

Томи Димовски, Скопје
Ана Димовска, Скопје

ПРИМЕНА НА МАТРИЦИТЕ ВО КРИПТОГРАФИЈАТА

Во оваа статија го разгледуваме Гаусовиот алгоритам за определување на инверзна матрица, ако истата постои. Притоа ќе го користиме множењето на матрици за кодирање на пораки и ќе ги користиме инверзната матрица и множење на матрици за декодирање на кодирана порака.

1. Вовед

Криптографијата датира од пред скоро 4000 години. Постојат записи дека Кинезите, Египќаните, Индијанците и Грците користеле шифри во нивните пораки со некаква цел. На пример, Цезар користел шема со која само ги заменува буквите А со С, В со D, С со Е, и.т.н. Замената на буквите денес е премногу едноставна и не се смета за безбедна. Кодирањето означува трансформирање на информации со цел да не бидат разбирливи за кој било освен за оние кои го имаат потребното знаење, обично назначено како ключ. Резултатот од процесот се кодирани информации. Декодирање означува трансформирање на неразбирлива информација во разбирлива информација со помош на некој клуч. Во дваесеттиот век примената на математичката теорија и математичките методи во кодирањето и декодирањето наоѓа примена за време на Втората светска војна при праќањето на пораките. Денес со развојот на информатичката наука кодирањето и декодирањето имаат примена во секоја сфера од човековото живеење.

Постапката на кодирање порака со помош на матрица се состои од неколку чекори. Најпрво ја конвертираме пораката во низа од броеви со тоа што на секоја буква му придружуваме број. Потоа ја конвертираме оваа низа во нова низа од броеви со помош на множење со квадратна матрица по наш избор која има инверзна матрица. На крај новата низа е всушност кодираната порака. Декодирањето на некоја порака се состои од следните чекори. Ја земаме низата од броеви која ја претставува кодираната порака и ја множиме со инверзната матрица на матрицата која сме ја избрале со што ја добиваме оригиналната порака.

2. Матрици и детерминанти (основни дефиниции и својства)

Дефиниција 2.1. Правоаголна шема од облик

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \text{ каде } a_{ij} \in \mathbb{R}, i = \overline{1, m}, j = \overline{1, n},$$

велиме дека е **матрица**. Користиме ознака $A = [a_{ij}]_{m \times n}$, $i = \overline{1, m}, j = \overline{1, n}$.
Хоризонталните n -торки $a_{k1}, a_{k2}, \dots, a_{kn}$, $k = \overline{1, m}$ ги нарекуваме **редици**, а вертикалните m -торки $a_{1k}, a_{2k}, \dots, a_{mk}$, $j = \overline{1, n}$ ги нарекуваме **колони** на матрицата A . Реалните броеви a_{ij} ги нарекуваме **елементи** на матрицата.

Матрица со m редици и n колони велиме дека е од ред $m \times n$. Ако $m = n$ матрицата велиме дека е **квадратна**.

Квадратната матрица $A = [a_{ij}]_{n \times n}$, $i, j = \overline{1, n}$ кај која елементите a_{ii} , $i = \overline{1, n}$ се еднакви на 1, а сите останати се еднакви на 0, ја нарекуваме **единична матрица од ред n** . Користиме ознака E_n или едноставно E , ако тоа не прави забуна.

Дефиниција 2.2. Квадратна шема од облик $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$ каде $a_{ij} \in \mathbb{R}$, $i, j \in \overline{1, 2}$ велиме дека е **детерминанта од втор ред**. Нејзината вредност изнесува

$$a_{11}a_{22} - a_{12}a_{21}.$$

Дефиниција 2.3. Квадратна шема од облик

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \text{ каде } a_{ij} \in \mathbb{R}, i, j \in \overline{1, 3}$$

велиме дека е **детерминанта од трет ред**. Нејзината вредност изнесува

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Дефиниција 2.4. Нека $A = [a_{ij}]_{m \times n}$ и $B = [b_{ij}]_{n \times p}$ се дадени матрици.

Матрицата $C = [c_{ij}]_{m \times p}$ каде што

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} \text{ за } i = \overline{1, m}, j = \overline{1, p},$$

велиме дека е **производ** на матриците A и B . Користиме ознака $C = AB$.

Забелешка 2.1. Производот AB е дефиниран кога бројот на колони на матрицата A е еднаков на бројот на редици на матрицата B .

Дефиниција 2.5. **Елементарни ридични трансформации** на матрицата $A = [a_{ij}]_{m \times n}$, $i = \overline{1, m}, j = \overline{1, n}$ велиме дека се:

1. Замена на местата на две редици. Означуваме $R_p \leftrightarrow R_l$;
2. Множење на елементите од една редица со број различен од нула. Означуваме $R_p \rightarrow cR_p$;
3. Множење на елементите од една редица со број различен од нула и додавање на соодветните елементи од друга редица. Означуваме $R_p \rightarrow R_p + cR_l$.

Дефиниција 2.6. Две матрици A и B велиме дека се **редично еквивалентни** ако B се добива од A со конечен број на елементарни редични трансформации. Означуваме $A \sim B$.

Дефиниција 2.7. Нека $A = [a_{ij}]_{n \times n}$ е квадратна матрица. Ако постои матрица B за која е исполнето $AB = BA = E$, тогаш матрица B ја нарекуваме инверзна матрица на матрицата A и ја означуваме со A^{-1} .

Својство 2.1. Ако постои инверзна матрица на матрицата $A = [a_{ij}]_{n \times n}$ таа е единствена.

Својство 2.2. Матрицата $A = [a_{ij}]_{n \times n}$ има инверзна ако $\det A \neq 0$.

Во следниот пример ќе го илустрираме Гаусовиот алгоритам (применување на конечен број на елементарни редични трансформации) за определување на инверзна матрица.

Пример 2.1. Определи ја инверзната матрица (ако постои) на матрицата:

а) $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$;

б) $B = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$.

Решение. а) Од $\det A = \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = 1 \neq 0$ следува дека постои A^{-1} .

Имаме:

$$[A|E] = \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{array} \right] \xrightarrow{R_2 \rightarrow R_2 - R_1} \sim \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{array} \right]$$

$$\xrightarrow{R_1 \rightarrow R_1 - 2R_2} \sim \left[\begin{array}{cc|cc} 1 & 0 & 3 & -2 \\ 0 & 1 & -1 & 1 \end{array} \right] = [E|A^{-1}].$$

Оттука $A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$.

б) Од $\det A = \begin{vmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{vmatrix} = -1 \neq 0$ следува дека постои A^{-1} . Имаме:

$$\begin{aligned}
[A|E] &= \left[\begin{array}{ccc|ccc} 1 & 1 & -1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 & 0 & 1 \end{array} \right] \begin{array}{l} R_2 \rightarrow R_2 - R_1 \\ \sim \\ R_2 \rightarrow R_2 - 2R_1 \end{array} \left[\begin{array}{ccc|ccc} 1 & 1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 1 & 0 \\ 0 & -1 & 3 & -2 & 0 & 1 \end{array} \right] \\
R_1 \rightarrow R_1 + R_2 & \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right] \\
\sim & \\
R_3 \rightarrow R_3 - R_2 & \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right] \\
R_1 \rightarrow R_1 - R_3 & \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & -1 \\ 0 & -1 & 0 & 1 & 3 & -2 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right] \\
\sim & \\
R_2 \rightarrow R_2 - 2R_3 & \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & -1 \\ 0 & -1 & 0 & 1 & 3 & -2 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right] \\
R_2 \rightarrow -R_2 & \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & -1 \\ 0 & 1 & 0 & -1 & -3 & 2 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right] = [E|A^{-1}]. \\
\sim & \\
\text{Оттука } B^{-1} &= \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix}. \blacksquare
\end{aligned}$$

3. Кодирање и декодирање

Во овој дел ќе ја користиме релацијата дадена подолу каде буквите од А до Ш одговараат на броевите од 1 до 31 и празното место одговара на бројот 32, при што интерпунктските знаци не ги земаме во предвид.

А	Б	В	Г	Д	Ѓ	Е	Ж	З	С	И	Ј	К	Л	Љ	М
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Н	Њ	О	П	Р	С	Т	Ќ	У	Ф	Х	Ц	Ч	Џ	Ш	—
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Пример 3.2. Искористи ја матрицата $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ за да ја кодираш пораката:

ПОБАРАЈ МЕ

Решение. Ги делиме буквите од пораката во групи од две букви:

ПО БА РА Ј_ МЕ

Придружуваме соодветни матрици од ред 2×1 на горенаведените групи со нивните соодветни броеви дадени во табелата.

$$\begin{bmatrix} П \\ О \end{bmatrix} \rightarrow \begin{bmatrix} 20 \\ 19 \end{bmatrix}, \begin{bmatrix} Б \\ А \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} Р \\ А \end{bmatrix} \rightarrow \begin{bmatrix} 21 \\ 1 \end{bmatrix}, \begin{bmatrix} Ј \\ _ \end{bmatrix} \rightarrow \begin{bmatrix} 12 \\ 32 \end{bmatrix}, \begin{bmatrix} М \\ Е \end{bmatrix} \rightarrow \begin{bmatrix} 16 \\ 7 \end{bmatrix}.$$

Кодирањето се состои всушност во множење на секоја од овие матрици од лево со матрицата A . Според тоа,

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 19 \end{bmatrix} = \begin{bmatrix} 58 \\ 77 \end{bmatrix},$$

$$\begin{aligned} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} &= \begin{bmatrix} 4 \\ 5 \end{bmatrix}, \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 21 \\ 1 \end{bmatrix} &= \begin{bmatrix} 23 \\ 24 \end{bmatrix}, \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 12 \\ 32 \end{bmatrix} &= \begin{bmatrix} 76 \\ 108 \end{bmatrix} \text{ и} \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 16 \\ 7 \end{bmatrix} &= \begin{bmatrix} 30 \\ 37 \end{bmatrix}. \end{aligned}$$

Значи кодираната порака е:

$$\begin{bmatrix} 58 \\ 77 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} \begin{bmatrix} 23 \\ 24 \end{bmatrix} \begin{bmatrix} 76 \\ 108 \end{bmatrix} \begin{bmatrix} 30 \\ 37 \end{bmatrix},$$

односно 58 77 4 5 23 24 76 108 30 37. ■

Пример 3.3. Декодирај ја пораката

$$\begin{bmatrix} 58 \\ 77 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} \begin{bmatrix} 23 \\ 24 \end{bmatrix} \begin{bmatrix} 76 \\ 108 \end{bmatrix} \begin{bmatrix} 30 \\ 37 \end{bmatrix}$$

со помош на матрицата $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$.

Решение. Бидејќи оваа порака е добиена со кодирање со помош на матрицата A , декодирањето е всушност множење на секоја од 2×1 матриците од лево со матрицата A^{-1} .

Во пример 2.1. а) видовме дека $A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$. Според тоа,

$$\begin{aligned} \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 58 \\ 77 \end{bmatrix} &= \begin{bmatrix} 20 \\ 19 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} &= \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 24 \end{bmatrix} &= \begin{bmatrix} 21 \\ 1 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 76 \\ 108 \end{bmatrix} &= \begin{bmatrix} 12 \\ 32 \end{bmatrix} \text{ и} \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 30 \\ 37 \end{bmatrix} &= \begin{bmatrix} 16 \\ 7 \end{bmatrix}. \end{aligned}$$

Ги бараме соодветните букви кои соодветствуваат на броевите во табелата и ја добиваме пораката ПОБАРАЈ МЕ. ■

Слично како со кирилицата може да се користи абецедата преку релацијата дадена подолу каде буквите од А до Z одговараат на броевите од 1 до 26 и празното место одговара на бројот 27, при што интерпунктските знаци не ги земаме во предвид.

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	—
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Пример 3.4. Со помош на матрицата $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ кодирај ја пораката
ATTACK NOW

Решение. Ги делиме буквите од пораката во групи од две букви:

AT TA CK _N OW

Придружуваме соодветни матрици од ред 2×1 на горенаведените групи со нивните соодветни броеви дадени во табелата.

$$\begin{bmatrix} A \\ T \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 20 \end{bmatrix}, \begin{bmatrix} T \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 20 \\ 1 \end{bmatrix}, \begin{bmatrix} C \\ K \end{bmatrix} \rightarrow \begin{bmatrix} 3 \\ 11 \end{bmatrix}, \begin{bmatrix} _ \\ N \end{bmatrix} \rightarrow \begin{bmatrix} 27 \\ 14 \end{bmatrix}, \begin{bmatrix} O \\ W \end{bmatrix} \rightarrow \begin{bmatrix} 15 \\ 23 \end{bmatrix}.$$

Кодирањето се состои всушност во множење на секоја од овие матрици од лево со матрицата A . Според тоа,

$$\begin{aligned} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} &= \begin{bmatrix} 41 \\ 61 \end{bmatrix}, \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} &= \begin{bmatrix} 22 \\ 23 \end{bmatrix}, \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} &= \begin{bmatrix} 25 \\ 36 \end{bmatrix}, \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} &= \begin{bmatrix} 55 \\ 69 \end{bmatrix} \text{ и} \\ \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} &= \begin{bmatrix} 61 \\ 84 \end{bmatrix}. \end{aligned}$$

Значи кодираната порака е:

$$\begin{bmatrix} 41 \\ 61 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \end{bmatrix} \begin{bmatrix} 25 \\ 36 \end{bmatrix} \begin{bmatrix} 55 \\ 69 \end{bmatrix} \begin{bmatrix} 61 \\ 84 \end{bmatrix},$$

односно 41 61 22 23 25 36 55 69 61 84. ■

Пример 3.5. Декодирај ја пораката

$$\begin{bmatrix} 21 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 53 \end{bmatrix} \begin{bmatrix} 45 \\ 54 \end{bmatrix} \begin{bmatrix} 74 \\ 101 \end{bmatrix} \begin{bmatrix} 53 \\ 69 \end{bmatrix}$$

со помош на матрицата $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$.

Решение. Бидејќи оваа порака е добиена со кодирање со помош на матрицата A , декодирањето е всушност множење на секоја од 2×1 матриците од лево со матрицата A^{-1} .

Според пример 2.1. а) имаме $A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$. Според тоа,

$$\begin{aligned} \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 26 \end{bmatrix} &= \begin{bmatrix} 11 \\ 5 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 37 \\ 53 \end{bmatrix} &= \begin{bmatrix} 5 \\ 16 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 45 \\ 54 \end{bmatrix} &= \begin{bmatrix} 27 \\ 9 \end{bmatrix}, \\ \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 74 \\ 101 \end{bmatrix} &= \begin{bmatrix} 20 \\ 27 \end{bmatrix} \text{ и} \end{aligned}$$

$$\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 53 \\ 69 \end{bmatrix} = \begin{bmatrix} 21 \\ 16 \end{bmatrix}.$$

Ги бараме соодветните букви кои одговараат на броевите во табелата и ја добиваме пораката KEEP IT UP. ■

Ако сакаме да користиме 3×3 матрица за кодирање на некоја порака, наместо делење на буквите во групи од две букви, ги делиме на групи од три букви.

Пример 3.6. Искористи ја матрицата

$$B = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$$

за да ја кодираш пораката

ATTACK NOW

Решение. Ги делиме буквите од пораката во групи од три букви.

ATT ACK _N O W _ _

Придружуваме соодветни матрици од ред 3×1 на горенаведените групи со нивните соодветни броеви дадени во табелата.

$$\begin{bmatrix} A \\ T \\ T \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix}, \begin{bmatrix} A \\ C \\ K \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix}, \begin{bmatrix} N \\ O \end{bmatrix} \rightarrow \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix}, \begin{bmatrix} W \\ - \\ - \end{bmatrix} \rightarrow \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix}.$$

Кодирањето се состои всушност во множење на секоја од овие матрици од лево со матрицата B . Според тоа,

$$\begin{aligned} \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix} &= \begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix}, \\ \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix} &= \begin{bmatrix} -7 \\ 12 \\ 16 \end{bmatrix}, \\ \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix} &= \begin{bmatrix} 26 \\ 42 \\ 83 \end{bmatrix}, \\ \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix} &= \begin{bmatrix} 23 \\ 50 \\ 100 \end{bmatrix}. \end{aligned}$$

Значи кодираната порака е:

$$\begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix} \begin{bmatrix} -7 \\ 12 \\ 16 \end{bmatrix} \begin{bmatrix} 26 \\ 42 \\ 83 \end{bmatrix} \begin{bmatrix} 23 \\ 50 \\ 100 \end{bmatrix},$$

односно 1 21 42 -7 12 16 26 42 83 23 50 100. ■

Пример 3.7. Декодирај ја пораката

$$\begin{bmatrix} 11 \\ 20 \\ 43 \end{bmatrix} \begin{bmatrix} 25 \\ 10 \\ 41 \end{bmatrix} \begin{bmatrix} 22 \\ 14 \\ 41 \end{bmatrix}$$

со помош на матрицата

$$B = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}.$$

Решение. Бидејќи оваа порака е добиена со кодирање со помош на матрицата B , декодирањето е всушност множење на секоја од 2×1 матриците од лево со матрицата B^{-1} . Од пример 2.1. б) имаме:

$$B^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix}.$$

За поедноставен запис наместо матрици од ред 3×1 можеме да користиме една матрица од ред 3×3 од буквите во групите напишани во колони. Според тоа,

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 11 & 25 & 22 \\ 20 & 10 & 14 \\ 43 & 41 & 41 \end{bmatrix} = \begin{bmatrix} 8 & 4 & 9 \\ 15 & 27 & 18 \\ 12 & 6 & 5 \end{bmatrix}.$$

Ги бараме соодветните букви кои одговараат на броевите во табелата и ја добиваме пораката HOLD FIRE. ■

Забелешка. За да се упрости работата со матриците и записот, аналогно како во претходниот пример и во примерите пред него при множењето на матриците може да се користи матрица од ред $2 \times$ бројот на групи или $3 \times$ бројот на групи во кои е поделена пораката.

Задачи за самостојна работа

1. Искористи ја матрицата $A = \begin{bmatrix} 5 & 2 \\ 3 & 3 \end{bmatrix}$ за да ја кодираш пораката
ПИШИ МИ ВЕДНАШ.

2. Декодирај ја пораката

8 23 7 4 47 - 2 15 102 -12 20 58 15 27 80 18 12 74 -7

со помош на матрицата $B = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 1 & 0 & -1 \end{bmatrix}$. Користи ја абecedата.

Литература

- [1] R. Sekhon. Applied Finite Mathematics, 2nd edition, 1996
- [2] К. Тренчевски, Б. Крстевска. Линеарна Алгебра, Универзитет Св. Кирил и Методиј, Скопје, 2019
- [3] Р. Малчески, В. Малческа. Математика 2 – Векторска и линеарна алгебра, Армаганка, Скопје, 2020