detaliat al proprietăților matricelor și al algoritmilor ce lucrează pe matrice, cum ar fi determinanții sau vectorii proprii, se consideră a fi parte a algebrei liniare.

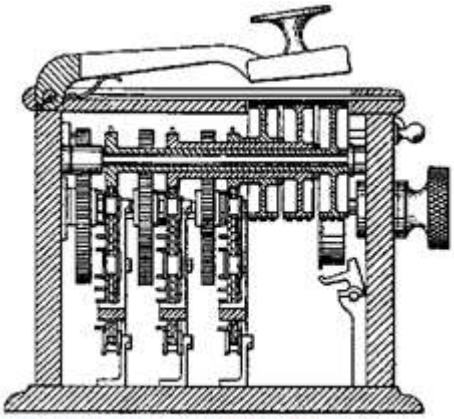
Metoda generală de a găsi un mod de abordare liniar pentru o problemă, de a exprima această abordare în termenii algebrei liniare, și apoi de a o rezolva dacă e nevoie prin calcul matriceal, este una dintre metodele cele mai general valabile din matematică [2].

Sistemul de criptare Hill este o metodă de substituție poligrafică bazată pe algebra liniară, mai exact, bazată pe calcule efectuate după modulo p [1]. A fost creat de către Lester Hill în anul 1929. În faza de preprocesare delimitatorul de spațiu este ignorat sau înlocuit cu caracterul cel mai puțin frecvent din limba în care este textul clar (în limba română Q).

Algoritmul procesează un bloc de date M de n caractere/litere, cheia de criptare fiind reprezentată de o matrice K de dimensiune $n \times n$, inversabilă după modulo p.

Există două clase ale algoritmului Hill pentru care regulile de criptare diferă prin ordinea în care se efectuează înmulțirile: prima clasă are ca regulă de cifrare operația de

înmulțire $C = MK$ cu decriptarea $M = CK^{-1}$, iar a doua clasă folosește regula de criptare înmulțirea $C = KM$, având decriptarea corespunzătoare $M = K^{-1}C$.



Mașina pentru cifrul lui Hill

Dacă matricea K este simetrică (matricea K și transpusa ei sunt egale), atunci regulile de criptare pentru cele două clase sânt echivalente.

În cazul alfabetului latin $p = 26$, cheia de criptare K trebuie să fie o matrice inversabilă după modulo 26, iar în cazul alfabetului român $p = 31$, matricea K trebuie să fie inversabilă după modulo 31.

Prin urmare, dacă definim un număr întreg fixat d ($d \geq 2$) și costruim mulțimile: $P = C = Z_{26}^d$, $K = \{K: K \in K_d(Z_{26}), \det(K) \neq 0\}$, atunci o cheie de criptare este o matrice pătrată K nesingulară/nedegenerată de dimensiune d, cu elemente din Z_{26}, iar K^{-1} formează cheia de decriptare.

Textul clar pt se împarte în blocuri de lungime d: $pt = \alpha_1\alpha_2 \ldots \alpha_n$, $|\alpha_i| = d$ (ultimul bloc se completează eventual cu 0 până a ajunge la lungimea d). Textul criptat va fi $ct = \beta_1\beta_2 \ldots \beta_n$, unde $\beta_i = e_K(\alpha_i) = \alpha_i \cdot K \pmod{26}$, $(1 \leq i \leq n)$. Pentru decriptare se folosește relația $d_K(\beta_i) = \beta_i \cdot K^{-1} \pmod{26}$.

Să luăm de exemplu $d = 3$ și cheia

$$K = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}, \text{ cu inversa } K^{-1} = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}.$$

Dacă textul clar pt este ERI SAU DUS, atunci vom avea:

$\alpha_1 = \text{ERI} = (4 \quad 17 \quad 8)$, $\alpha_2 = \text{SAU} = (18 \quad 0 \quad 20)$ și $\alpha_3 = \text{DUS} = (3 \quad 20 \quad 18)$.

Din relațiile

$$\beta_1 = \alpha_1 \cdot K \pmod{26} = (4 \quad 17 \quad 8) \cdot \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} = (11 \quad 18 \quad 19) = (L \quad S \quad T);$$

$$\beta_2 = \alpha_2 \cdot K \pmod{26} = (18 \quad 0 \quad 20) \cdot \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} = (18 \quad 18 \quad 2) = (S \quad S \quad C);$$

$$\beta_3 = \alpha_3 \cdot K \pmod{26} = (3 \quad 20 \quad 18) \cdot \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} = (16 \quad 1 \quad 22) = (Q \quad B \quad W).$$

se obține textul criptat LST SSC QBW.

Pentru a decripta criptotextul utilizăm relațiile: $d_K(\beta_i) = \beta_i \cdot K^{-1} \pmod{26}$, adică

$$d_K(\beta_1) = \beta_1 \cdot K^{-1} \pmod{26} = \begin{pmatrix}11 & 18 & 19\end{pmatrix} \cdot \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} = \begin{pmatrix}4 & 17 & 8\end{pmatrix} = \text{ERI};$$

$$d_K(\beta_2) = \beta_2 \cdot K^{-1} \pmod{26} = \begin{pmatrix}18 & 18 & 2\end{pmatrix} \cdot \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} = \begin{pmatrix}18 & 0 & 20\end{pmatrix} = \text{SAU};$$

$$d_K(\beta_3) = \beta_3 \cdot K^{-1} \pmod{26} = \begin{pmatrix}3 & 20 & 18\end{pmatrix} \cdot \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} = \begin{pmatrix}3 & 20 & 18\end{pmatrix} = \text{DUS}.$$

Astfel am obținut ERI SAU DUS. La criptarea și decriptarea acestui text am folosit formulele $C = MK$ (pentru criptare) și respectiv, $M = CK^{-1}$ (pentru decriptare).

Să realizăm acum criptarea și decriptarea textului ERI SAU DUS după formulele $C = KM$ (pentru criptare) și respectiv $M = K^{-1}C$ (pentru decriptare). Vom considera:

$$\alpha_1 = \begin{pmatrix}4 & 17 & 8\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}, \alpha_2 = \begin{pmatrix}18 & 0 & 20\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix} \text{ și } \alpha_3 = \begin{pmatrix}3 & 20 & 18\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$

$$\beta_1 = K \cdot \alpha_1 \pmod{26} = \begin{pmatrix}8 & 5 & 10\\ 21 & 8 & 21\\ 21 & 12 & 8\end{pmatrix} \cdot \begin{pmatrix}4 & 17 & 8\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix} = \begin{pmatrix}6 & 6 & 12\\ 6 & 19 & 12\\ 6 & 19 & 12\end{pmatrix};$$

$$\beta_2 = K \cdot \alpha_2 \pmod{26} = \begin{pmatrix}8 & 5 & 10\\ 21 & 8 & 21\\ 21 & 12 & 8\end{pmatrix} \cdot \begin{pmatrix}18 & 0 & 20\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix} = \begin{pmatrix}14 & 0 & 4\\ 14 & 0 & 4\\ 14 & 0 & 4\end{pmatrix};$$

$$\beta_3 = K \cdot \alpha_3 \pmod{26} = \begin{pmatrix}8 & 5 & 10\\ 21 & 8 & 21\\ 21 & 12 & 8\end{pmatrix} \cdot \begin{pmatrix}3 & 20 & 18\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix} = \begin{pmatrix}24 & 4 & 14\\ 11 & 4 & 14\\ 11 & 4 & 14\end{pmatrix}.$$

La decriptare vom obține:

$$\alpha_1 = K^{-1} \cdot \beta_1 \pmod{26} = \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} \cdot \begin{pmatrix}6 & 6 & 12\\ 6 & 19 & 12\\ 6 & 19 & 12\end{pmatrix} = \begin{pmatrix}4 & 17 & 8\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix};$$

$$\alpha_2 = K^{-1} \cdot \beta_2 \pmod{26} = \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} \cdot \begin{pmatrix}14 & 0 & 4\\ 14 & 0 & 4\\ 14 & 0 & 4\end{pmatrix} = \begin{pmatrix}18 & 0 & 20\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix};$$

$$\alpha_3 = K^{-1} \cdot \beta_3 \pmod{26} = \begin{pmatrix}6 & 24 & 1\\ 13 & 16 & 10\\ 20 & 17 & 15\end{pmatrix} \cdot \begin{pmatrix}24 & 4 & 14\\ 11 & 4 & 14\\ 11 & 4 & 14\end{pmatrix} = \begin{pmatrix}3 & 20 & 18\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$

Poate fi utilizată și o modificare a metodei a doua considerând α_1 prima linie, α_2 – a doua linie și α_3 – a treia linie a unei matrice pătratice de dimensiunea $d = 3$. Atunci primim:

$$C = \begin{pmatrix}8 & 5 & 10\\ 21 & 8 & 21\\ 21 & 12 & 8\end{pmatrix} \cdot \begin{pmatrix}4 & 17 & 8\\ 18 & 0 & 20\\ 3 & 20 & 18\end{pmatrix} = \begin{pmatrix}22 & 24 & 6\\ 5 & 23 & 4\\ 12 & 23 & 6\end{pmatrix}.$$

Prin urmare, textul criptat este WYG FXE MXG.

La decriptare avem:

$$M = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \cdot \begin{pmatrix} 22 & 24 & 6 \\ 5 & 23 & 4 \\ 12 & 23 & 6 \end{pmatrix} = \begin{pmatrix} 4 & 17 & 8 \\ 18 & 0 & 20 \\ 3 & 20 & 18 \end{pmatrix} = \begin{pmatrix} E & R & I \\ S & A & U \\ D & U & S \end{pmatrix}.$$

Să luăm, în continuare, $d = 2$ și cheia

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \text{ cu inversa } K^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \text{ (vezi [1, pag. 14].}$$

Dacă textul clar este α = FRAC, atunci vom avea

$$\alpha_1 = (F \quad R) = (5 \quad 17),\ \alpha_2 = (A \quad C) = (0 \quad 2).$$

Din relațiile

$$\beta_1 = \alpha_1 \cdot K \pmod{26} = (5 \quad 17) \cdot \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (23 \quad 22) = (X \quad W);$$

$$\beta_2 = \alpha_2 \cdot K \pmod{26} = (0 \quad 2) \cdot \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (4 \quad 10) = (E \quad K)$$

primim criptarea XWEK.

Să ne situăm acum pe poziția unui criptanalist: admitem că am găsit dimensiunea $d = 2$ și încercăm să determinăm matricea K sau echivalent K^{-1} cunoscând perechea (text clar, text criptat) = (FRAC, XWEK).

Prin urmare, criptanalistul se află acum în fața următoarei probleme: trebuie să determine matricea $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $a, b, c, d \in \{0, 1, 2, 3, \ldots, 24, 25\}$, astfel ca

$$\begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 23 & 22 \\ 4 & 10 \end{pmatrix}.$$

Pentru a putea afla matricea $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ criptanalistul trebuie să afle inversa matricei $\begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix}$. Deoarece $\det\begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix} = 10$ și $cmmdc(10, 26) = 2 > 1$, rezultă că $10^{-1} \pmod{26}$ nu există și deci matricea $\begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix}$ nu este inversabilă. Prin urmare, în acest caz, criptanalistul nu poate determina cheia de criptare.

Admitem acum că criptanalistul cunoaște criptarea unor texte clare selectate de el (este atacul cu text clar): alege un text clar a cărui matrice este inversabilă și îi află criptarea. Fie BRAD acest text clar cu matricea asociată $A = \begin{pmatrix} 1 & 17 \\ 0 & 3 \end{pmatrix}$. Criptanalistul solicită criptarea lui BRAD și primește LKGP, de matricea asociată $B = \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix}$. Deci el dispune de perechea (BRAD, LKGP). Criptanalistul determină mai întâi $A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix}$, iar apoi din ecuația $A \cdot K = B$, va determina soluția: $K = A^{-1} \cdot B = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix} \cdot \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$.

Complicația care poate apărea este faptul că nu toate matricele sânt inversabile. Există o metodă directă de determinare a acestei proprietăți. Dacă determinantul matrice este 0, sau are factori comuni cu modulul (adică factori ca 2 sau 13, în cazul modulului 26), atunci matricea nu poate fi folosită în cifrul Hill. Din fericire, dacă baza nu are factori mici, cele

mai multe matrice au inverse. Riscul ca determinantul să aibă factori comuni cu modulul poate fi eliminat prin alegerea unui modul prim. În consecință, o variantă utilă de cifru Hill adaugă încă 3 simboluri pentru a crește modulul la 29. Pentru limba română cu diacritice întotdeauna avem modulul 31, adică un număr prim.

Definiție. *Fie n un număr natural nenul. Un cifru de permutare este un sistem* (*P, C, K, E, D*) unde $P = C = Z_{26}^n$, $K = P_n$. *Pentru o cheie* (*permutare*) $\pi \in S_n$

$$e_\pi(\alpha_1\alpha_2 \dots \alpha_n) = \alpha_{\pi(1)}\alpha_{\pi(2)} \dots \alpha_{\pi(n)}, \quad d_\pi(\beta_1 \beta_2 \dots \beta n) = \beta_{\pi^{-1}(1)}\beta_{\pi^{-1}(2)} \dots \beta_{\pi^{-1}(n)}.$$

La acest sistem de criptare, textul clar se împarte în blocuri de n ($n \geq 2$) caractere, după care fiecărui bloc i se aplică o permutare $\pi \in P_n$ (mulțimea permutărilor de n elemente). Elementele n și π sunt fixate; π este cheia de criptare, iar π^{-1} va fi cheia de decriptare.

Să admitem că avem cheia de criptare $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Atunci un text clar, de exemplu CRIPTOGRAFIE se împarte în blocuri de trei caractere:

$$(C \quad R \quad I) \quad (P \quad T \quad O) \quad (G \quad R \quad A) \quad (F \quad I \quad E),$$

atunci textul criptat va fi:

$$(R \quad I \quad C) \quad (T \quad O \quad P) \quad (R \quad A \quad G) \quad (I \quad E \quad F),$$

adică RICTOPRAGIEF.

Se poate de demonstrat că un cifru de permutare este un cifru Hill. De exemplu, permutării $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ îi corespunde matricea de permutare $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

De exemplu, dacă criptăm cuvântul ARE după cifrul lui Hill, atunci obținem RAE, iar dacă aplicăm matricea de permutare, obținem:

$$(0 \quad 17 \quad 4) \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (17 \quad 0 \quad 4),$$

ceea ce reprezintă criptotextul RAE, adică se obține același rezultat.

Acest articol a fost elaborat în cadrul proiectului de cercetări științifice „Metodologia implementării TIC în procesul de studiere a științelor reale în sistemul de educație din Republica Moldova din perspectiva inter/transdisciplinarității (concept STEAM)”, Programul „Program de stat” (2020- 2023), Prioritatea IV: Provocări societale, cifrul 20.80009.0807.20.

Bibliografie

1. ATANASIU, Adrian. *Securitatea Informației*. Vol. 1 (Criptografie). Cluj: Editura INFODATA, 2012.
2. https://ro.wikipedia.org/wiki/Algebră_liniară.