

Latin négyzetek alkalmazásai a titkosításban

DÉNES TAMÁS

tdenest@freemail.hu

Kulcsszavak: korai módszerek, latin négyzetek tulajdonságai, kódfejtés

A rejtjelző rács figyelemreméltó „divattá” vált évszázadokon keresztül a kriptográfiában. A Cardano-rács történetét és alkalmazását a titkosításban e folyóirat már közölte [5], ezért jelen dolgozatom a permutációs mátrixokkal és latin négyzetekkel való kapcsolatát mutatja be, amely egyúttal rávilágít eme 450 éves találmány 21. századi rendkívüli lehetőségeire. A digitális technika új perspektívákat nyit a sztegonográfiának és ezen belül a rejtjelző rácsoknak is.

Girolamo Cardano (1501–1576) korszakos és mai napig ható módszercsaládja – amely a sztegonográfia [6] új ágát indította útjára –, a róla elnevezett Cardano-rács. Tulajdonképpen egy betűmátrixra helyezhető sablonról van szó. A pontosabb megértéshez idézzük fel magának Cardanonak a szavait:

„Végy két azonos méretű pergamen lapot és azonos vonalak mentén készíts kivágásokat különböző helyeken. Ezek a kivágások legyenek kicsik, de mégis legálább akkorák, mint az ABC nagybetűi. Az összes kivágásokba összesen 120 betűt lehessen elhelyezni. Az egyik pergamen lapot majd a levelező társadnak adod. Amikor alkalom adódik, először írd az üzenetedet olyan tömören, ahogy csak lehetséges, így az üzenet kevesebb betűt is tartalmazhat, mint amennyi a kivágott ablakokban elhelyezhető. Amikor beírtad az üzeneted az egyik pergamen lapra, tedd ugyanezt a másikkal is. Ezután töltsd ki az első lapon az üresen maradt helyet úgy, hogy teljes mondatokra egészítsék ki a már ráírt szöveget. Ez a kitöltés úgy történjen, hogy a teljes szöveg stílusa és tartalma összefüggő és egységes legyen. Amikor a levelező társad megkapja a te üzenetedet, ráhelyezi a megfelelő kivágásokkal ellátott pergamment és így elolvashatja az üzenetet.”

Latin négyzetek és permutációs mátrixok kapcsolata

Egy $P(n)$ $n \times n$ -es, $(0,1)$ -es mátrixot permutációs mátrixnak nevezünk, ha a mátrix pontosan n darab 1-t tartalmaz úgy, hogy minden sorban és oszlopban pontosan egy darab 1 lehet, a többi elem nulla.

Érdekes és a rejtjelző-rácsok szempontjából fontos eredmény az alábbi:

Egy $L(n)$ $n \times n$ -es latin négyzet kölcsönösen-egyértelműen felbontható n darab permutációs mátrix összegére [2,3], azaz

$$L(n) = 1 \cdot P_{i1} + 2 \cdot P_{i2} + \dots + n \cdot P_{in} \quad (1)$$

ahol P_{ik} az i_k -adik permutációs mátrix, azaz a mátrixban 1 szerepel mindenhol, ahol $L(n)$ -ben k van, a más-

rix többi eleme nulla. (A „+” összeadás művelet a mátrixok összeadását, míg a „•” szorzás a mátrixok skalár szorzását jelöli.)

Ezen megfeleltetések következménye, hogy az így adódó permutációs mátrixok jól felhasználhatók rejtjelző rácsként. A következő szemléltető példában a (2) -beli $L(4)$ latin négyzet P_1, P_2, P_3, P_4 permutációs mátrixokra való egyértelmű felbontása látható:

$$\begin{aligned} L(4) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad (2) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} P_1 + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} P_2 + \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} P_3 + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} P_4 \end{aligned}$$

A rejtjelző rács tulajdonképpen egy betűkeverési rejtjelző eszköz, amely az úgynevezett nyílt szöveg betűit egy betűmátrixba képezi le. Mindegyik P_i permutációs mátrix egy rejtjelző rácsként fogható fel, ahol az 1-esek helyén „ablakok” vannak.

Példaként legyen a nyílt szöveg a „SZIA” és használjuk a P_1 permutációs mátrixot rejtjelző rácsként. Ekkor egy tetszőleges B 4×4 -es betűmátrixban hagyjuk üresen azokat a cellákat, ahol P_1 -ben 1-es van (ezek a rejtő „ablakok”).

$$B = \begin{pmatrix} [] & E & I & M \\ B & F & J & [] \\ C & [] & K & O \\ D & H & [] & P \end{pmatrix} \quad (4)$$

Majd az „ablakokba” balról-jobbra, fentről-lefelé írjuk be a nyílt szöveget, így kapjuk a P_1 -nek megfelelő ráccsal rejtjelzett B_1 betűmátrixot.

$$B_1 = \begin{pmatrix} S & E & I & M \\ B & F & J & Z \\ C & I & K & O \\ D & H & A & P \end{pmatrix} \quad (5)$$

Így a permutációs mátrixok (mint rácsok) egymás utáni betűmátrixra helyezésével tudjuk a kívánt szöveget a betűmátrixba írni és a fordított eljárással kiolvas-

ni. Mivel a latin négyzetekre vonatkozó fenti egyértelmű felbontási tétel miatt az így készített rácsok ablakai pontosan lefedik a betűmátrix n^2 mezőjét, ezzel a módszerrel elértük, hogy a teljes betűmátrixot kitölthetjük rejtett szöveggel. További előny, hogy a latin négyzet felbontásának egyértelműsége nem sérül, ha a felbontást adó permutációs mátrixok (rácsok) sorrendjét megváltoztatjuk. Így a felbontások számának $n!$ -szorososa a lehetséges rácsfelhasználások száma.

A rejtjelzésben a kulcstér mérete is fontos tényező, ezért igen érdekesek a latin négyzetek számára vonatkozó eredmények. Az $L(n)$ $n \times n$ -es latin négyzetek permutációs mátrixokra való felbontásainak száma megegyezik az összes $n \times n$ -es latin négyzetek számával. A latin négyzetek számára pontos formula egyelőre nem létezik, azt azonban tudjuk, hogy ha T_n -nel jelöljük az úgynevezett redukált $n \times n$ -es latin négyzetek számát (redukált latin négyzet, melynek első sora és oszlopa az $1, 2, \dots, n$ természetes számokat alapsorrendben tartalmazza), akkor $T_n \geq (n-2)!(n-3)! \dots (2)!(1)!$, míg az összes $n \times n$ -es latin négyzetek számára fennáll az $U_n = n!(n-1)! T_n$ összefüggés.

A redukált latin négyzetek számának pontos értékét eddig csupán $n=10$ -ig sikerült számítógéppel meghatározni, hogy mekkora számokról van szó, annak illusztrálására álljon itt $T_9 = 377.597.570.964.258.816$ [1]. Ez a szám kb. 38 milliószorososa a Földön ma élő emberiség létszámának. A rejtjelzésben javasolható rácsméretek az $20 \leq n \leq 30$ értékek!

A következőkben megmutatjuk, hogy a permutációs mátrixok (és bizonyos feltételek mellett a latin négyzetek is) megsorsorozhatók, azaz az $n \times n$ -es permutációs mátrixok és az $1, 2, \dots, n!$ természetes számok között kölcsönösen egyértelmű megfeleltetés létesíthető. Az 1., 2., 3. tételek bizonyítása megtalálható [4]-ben.

1. Tétel

Bármely P_i $n \times n$ -es permutációs mátrixhoz kölcsönösen egyértelműen hozzárendelhető egy p_i n -edfokú permutáció.

Az 1. tétel illusztrálásához lássuk el a (3)-beli P_1 permutációs mátrixot perem elemekkel. Ekkor a (6) mátrixot kapjuk.

$$\begin{pmatrix} & 1 & 2 & 3 & 4 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 \\ 3 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (6)$$

A P_1 permutációs mátrixhoz rendeljük a p_1 permutációt a következőképpen:

- A P_1 mátrix első sorában található 1-hez tartozó vízszintes és függőleges perem elemeket írjuk egymás alá, ez lesz a p_1 permutáció első oszlopa.
- Tegyük ugyanezt a P_1 mátrix második, harmadik, negyedik sorával, így kapjuk a p_1 permutáció megfelelő oszlopait, azaz, ha $P(i, j) = 1$, akkor p_1 megfelelő oszlopa $\begin{pmatrix} i \\ j \end{pmatrix}$ (lásd a (7) levezetést).

$$P_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{(6)} p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad (7)$$

Permutációk és

a „faktoriális alapú” számrendszer

Ahhoz, hogy a permutációs mátrixokhoz sorszámot rendeljünk, az 1. tétel alapján elegendő a permutációk megsorsozása. Erre ad módot a következő 2. és 3. tétel.

2. Tétel („faktoriális alapú” számrendszer)

Legyenek m és b_i természetes számok, melyekre teljesül, hogy

$$1 \leq m \leq n! \quad (8)$$

$$0 \leq b_i \leq i-1 \quad (i=1, 2, 3, \dots, n) \quad (9)$$

$$m = 1 + \sum_{i=2}^n b_i (i-1)! \quad (10)$$

Ekkor bármely (8)-nak megfelelő m -hez pontosan egy b_i sorozat létezik, amely eleget tesz a (9), (10) összefüggéseknek.

Amint azt láttuk, az összes n -ed rendű latin négyzet előállítására teljesen megoldatlan probléma, hiszen akkor egyúttal megoldódna a leszámlálásuk is, de $n > 10$ esetén még az összes latin négyzetek pontos számát sem ismerjük. Így a latin négyzetek alkalmazása szempontjából különleges jelentősége van, ha bizonyos típusú latin négyzet osztályok előállítására tudunk algoritmust adni, főleg ha ez egyszerre a természetes számokhoz való egyértelmű hozzárendelést is jelent. Ekkor ugyanis a rejtjelzésben jelentős véletlenszám generátorok felhasználására is mód nyílik, másrészt tárolási és továbbítási előnye van. A következőkben olyan latin négyzet osztályt állítunk elő, amelynek soraiban lévő permutációk elemi transzpozíciókkal származtathatók egymásból. Az algoritmus részletes leírása [4]-ben megtalálható.

Az eljárás elemi transzpozíciók segítségével állítja elő a permutációkat. Legyen a kiindulási permutáció (a π_1 kezdőpermutáció megválasztása tetszőleges lehet):

$$\pi_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \quad (11)$$

Ekkor a rekurziós formula a következő:

$$\pi_{m+1} = \sigma_m \cdot \pi_m \quad 1 \leq m \leq n! - 1 \quad (12)$$

σ_m meghatározásához soroljuk a természetes számokat az $A_1, A_2, \dots, A_k$ osztályokba úgy, hogy

$$m \in A_k \Leftrightarrow k \nmid m \text{ és } (k+1) \nmid m \quad (13)$$

$$\sigma_m = \begin{cases} \tau_1 \cdot \tau_3 \cdot \tau_5 \cdot \dots \cdot \tau_k & \text{ha } m \in A_k \text{ és } k = 2r+1 \\ \tau_2 \cdot \tau_4 \cdot \tau_6 \cdot \dots \cdot \tau_k & \text{ha } m \in A_k \text{ és } k = 2r \end{cases} \quad (14)$$

A σ_m transzpozíció szorzatot a továbbiakban σ_m transzformációnak nevezzük.

A τ_i jelölés elemi transzpozíciót jelöl, azaz $\tau_i = (i \ i+1)$, így (14) a következőképpen írható:

$$\sigma_m = \begin{cases} (12)(34)(56)\dots(k\ k+1) & \text{ha } m \in A_k \text{ és } k = 2r+1 \\ (23)(45)(67)\dots(k\ k+1) & \text{ha } m \in A_k \text{ és } k = 2r \end{cases} \quad (15)$$

Az eljárás tehát a következő transzformáció-szorzatot állítja elő:

$$\pi_{k+1} = \sigma_k \cdot \sigma_{k-1} \cdot \dots \cdot \sigma_2 \cdot \sigma_1 \cdot \pi_1 \quad (k=1, 2, \dots, n!-1) \quad (16)$$

Osztályozzuk a transzformációkat az indexük szerint, vagyis σ_r és σ_s akkor és csak akkor tartozik egy osztályba, ha r és s a (13) definíció szerint egy osztályba tartozik.

Ekkor könnyen belátható, hogy az egy osztályba tartozó transzformációk egyenlők, hiszen r és s egyértelműen határozzák meg a (15) definíció k osztályindexét.

A (13)-(16) osztályozási definíciók és a transzformációk egyenlősége miatt igaz a következő:

$$\begin{aligned} \sigma_1 &= \sigma_{(n-1)!+1} = \sigma_{2(n-1)!+1} = \dots = \sigma_{(n-1)(n-1)!+1} \\ \sigma_2 &= \sigma_{(n-1)!+2} = \sigma_{2(n-1)!+2} = \dots = \sigma_{(n-1)(n-1)!+2} \\ &\vdots \\ \sigma_{(n-1)!} &= \sigma_{2(n-1)!} = \sigma_{3(n-1)!} = \dots = \sigma_{n(n-1)!} \end{aligned} \quad (17)$$

Helyettesítsük be (16)-ba a (17) egyenlőségrendszerben kapottakat:

$$\pi_{n!} = \sigma_{(n-1)!+1} \cdot \dots \cdot \sigma_1 \cdot [\sigma_{(n-1)!} \cdot \dots \cdot \sigma_1]^{n-1} \cdot \pi_1 \quad (18)$$

Mivel a $\sigma_{(n-1)!+1} \cdot \dots \cdot \sigma_1$ transzformáció szorzat nem más, mint az összes $(n-1)$ -ed fokú permutációk előállításához szükséges transzformációk szorzata, vezessük be a következő egyszerűbb jelölést:

$$\rho_r = \sigma_{r!+1} \cdot \dots \cdot \sigma_1 \quad (19)$$

Ahol tehát ρ_r az összes r -ed fokú permutáció előállításához szükséges transzformációk szorzatát jelöli. Ekkor (18) így írható:

$$\rho_n = \rho_{n-1} \cdot [\sigma_{(n-1)!} \cdot \rho_{n-1}]^{n-1} \cdot \pi_1 \quad (20)$$

Latin négyzetek megszámozása

3. Tétel

A (20) formula $n!$ különböző permutációt állít elő.

Következmények:

K3.1.

A 3. tétel következményeként adódik, hogy a (17) egyenlőségrendszer minden sorának első eleme különböző permutációt állít elő. Az egy sorban levő transzformációk a teljes n -edfokú ciklus (C_n) különböző hatványaival szorozzák a sor első (kezdő) permutációját, így ezek is különbözőek és teljes ciklust alkotnak.

Ebből következik, hogy (17) minden sora n darab olyan permutációt generál, amelyek egy latin négyzetet alkotnak.

K3.2.

Másrésről (17) minden sora különböző latin négyzetet állít elő, így a fenti rekurzív eljárással $(n-1)!$ latin négyzet könnyen előállítható.

K3.3.

A K3.1. következményből adódik, hogy az így generált latin négyzetek reprezentálhatók a megfelelő sorkezdőpermutációjával. Azaz a kezdőpermutációhoz rendelt sorszámmal azonosíthatók. A fentiekben bevezetett jelölésekkel az alábbi sorszámozott latin négyzeteket kapjuk:

$$L_m(n) = \begin{bmatrix} \pi_m \\ \pi_{(n-1)!+m} \\ \pi_{2(n-1)!+m} \\ \vdots \\ \pi_{(n-1)(n-1)!+m} \end{bmatrix} \quad 1 \leq m \leq (n-1)! \quad (21)$$

Példa: $n=4$, $m=3$ (lásd az 1. táblázatot)

$$L_3(4) = \begin{bmatrix} \pi_3 \\ \pi_9 \\ \pi_{15} \\ \pi_{21} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 4 \\ 1 & 4 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 2 & 3 \end{bmatrix} \quad (22)$$

Az (1) felbontásnak megfelelően permutációs mátrixok összegeként felírva:

$$LP_m(n) = 1 \cdot P_m + 2 \cdot P_{(n-1)!+m} + 3 \cdot P_{2(n-1)!+m} + \dots + n \cdot P_{(n-1)(n-1)!+m} \quad 1 \leq m \leq (n-1)! \quad (23)$$

Példa: $n=4$, $m=3$ (lásd az 1. táblázatot)

$$\pi_3 = \begin{pmatrix} 1234 \\ 2314 \end{pmatrix} \Rightarrow P_3 = \begin{bmatrix} 0100 \\ 0010 \\ 1000 \\ 0001 \end{bmatrix} \quad \pi_9 = \begin{pmatrix} 1234 \\ 1432 \end{pmatrix} \Rightarrow P_9 = \begin{bmatrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{bmatrix} \quad (24)$$

$$\pi_{15} = \begin{pmatrix} 1234 \\ 3241 \end{pmatrix} \Rightarrow P_{15} = \begin{bmatrix} 0010 \\ 0100 \\ 0001 \\ 1000 \end{bmatrix} \quad \pi_{21} = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} \Rightarrow P_{21} = \begin{bmatrix} 0001 \\ 1000 \\ 0100 \\ 0010 \end{bmatrix}$$

$$LP_3(4) = 1 \cdot P_3 + 2 \cdot P_9 + 3 \cdot P_{15} + 4 \cdot P_{21} = \begin{bmatrix} 2134 \\ 4312 \\ 1423 \\ 3241 \end{bmatrix} \quad (25)$$

Latin négyzet alapú rejtjelzés

Használjuk a példa permutációs mátrixait rejtjelző-rácsként. Legyen a nyílt szöveg: „AMI TITOK AZ TITOK!” és legyen a rácsok sorrendje a fenti (3, 9, 15, 21), ekkor a rejtett betűmátrix a következő (26):

$$R_3 = \begin{matrix} 0A00 \\ 00M0 \\ I000 \\ 000T \end{matrix} \quad R_9 = \begin{matrix} I000 \\ 000T \\ 0000 \\ 0K00 \end{matrix} \quad R_{15} = \begin{matrix} 00A0 \\ 0Z00 \\ 000T \\ I000 \end{matrix} \quad R_{21} = \begin{matrix} 000T \\ 0000 \\ 0K00 \\ 00!0 \end{matrix} \Rightarrow R_3 + R_9 + R_{15} + R_{21} = \begin{matrix} IAAT \\ OZMT \\ IKOT \\ IK!T \end{matrix}$$

Mint azt megjegyeztük, ugyanezzel a négy ráccsal $4!=24$ -féleképpen állíthatjuk elő a rejtett betűmátrixot. Példaként bemutatjuk a 15, 3, 21, 9 sorrendhez tartozó betűmátrixot is (27):

$$R_{15} = \begin{matrix} 00A0 \\ 0M00 \\ 000I \\ T000 \end{matrix} \quad R_3 = \begin{matrix} 0I00 \\ 00T0 \\ 0000 \\ 000K \end{matrix} \quad R_{21} = \begin{matrix} 000A \\ Z000 \\ 0T00 \\ 00I0 \end{matrix} \quad R_9 = \begin{matrix} T000 \\ 0000 \\ 00K0 \\ 0!00 \end{matrix} \Rightarrow R_{15} + R_3 + R_{21} + R_9 = \begin{matrix} TIAA \\ ZMTO \\ OTKI \\ T!IK \end{matrix}$$

A fenti rekurziós algoritmus az összes n -edfokú permutációknak egy egymásbaskatulyázott blokkos elrendezését adja (1. táblázat), amelyre teljesülnek az alábbiak:

- A1) Minden blokk utolsó oszlopában azonos elemek vannak.
- A2) Azonos fokszerű, de különböző blokkok utolsó oszlopoi különbözők.
- A3) Az A1., A2. tulajdonságokból következik, hogy egy tetszőleges

$$\pi_m = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ a_1 & a_2 & \dots & a_i & \dots & a_n \end{pmatrix}$$

n -edfokú permutáció minden eleme egyértelműen meghatároz egy blokkot, mégpedig az a_i elem egy $(i-1)$ -edfokú blokkot, amelyhez hozzárendelhetjük a (9) szerinti b_i értéket. Az így nyert b_i ($i=1,2,\dots,n$) sorozat (10) szerint egyértelműen rendel a permutációhoz az m természetes számot.

1. táblázat

1.	1	2	3	4
2.	2	1	3	4
3.	2	3	1	4
4.	3	2	1	4
5.	3	1	2	4
6.	1	3	2	4
7.	3	1	4	2
8.	1	3	4	2
9.	1	4	3	2
10.	4	1	3	2
11.	4	3	1	2
12.	3	4	1	2
13.	4	3	2	1
14.	3	4	2	1
15.	3	2	4	1
16.	2	3	4	1
17.	2	4	3	1
18.	4	2	3	1
19.	2	4	1	3
20.	4	2	1	3
21.	4	1	2	3
22.	1	4	2	3
23.	1	2	4	3
24.	2	1	4	3

Ha a permutációs mátrixokat rejtjelző-rácsként alkalmazzuk, akkor a P_i mátrix, illetve az ehhez tartozó p_i permutáció helyett elegendő az i szám tárolása az azonosításhoz.

Egy n -ed fokú permutáció tárolásához (csak a képelemeket tároljuk!) $c(n)$ számú karakterre van szükség, ahol

$$c(n) = (\lceil \log_{10} n \rceil + 1)n \quad (28)$$

Az $n!$ szám számjegyeinek száma (jelöljük $j(n)$ -nel):

$$j(n) = \lceil \log_{10} n! \rceil \quad (29)$$

Ekkor bár fennáll, hogy

$$\frac{j(n)}{c(n)} = \frac{\lceil \log_{10} n! \rceil}{n(\lceil \log_{10} n \rceil + 1)} = \frac{\sum_{i=1}^n \log_{10} i}{n(\lceil \log_{10} n \rceil + 1)}$$

amelyre $\lim_{n \rightarrow \infty} \frac{j(n)}{c(n)} = 1$ (31)

mégis a gyakorlatban ez a megfeleltetés jól használható, mivel az általában használatos $10 \leq n \leq 500$ értékekre a 2. táblázat (jobbra) értékei adódnak, ami azt mutatja, hogy 25-50% helymegtakarítást érhetünk el.

Latin négyzet alapú digitális aláírás

Az elektronikus pénz átutalás (EFT=Electronic Fund Transfer) és általában az elektronikus posta elterjedése felvetette a hagyományos aláírás helyettesítését digitálisan előállított (kódolt) elektronikus aláírással. A számítógépes terminálok használóinak, vagy az adatbankokhoz való hozzáférés jogosságának ellenőrzésénél hasonló problémákat kell megoldani, mint a hagyományos levél, illetve más papíralapú dokumentumok hitelesítésénél, ahol ezt a

célt szolgálta a kézi aláírás. Nyilvánvaló, hogy egy digitális, teljesen elektronizált rendszerben a kézi hitelesítést is helyettesíteni kell, erre való a digitális aláírás, amely azonban olyan kódolási módszereket használ, amelyek nem csupán a dokumentum aláíróját, hanem a dokumentum tartalmát is hitelesítik.

Sok módszer ismeretes a digitális aláírás megvalósítására. Most egy olyan eljárást mutatunk be, amely latin négyzeteken alapul és közvetlenül alkalmas párhuzamos működésű számítógépen való implementálásra, ami rendkívüli módon megnöveli a működési sebességet.

Legyen adott egy $U=a_1, a_2, \dots, a_n$ üzenet ahol az üzenet betűi (a_i) egy q elemű ábécéből valók. Az üzenet hitelesítését (digitális aláírását) az üzenettel azonos ábécéből vett s darab ($A=b_1, b_2, \dots, b_s$) betűvel kívánjuk elvégezni. Tegyük fel az egyszerűség kedvéért, hogy n osztható s -sel, vagyis $n=s \cdot t$. Válasszuk szét az üzenetet s darab részüzenetre (a szétválasztás egy kulcs szerint fog történni, ami esetünkben egy latin négyzet).

Minden részüzenet t darab betűből fog állni és minden egyes részüzenet az elektronikus aláírás egy betűjét határozza meg.

Az eljárást egy példán fogom szemléltetni, amely a könnyebb áttekinthetőség érdekében kis n és q értékekre vonatkozik. Legyen az üzenet $U=1032203101231003$ (vagyis $n=16$, $q=4$, $s=4$). A kulcs amely szerint az üzenetet részüzenetekre bontjuk egy s -ed rendű (jelen esetben 4-ed rendű) latin négyzet:

$$\begin{matrix} 0 & 2 & 3 & 1 \\ 2 & 1 & 0 & 3 \\ 1 & 3 & 2 & 0 \\ 3 & 0 & 1 & 2 \end{matrix} \quad (32)$$

2. táblázat

n	j(n)	c(n)	$\frac{j(n)}{c(n)}$
10	7	20	.35
100	158	300	.526
200	375	600	.625
300	614	900	.682
400	869	1200	.724
500	1134	1500	.756

A (33) mátrix egy segéd táblázat, amelynek felhasználása a következőkben kerül ismertetésre.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix} \quad (33)$$

Az U üzenet $U_1, U_2, U_3, \dots, U_s$ részüzenetekre való bontásának lépései a következők:

Válasszuk ki a (32) latin négyzetben szereplő azonos elemek sorszámát a (33) mátrix szerint úgy, hogy például a 0 elemekhez tartozó sorszámok a (33) mátrix ráhelyezésével a következőknek adódnak: 1, 7, 12, 14. Ugyanezt az eljárást alkalmazva a (32) latin négyzet 1-es, 2-es és 3-as elemeire is, a sorszámokat négy osztályba osztjuk: (1, 7, 12, 14), (4, 6, 9, 15), (2, 5, 11, 16), (3, 7, 9, 13).

Ezután a sorszámokat (megtartva az osztályozást) helyettesítjük az U üzenetnek az illető sorszám szerinti helyén álló elemével. Így a következő kevert részüzeneteket kapjuk: $U_1 = (1, 3, 3, 0)$, $U_2 = (2, 0, 0, 0)$, $U_3 = (0, 2, 2, 3)$, $U_4 = (3, 1, 1, 1)$. Most lássuk el a (32) latin négyzetet perem elemekkel:

$$\begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 2 & 3 & 1 \\ 1 & 2 & 1 & 0 & 3 \\ 2 & 1 & 3 & 2 & 0 \\ 3 & 3 & 0 & 1 & 2 \end{array} \quad (34)$$

Így tulajdonképpen a $(0,1,2,3)$ halmazon definiálunk egy $*$ műveletet, amelynek művelet táblája a (34) latin négyzet. A (34) művelet táblát pontosan úgy használjuk, mint a jól ismert szorzótáblát, például azt kapjuk, hogy $0*1=2$, $1*2=0$, stb.

A nem matematikus olvasó számára talán szokatlan, hogy a $*$ művelet nem asszociatív, vagyis $a*(b*c) \neq (a*b)*c$, azaz például $2*(3*1)=2*0=1$, de $(2*3)*1=0*1=2$, vagyis $2*(3*1) \neq (2*3)*1$. Ennek a tulajdonságnak nagy jelentősége van a következőkben bemutatott kódolási eljárásnál.

A példánkban szereplő U üzenet digitális aláírásához az egyes U_1, U_2, U_3, U_4 részüzenetek szorzatát kell előállítani a (34) művelet tábla alapján:

$$\begin{aligned} b_1 &= ((1*3)*3)*0 = (3*3)*0=2*0=1 \\ b_2 &= ((2*0)*0)*0 = (1*0)*0=2*0=1 \\ b_3 &= ((0*2)*2)*3 = (3*2)*3=1*3=3 \\ b_4 &= ((3*1)*2)*1 = (0*1)*1=2*1=3 \end{aligned} \quad (35)$$

vagyis az U üzenethez tartozó hitelesítő aláírás:

$$A=(b_1b_2b_3b_4)=1133$$

A fenti eljárás teljesen egyértelmű eredményre vezet, hiszen az U üzenet felbontása részüzenetekre a latin négyzet elemeinek diszjunkt osztályozásán alapul, ez viszont a fentiekben ismertetett permutációs mátrixokra való felbontási tétel miatt kölcsönösen egyértelmű.

A latin négyzeteken alapuló művelet táblák nem asszociatív algebrai struktúrát (úgynevezett kvázicsoport-

tot) reprezentálnak, aminek nagy jelentősége van az illetéktelen hamisítás elleni védekezésnél, mivel két karakter egyszerű felcserélését is kimutatja. Ezzel a képességgel a paritás ellenőrzésen alapuló módszerek, vagy a numerikus eljárások nem rendelkeznek.

Záró megjegyzés

Végül szeretném felhívni az olvasó figyelmét arra, hogy a rejtjelzés, hitelesítés, illetve a digitális aláírás numerikus módszereinek biztonsága (feltörhetősége) alapvetően függ a pillanatnyi számítástechnikai eszközök kapacitásától. Azaz a feltörhetetlenség mellett szóló érvek, a több ezer éves számolási igény a rejtett kulcsok megfejtéséhez, a gyors hardver fejlődéssel bizonytalanra válnak.

Bízom benne, hogy a latin négyzetek titkosítási alkalmazásainak e vázlatos ismertetéséből egyértelműen kitűnik, hogy a latin négyzeteken alapuló strukturális módszerrel aláírt és rejtjelzett elektronikus dokumentumok esetén nem kell tartani a számítógépek sebesség és kapacitás növekedésétől.

Irodalom

- [1] J. Dénes, A.D. Keedwell:
Latin squares and their applications,
Akadémiai Kiadó, Budapest, 1974.
- [2] J. Dénes, A.D. Keedwell: Latin squares and
1-factorizations of complete graphs, I.
Ars Combinatorica, 25A (1988), pp.109–126.
- [3] J. Dénes, A.D. Keedwell: Latin squares and
1-factorizations of complete graphs, II.
Utilitas Math., 34 (1988), pp.73–83.
- [4] Dénes Tamás: Algoritmusok az összes n -edfokú
permutáció előállítására, I.-II.
Információ Elektronika, 1975/1.-2.
- [5] Dénes Tamás: A rejtjelző rácsok születése
Híradástechnika, 2001/10, pp.57–63.
- [6] Dénes Tamás:
SZTEGONOGRÁFIA – rejtett információk rejtjelzés nélkül
Híradástechnika, 2001/8, pp.15–21.