**ӘОЖ 51(071.1):378.96**
**ҒТАМР 14.35.09**
**https://doi.org/10.48371/PEDS.2025.76.1.031**

# MS EXCEL КӨМЕГІМЕН ХИЛЛ АЛГОРИТМІН ЕСЕПТЕУ ӘДІСІ

Әбілқасымова А.Е.[1], Жадраева Л.У.[2], *Урстемова Г.К.[3], Темирбекова Ж.Е.[4]
[1,2,*3]Абай атындағы Қазақ Ұлттық педагогикалық университеті,
Алматы, Қазақстан
[4]әл-Фараби атындағы Қазақ Ұлттық университеті,
Алматы, Қазақстан

**Аңдатпа.** Мақалада техникалық жоғары оқу орындары студенттеріне математиканы оқытуда қолданбалы бағытағы есептерді шешуді үйретудің қажетілігі, ал нақтырақ айтсақ, матрица тақырыбын қолданбалы есептер арқылы оқыту қарастырылған. Студенттердің математикаға, болашақ кәсіби мамандығына деген қызығушылығын арттыруда қолданбалы есептердің алатын орны ерекше. Арнайы бағдарламалар арқылы математикалық және қолданбалы бағыттағы есептерді шешуде компьютерлік технологияны қолданудың маңыздылығы зор. Құпия ақпаратты қауіп-қатерден қорғау үшін оны шифрлау керек. Шифрлау алгоритмдерінің бірі – Хилл криптожүйесі. Хилл криптожүйесінде купия деректерді шифрлау және кері шифрлау үшін, құпия кілті ретінде $(n \times n)$ өлшемді матрицаны пайдаланады. Ақпараттың қауіпсіздігін қамтамасыз ету мақсатында, Хилл криптожүйенің көмегімен құпия деректерді нақты уақытта шифрлау және кері шифрлау жылдамдығын арттыру мақсатында MS Excel қолданылады. Мақалада ұсынылған қолданбалы есептердегі өлшемі үлкен матрицаларды MS Excel-де есептеу шамамен 4,2 есе жылдам есептелінді. Ақпараттық қауіпсіздік саласының болашақ мамандарының математикалық дайындығы аясында қолданбалы есептерге қойылатын талаптары нақтыланды. Хилл криптожүйенің негізгі артықшылықтары мен кемшіліктері туралы сипатталды. Матрицаның көмегімен құпия кілттерді генерациялауды, құпия мәтінді шифрлауды, шифрланған мәтінді кері шифрлау әдістерін оқуды оңтайландыру және қолданбалы есептерді шешуге әдістемелік нұсқаулықтар көрсетіліп, Хилл криптожүйенің блок-схемасы құрылып, MS Excel-де жүзеге асырылды. Техникалық жоғары оқу орны студенттеріне математика курсы бойынша қолданбалы бағыттағы кәсіби есептерді шығаруды үйрету арқылы олардың кәсіби тұрғыда құзыретті, білікті маман болып қалыптастыруына үлкен жол ашылады. Сол себепті бұл мақаланың берері көп, маңыздылығы да жоғары.

**Тірек сөздер:** матрица, кері матрица, криптография, шифр мәтін, шифрлау, құпия кілттерді генерациялау, криптожүйе, криптографиялық алгоритм

**Кіріспе**

Басқа барлық пәндер ішінде математика өте абстрактілі және барлық жаратылыстану пәндерінің ішіндегі ең негізгісі. Бекерге гректер бұл пәнді «матема» - білім (грек.) деп айтпаған, себебі ол білімге апарар жолдың кілті. Математика, физика және басқа негізгі пәндер саласында терең білімі бар инженер өзінің кәсіби саласындағы жаңа мәліметтерді оңай меңгереді. Сондықтан, техникалық жоғары оқу орнында білім берудің ең бірінші дәрежелі мақсаттардың бірі инженердің түбегейлі математикалық білімін жетілдіру болып табылады.

Техникалық жоғары оқу орындарында математикалық дайындықтың негізгі міндеттерінің бірі студенттерді қолданбалы есептерді шешуге үйрету болып табылады, сонымен матрицаларға тоқталайық, өйткені бұл тақырып қолданбалы бағыттағы математика курсында ерекше орын алады.

Матрицаның, анықтауыштың қасиеттерін, түрлерін және оларға қолданылатын амалдарды тұжырымдауда, ерекшелігін ашып түсіндіруде студенттердің математикалық терминдерді дұрыс пайдаланып, сөйлеу мәдениетін қалыптастыруда, өзінің ойын сауатты жеткізуге машықтандыруда, тарихи мағлұматтарды зерделеп, ұғымның тарихи қалыптасуына шолу жасауда, кәсіби пәндермен байланыс жасауы маңызды.

Техникалық жоғары оқу орындарында математика курсындағы матрица тақырыбы 1 курста басталады және оны кәсіби мамандыққа сәйкес пәндерді оқытуда қолданбалы бағыты жалғасын табады. Сондықтан студенттердің математиканың барлық бөлімін оқуда әсер етеді, сондай-ақ аналитикалық, шығармашылық ойлауының дамуына зор үлесін қосады. Студенттер $n$-ші ретті анықтауышты тез есептеу және матрицаларды көбейтуге кезінде көп уақыт жұмсайды.

Студенттің математиканың қолданбалы бағытта ойлауын қалыптастыруда, дамытуда оқытушының жаңашылдығы мен әдістемесінің маңыздылығы орасан зор. Соңғы жылдардағы нәтижелерге сүйеніп қарасақ, студенттер қолданбалы бағыттағы есептерді шығару кезінде біршама қиындықтарға тап болуда, оның бірден-бір себебі уақыттың тапшылығы.

Практикалық сабақтарда компьютерді пайдалану үшін бағдарламалық құралдардың барлық түрінің ішінен бағдарламалық құралдардың келесі топтарын қарастырсақ болады:

- кестелік процессор (Microsoft Excel);
- математикалық пакеттер (MathCAD, Maple, Khan Academy және т. б.) [1].

Арнайы бағдарламалар әртүрлі қолданбалы есептерді шешудің ыңғайлы құралдары болып табылады. Олардың көмегімен күнделікті немесе маңызды емес операцияларды орындай отырып, студенттер бірнеше минут ішінде күрделі, көлемді есептеулер жүргізеді, мазмұнды есептерді

шешеді, әртүрлі жағдайларды модельдейді. Сондай-ақ, осы арнайы бағдарламаларды қолданудың артықшылығы - тапсырманы шешудің барлық кезеңдерін визуализациялау мүмкіндігі. Практикалық сабақта студенттерге компьютерді қолдана отырып, математика мен компьютерлік қауіпсіздіктің байланысын көрнекі түрде көрсетуге болады. Сонымен қатар математикалық және кәсіби есептерді шешуде компьютерлік технологияны қолданудың маңызды артықшылықтарын бағалауға мүмкіндік береді.

Зерттеу жұмысының мақсаты — студенттерге математика курсын оқытуда матрицаның көмегімен кілтті генерациялау, құпия мәтінді шифрлау, шифрланған мәтінді кері шифрлау әдістерін оқытуды оңтайландыру және қолданбалы есептерді шешуге әдістемелік нұсқаулықтар көрсету, MS Excel-де Хилл алгоритмін нақты уақытта есептеу, тақырыптың маңызы мен мәнін ұғындыру болып табылады.

**Материалдар мен әдістер**

Педагогикада бірінші орынға оқытудың дамытушылық, тәрбиелік (әсіресе, дүниеге ғылыми көзқарасты тәрбиелеу) мақсаттары мен кәсіби шеберлікті шыңдай білу жоғары орынға қойылады. Әр сабақ студент үшін ойлау мен таразылай білу мектебі болу керек. Оқытушы ғылыми ойлау мен логикалық тұжырым жасай білуге жаттықтырудың бапкері. Оқытушының басты міндеті – тыңдаушысын қуанышқа бөлеу және танымдық сезімін ояту, қызығушылығына қамшы салу, өз бетімен ойлауына жағдай туғызу.

Оқытушының математикадан практикалық сабақтағы міндеттері төмендегідей болады:

-көрсетілген тақырып бойынша есепті шығару әдісін (үлгісін) түсіндіру;

-есептің шығару жолын (үлгісін) талдау;

-түсіндіру барысында студенттер сұрағына жауап беру;

-нәтижені тексеру;

-мотивацияны үздіксіз қалыптастыру арқылы таным процесін басқару.

Сондықтан, сабақтың тақырыбын тереңірек меңгеру үшін белгілі дидактикалық тәсіл – қарапайым есептен, күрделі есепке, содан кейін кәсіби бағдарланған қолданбалы есептерге көшу. Соңында бақылау арқылы сабақтың мақсаты орындалғанына көз жеткізу қажет. Студенттер арасында жарыс элементтерін енгізе отырып, олардың ойлау жүйесін ширақ ұстап, есепті көбірек шығаруға ынталандыру үшін оқытушының өзіндік тәсіл-әрекеттерінің жиынтығы болуы керек. Нақты жағдайларда тақырыпты студенттер нәтижелі меңгеруі үшін, сабақтың әдістемелік қамтамасыз етілуі ақпараттық және дидактикалық материалдың ең тиімді берілуі туралы қағидаларға бағынуы керек.

Қазіргі криптография – ғылымның ең көп қажет ететін салаларының бірі. Атап айтқанда, онда қазіргі алгебраның барлық дерлік бөлімдері қолданылады. Бұл алгебраның басқа криптографиялық пәндерді зерттеуде кеңінен қолданылатын негізгі пәндердің бірі екендігін түсіндіреді.

Криптография – бұл ақпаратты білмейтін адамдар үшін түсініксіз болатындай етіп түрлендіру арқылы қорғау туралы ғылым. Криптографияның классикалық әдістерінің бірі-американдық математик Лестер Хиллдің атымен аталған Хилл шифры [2]. Бұл шифрлау әдісі матрицалар мен сызықтық алгебраны қолдануға негізделген және XX ғасырдың басында жасалған. Хилл шифрының негізгі идеясы - кілтті (матрицаны) пайдаланып ашық мәтінді шифр мәтініне түрлендіру және кері матрицаны пайдаланып шифр мәтінін ашық мәтінге кері түрлендіру [3]. Шифрлау және шифрды шешу процесі алфавит өлшемі модулі бойынша сәйкес матрицаларды бір-біріне көбейту болып табылады (әдетте ағылшын алфавиті үшін 26)

Хиллдің криптографиялық шифры құпия ақпаратты шифрлау арқылы қорғауды қажет ететін әртүрлі салаларда қолданылады.

- *байланыс және деректерді беру:* Хилл шифрын электрондық пошта, мессенджерлер немесе басқа байланыс құралдары арқылы жіберілетін хабарламалардың құпиялылығын қорғау үшін пайдалануға болады. Бұл жіберуші мен қабылдаушыға үшінші тұлғалардың хабарламалардың мазмұнын ұстап алудан және ашудан қорықпай ақпарат алмасуға мүмкіндік береді [4];

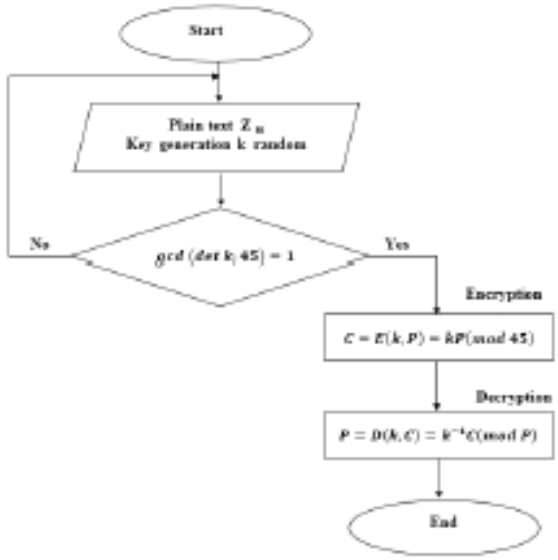
- *файлдарды шифрлау:* компьютерлік қауіпсіздікте Хилл шифрын компьютердегі немесе желідегі файлдар мен деректерді қорғау үшін қолдануға болады. Бұл әсіресе құпия құжаттарды беру немесе сезімтал ақпаратты деректер тасымалдаушыларында сақтау кезінде пайдалы болуы мүмкін [5];

- *банктік транзакциялар:* қаржы саласында Хилл шифрын банктік транзакциялар мен клиенттер туралы ақпаратты қорғау үшін пайдалануға болады. Бұл банктер мен клиенттер арасындағы төлемдер, баланстар және басқа қаржылық операциялар туралы деректерді беру кезінде қауіпсіздікті қамтамасыз етуге көмектеседі.

- *әскери байланыс:* қорғаныс саласында Хилл шифрын әскери байланысты шифрлау, әскери ақпаратты ұстап қалудан қорғау және талдау үшін қолдануға болады. Бұл стратегиялық командалардың қауіпсіздігін және әскери бөлімшелер арасындағы жедел өзара әрекеттесуді қамтамасыз ету үшін маңызды;

- *білім беру мақсаттары:* Хилл шифры криптография мен сызықтық алгебра негіздерін зерттеу үшін білім беру мақсатында да қолданылады. Бұл студенттерге ақпаратты қорғаудың заманауи жүйелерінде қолданылатын шифрлау принциптерін түсінуге көмектеседі [6].

Жалпы алғанда, Хилл криптографиялық шифры берілетін немесе сақталатын ақпараттың құпиялылығы мен қауіпсіздігін қамтамасыз ету талап етілетін әртүрлі салаларда қолданудың кең ауқымына ие [7, 327 б.]. Хилл криптографиялық шифрының жалпы блок схемасы 1-суретте көрсетілген.




Сурет 1 - Хилл криптожүйесі

**Есеп.** Қазақ әліппесінің нөмірленген цифрларын сақинасындағы $K = \begin{pmatrix} 1 & 1 & 0 & 3 \\ 1 & 0 & 1 & 4 \\ 0 & 3 & 4 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix}$ кілттік матрицасын (құпия кілт генерациялау) және Хилл криптожүйесін қолданып:

а) мәтінді шифрлау: **КРИПТОГРАММА – ШИФРЛАНҒАН МӘТІН.**

б) криптограммасын жазу;

в) алынған криптограмманы кері шифрлау.

**Шешуі:** $K$ матрицасының анықтауышын есептейік:

$$|K| = \begin{vmatrix} 1 & 1 & 0 & 3 \\ 1 & 0 & 1 & 4 \\ 0 & 3 & 4 & 1 \\ 2 & 5 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 0 & 3 \\ 0 & -1 & 1 & 1 \\ 0 & 3 & 4 & 1 \\ 0 & 4 & 1 & -6 \end{vmatrix} = \begin{vmatrix} -1 & 1 & 1 \\ 3 & 4 & 1 \\ 3 & 1 & -6 \end{vmatrix} =$$

$$= -1 \cdot 4 \cdot (-6) + 3 \cdot 1 \cdot 1 + 1 \cdot 1 \cdot 3 - 1 \cdot 4 \cdot 3 - 1 \cdot 1 \cdot (-1) - 1 \cdot 3 \cdot (-6) =$$

$$= 24 + 3 + 3 - 12 + 1 + 18 = 37.$$

$|K| = 37.\ (37,45) = 1$ өзара жай сандар. Ал $37^{-1} mod\ 45 = 28$ екенін ескерейік. $K$ матрицасының $K^{-1}$ кері матрицасын табайық:

Ашық мәтін ретінде қазақ әліпбиіндегі реттік нөмірлермен тыныс белгілеріде нөмірленеді.

КРИПТОГРАММА – ШИФРЛАНҒАН МӘТІН.

| К | Р | И | П | Т | О | Г | Р | А | М | М | А | - | Ш | И |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 22 | 11 | 21 | 24 | 19 | 04 | 22 | 00 | 16 | 16 | 00 | 42 | 33 | 11 |
| Ф | Р | Л | А | Н | Ғ | А | Н | _ | М | Ә | Т | І | Н | . |
| 28 | 22 | 15 | 00 | 17 | 05 | 00 | 17 | 43 | 16 | 01 | 24 | 37 | 17 | 44 |

Енді әрбір реттік нөмірі бойынша нөмірленген блокты негізгі матрицаға, яғни 8 рет көбейту керек. Нөмірленген блоктарды тіктөртбұрышты $(8 \times 4)$ $X$ матрицасының жолдары ретінде жазылып және оны оң жағынан $K$ кілт матрицаға көбейтіп, $Y$ матрицасы алынады, оның жолдарында шифрланған мәтіннің реттік нөмірі бойынша нөмірленген блоктары жазылады:

$$Y = XK = \begin{pmatrix} 13 & 22 & 11 & 21 \\ 24 & 19 & 4 & 22 \\ 0 & 16 & 16 & 0 \\ 42 & 43 & 42 & 33 \\ 11 & 28 & 22 & 15 \\ 0 & 17 & 5 & 0 \\ 17 & 42 & 16 & 1 \\ 24 & 37 & 17 & 44 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 3 \\ 1 & 0 & 1 & 4 \\ 0 & 3 & 4 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 77 & 151 & 87 & 138 \\ 87 & 146 & 57 & 152 \\ 16 & 48 & 80 & 80 \\ 151 & 333 & 244 & 340 \\ 69 & 152 & 131 & 167 \\ 17 & 15 & 37 & 73 \\ 61 & 70 & 107 & 235 \\ 149 & 295 & 149 & 237 \end{pmatrix} mod\ 45 = \begin{pmatrix} 32 & 16 & 42 & 3 \\ 42 & 11 & 12 & 17 \\ 16 & 3 & 35 & 35 \\ 16 & 18 & 19 & 25 \\ 24 & 17 & 41 & 32 \\ 17 & 15 & 37 & 28 \\ 16 & 25 & 17 & 10 \\ 14 & 25 & 14 & 12 \end{pmatrix}$$

Осылайша, біз шифрланған мәтін алынады: 32, 16, 42, 3, 42, 11, 12, 17, 16, 3, 35, 35, 16, 18, 19, 25, 24, 17, 41, 32, 17, 15, 37, 28, 16, 25, 17, 10, 14, 25, 14, 12. Келесідей криптограмма алынады:

Ч М - В – ИЙНМКЪЪМҢОУТНЯЧН ЛІФМУНЗҚУЛЙ.

Құпия мәтінді кері шифрлау:

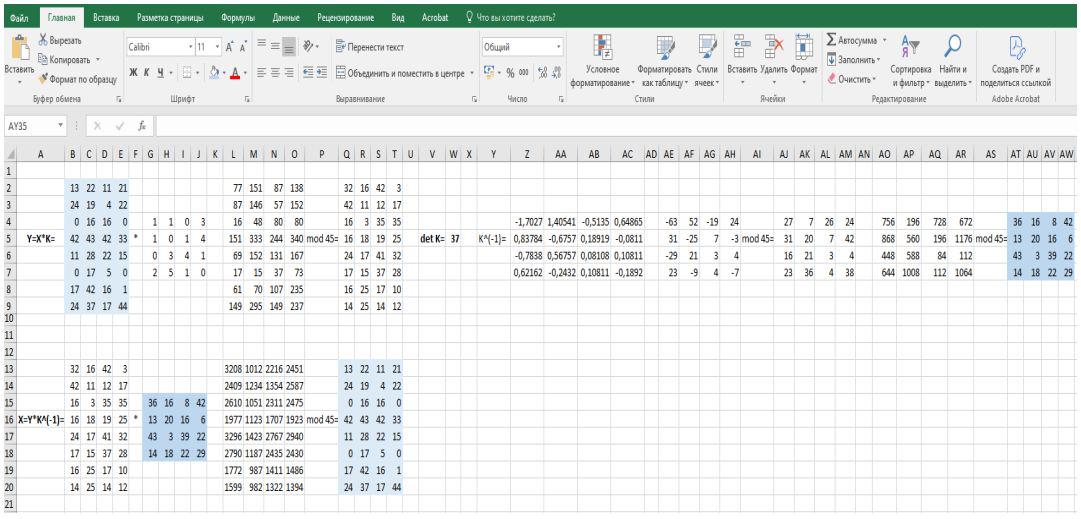
Ч М - В - ИЙНМКЪЪМҢОУТНЯЧН ЛІФМУНЗҚУЛЙ криптограммасы реттік нөмірі бойынша нөмірленеді: 32, 16, 42, 3, 42, 11, 12, 17, 16, 3, 35, 35, 16, 18, 19, 25, 24, 17, 41, 32, 17, 15, 37, 28, 16, 25, 17, 10, 14, 25, 14, 12. Әрі қарай, шифрланған мәтінбөліктерге бөлінеді: 32, 16, 42, 3; 42, 11, 12, 17; 16, 3, 35, 35; 16, 18, 19, 25; 24, 17, 41, 32; 17, 15, 37, 28; 16, 25, 17, 10; 14, 25, 14, 12. Осыдан өлшемі (8×4) *Y* матрицасы құрылады және ол $K^{-1}$ кері матрицаға көбейтіледі:

$$Y = XK^{-1} = \begin{pmatrix} 32 & 16 & 42 & 3 \\ 42 & 11 & 12 & 17 \\ 16 & 3 & 35 & 35 \\ 16 & 18 & 19 & 25 \\ 24 & 17 & 41 & 32 \\ 17 & 15 & 37 & 28 \\ 16 & 25 & 17 & 10 \\ 14 & 25 & 14 & 12 \end{pmatrix} \cdot \begin{pmatrix} 36 & 16 & 8 & 42 \\ 13 & 20 & 16 & 6 \\ 43 & 3 & 39 & 22 \\ 14 & 18 & 22 & 29 \end{pmatrix} =$$

$$\begin{pmatrix} 3208 & 1012 & 2216 & 2451 \\ 2409 & 1234 & 1354 & 2587 \\ 2610 & 1051 & 2311 & 2475 \\ 1977 & 1123 & 1707 & 1923 \\ 3296 & 1423 & 2767 & 2940 \\ 2790 & 1187 & 2435 & 2430 \\ 1772 & 987 & 1411 & 1486 \\ 1599 & 982 & 1322 & 1394 \end{pmatrix} mod\ 45 = \begin{pmatrix} 13 & 22 & 11 & 21 \\ 24 & 19 & 4 & 22 \\ 0 & 16 & 16 & 0 \\ 42 & 43 & 42 & 33 \\ 11 & 28 & 22 & 15 \\ 0 & 17 & 5 & 0 \\ 17 & 42 & 16 & 1 \\ 24 & 37 & 17 & 44 \end{pmatrix}$$

Алынған матрицаның жолдарын жаза отырып, реттік нөмірі бойынша нөмірленген ашық мәтін алынады 13, 22, 11, 21, 24, 19, 4, 22, 0, 16, 16, 0, 42, 33, 11, 28, 22, 15, 0, 17, 5, 0, 17, 43, 16, 1, 24, 37, 17. 44. Әріптерге өтіп, бастапқы мәтін алынады: **КРИПТОГРАММА – ШИФРЛАНҒАН МӘТІН.**

Үлкен өлшемді құпия деректермен жұмыс жасауда MS Excel-ді қолдану тиімді. Осы жоғарыда келтірілген есепті есептеу барысында MS Excel-ді мүмкіншіліктерін қолданып матрицаларды көбейтуде, анықтауышты тез есептеуге қол жеткізілді, ол 2-суретте көрсетілген.



Сурет 2 - MS Excel-де Хилл алгоритмін іске асыру

***Есепті шығаруға арналған әдістемелік нұсқаулық***

Минорды, алгебралық толықтауышты қалай табамыз? $n$-ші ретті анықтауышты қалай есептейміз? Матрица дегеніміз не? $n$-ші ретті матрицаларды қалай көбейтеміз? Кері матрицаларды қалай табамыз?

$n$-ші ретті $\Delta$ анықтауыштың $a_{ik}$ элементінің $M_{ik}$ миноры деп, $\Delta$ анықтауыштың $i$ жолын және $k$ бағанын сызып тастағаннан соң қалған $(n-1)$-ші ретті анықтауышты айтады, ал $n$-ші ретті $\Delta$ анықтауыштың $a_{ik}$ элементінің $A_{ik}$ алгебралық толықтауышы деп $(-1)^{i+k}$ таңбамен алынған оның минорын айтады, яғни $A_{ik} = (-1)^{i+k} M_{ik}$.

$n$ -ші ретті анықтауыш деп мына түрде жазылған:

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix},$$

$n$ санын айтады.

–ші ретті анықтауышты есептеу үшін анықтауыштын ретін төмендетіп ең болмағанда 3-ші реттіге келтіріп келесі формуланың көмегімен есептейміз.

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{13} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

және үшбұрыштар тәсілі арқылы есептелінетін $\Delta -$ санын айтады.

$m$ жолдан $n$ бағаннан тұратын, тік бұрышты сандар кестесі $m \times n$ өлшемді матрица деп аталады да, мына жазулардың бірімен белгіленеді:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} =$$

$$= \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{Vmatrix} = [a_{ij}], \qquad i = \overline{1,m}, \quad j = \overline{1,n}.$$

$a_{ij} \quad (i = \overline{1,m}, \quad j = \overline{1,n})$ сандары матрицаның элементтері деп аталады. Екі матрицаны $A$ және $B$-ы *келісілген* дейді, егер $A$ матрицаның бағандарының саны $B$ матрицаның жолдарының санына тең болса, яғни $A_{m\times n}$ және $B_{n\times k}$ болса. Тек екі келісілген матрицаларды бір-бірімен көбейтуге болады.

$A_{m\times n}=[a_{ij}]$ және $B_{n\times k}=[b_{ij}]$ матрицалардың көбейтіндісі деп, элементтері мына формуламен есептелінетін

$$c_{ij}=\sum_{s=1}^{n}a_{is}b_{sj}, \quad (i=\overline{1,m}, \quad j=\overline{1,k}),$$

жаңа $C_{m\times k}=A\cdot B$ матрицасын айтады.

$A^{-1}$ матрицаны $A$ матрицаға кері дейді, егер мына теңдік орындалса

$$A\cdot A^{-1}=A^{-1}\cdot A=E.$$

**Теорема.** Квадрат $A$ матрицаның кері матрицасы болу үшін, оның өзгеше емес болуы қажетті және жеткілікті.

Кері матрица мына формуламен есептелінеді:

$$A^{-1}=\frac{1}{|A|}\begin{bmatrix}A_{11} & A_{21} & \dots & A_{n1}\\ A_{12} & A_{22} & \dots & A_{n2}\\ \dots & \dots & \dots & \dots\\ A_{1n} & A_{2n} & \dots & A_{nn}\end{bmatrix}.$$

**Нәтижелер**

Матрицаның көмегімен Хилл алгоритмін есептеу кезінде студенттердің деңгейі мен қызығушылығын анықтау үшін 2023 жылдың қыркүйек айы мен 2024 жылдың ақпан айы аралығында тәжірибелік-эксперименттік зерттеу жұмыстары ұйымдастырылды.

Педагогикалық эксперимент жұмысы 2023-2024 оқу жылында Алматы қаласындағы әл-Фараби атындағы Қазақ Ұлттық университетінің, Ақпараттық технологиялар факультетінің «6B06301-Ақпараттық қауіпсіздік жүйелер» білім беру бағдарламасы бойынша білім алатын студенттерімен өткізілді.

Тәжірибелік-эксперименттік жұмыстың мақсаты:

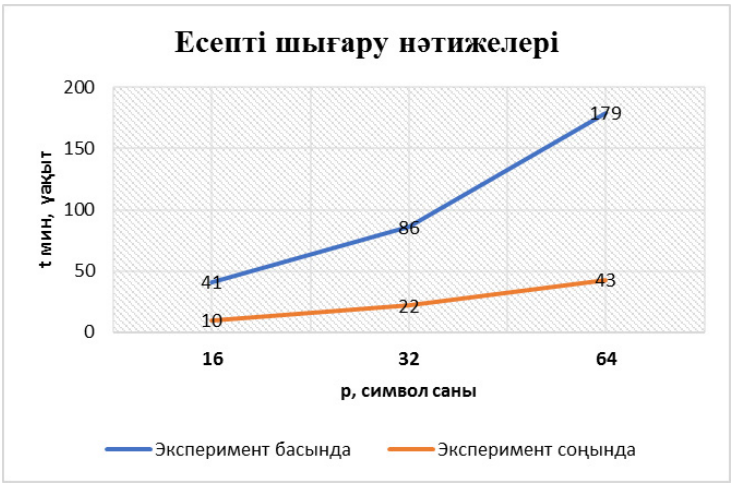
- жоғары оқу орындарында қолданбалы есептерді шығаруда студенттердің білім деңгейін анықтау;

- жоғары оқу орындарында қолданбалы есептерді шығаруда тиімді әдістерді оқытуды ұйымдастыру, әртүрлі әдістермен есептерді шығаруға үйрету, компьютерлік бағдарламаларды қолдану, пәнаралық байланыстарды жүзеге асыру әдістемесінің тиімділігін дәлелдеу;

- қорытынды нәтижелік кезеңінде: MS Excel көмегімен Хилл алгоритмін есептеу әдісін оқытудың тиімділігін анықтау.

Мониторингті жүргізудің құралы ретінде, яғни 2023 жылдың қыркүйек айы мен 2024 жылдың ақпан айы аралығында жоғары оқу орны студенттерінің тақырыпты түсіну деңгейін анықтау мақсатында бағалау жұмысы өткізілді.

Бағалау жұмысында MS Excel көмегімен Хилл алгоритмін есептеудің 16, 32, 64 разрядты (символ саны) ашық мәтін қарастырылды. Есепті қолмен есептеу кезінде әр түрлі рязрядта ашық мәтінді шифрлау және кері шифрлау үшін шамамен 4,2 есе уақыт көп жұмсалды. Эксперименттік жұмыс жүргізілгеннен кейін эксперименттің нәтижелерін бақылау мақсатында бақылау тобы мен эксперименттік топтың соңғы нәтижелері кесте түрінде (3-сурет) көрсетілді.




Сурет 3 – Студенттердің есепті шығару нәтижелері

Жүргізілген зерттеулер нәтижесінде келесідей қорытындылар жасалды:

- студенттердің болашақ мамандықтарына деген қызығушылығы мен пәнаралық байланысы артты;
- есептерді шешу студенттердің математикалық дайындығын күшейтуге бағытталуы және оның басты міндеті кәсіби маман даярлау сапасын арттыруына ықпал етеді;
- жоғары оқу орындарында MS Excel көмегімен Хилл криптожүйесін есептеу әдісі бойынша ұсынылған әдістеменің педагогикалық тиімділігі эксперимент арқылы тексеріліп, нәтижелер шығарылды.

**Талқылау**

Студенттерге математиканы оқыту процесінде қолданбалы бағытта берілген есептерді шығаруда аналитикалық және шығармашылық ойлауының жеткіліксіз дамуы әсерінен математиканы игеруде кедергілер

туындайтыны тәжірибе көрсетіп отыр, әсіресе алгебра курсын оқу барысында жоғары оқу орындарында кәсіби пәндерді меңгеруде елеулі қиындықтар туғызады. Жоғары оқу орны студенттерінің қолданбалы математика бойынша *түсініктері* мен ойлауын қалыптастыру мен дамытуға ғалым-әдіскерлердің еңбектері арналған.

Қазіргі уақытта қолданбалы бағыттын қолданып оқытудың құзыреттілік тәсіліне арналған зерттеулер өзекті болып табылады. Бұл тәсіл өз бетінше білім алуға, стандартты емес мәселелерді шешуге шығармашылық көзқарасқа үйретуді қамтиды. Көптеген ғалымдардың еңбектерінде оқытудың қолданбалы бағытының қажеттілігі теориялық тұрғыдан негізделген.

А.Е. Әбілқасымова «Оқу жоспары аясында математикадан элементар математикалық алгоритмдерден бастап жоғары оқу орнына арналған математика курсының мазмұны бойынша қолданбалы сипаттағы есептерге дейінгі барлық кәсіби маңызды білімдердің тізімін келісу қажет және ол студенттерге математиканың теориялық бөлімдері мен олардың қосымшалары арасындағы байланысты тереңірек түсінуге көмектеседі» - деп тұжырымдайды [8, 68 б].

Білім беруді дамытудың барлық кезеңдерінде оқытудың қолданбалы бағыты туралы мәселені бүкіл әлемнің прогрессивті педагогтары үнемі көтеріп отырды. Мысалы, XIX–XX ғасырлардағы әйгілі ғалым П. Ф. Лесгафт теория практикаға және практикаға нұсқауға сәйкес болған кезде ғана сұранысқа ие болады деп есептеді. П. Ф. Лесгафт теориялық материалды ресми түрде жаттауды сынға алды. «Жоғары мектепте тыңдаушы өз ойын өз бетінше дамытып, оны өмірде қолдана білуі керек» – деп айтты [9,127 б.].

Техникалық жоғары оқу орнында еңбек ететін атақты әдіскер-педагогтар мен ғалымдар Б.В. Гнеденко, Д.Б. Гнеденко [10], ойынша, математика курсын пәнді ары қарай танып кәсіби құзыреттілігіне қызығушылығын оятатын, теорияның практикамен байланысын көрсететін біліммен толықтыру керек. Білім берудің қазіргі құзыретті парадигмасы дәстүрлі «білімдар» парадигмасын жоққа шығару емес, керісінше оның негізінде құрылады.

- студенттердің бойында іргелі математикалық білімді қалыптастыру;
- болашақ кәсіби қызметінде, атап айтсақ, математикалық модельдеу дағдыларын қалыптастыруда математикалық білімдерін қолдануды үйрету;
- осы дағдылардың қолданылу мүмкіндіктерін арттыратын құзыреттілік жеке тұлғаның ерекше қасиетін қалыптастырады.

«Қолданбалы тапсырма» ұғымына жүгінген кезде біз А.А. Столяр берген анықтаманы қолданайық [11]. Қолданбалы тапсырма арқылы автор математикадан тыс қойылған және математикалық құралдармен шешілетін есепті түсінеді.

М.И. Махмутов оқытудың қолданбалы бағыты «Педагогикалық құралдарды (оқытудың мазмұны, формалары, әдістері) пайдалану, бұл студенттердің бағдарламаларында қарастырылған минималды білім, білік және дағдыларды игеруін қамтамасыз ете отырып, сонымен бірге осы мамандыққа деген қарым-қатынас сипаты, жеке тұлғаның кәсіби қасиеттерін қалыптастыру бойынша біртұтас дамуға ықпал етеді» - деп санайды [12, 52 б.].

Техникалық жоғары оқу орындарында студенттерді математикалық дайындаудың ұстанымдарын С.Д.Тыныбекова [13] ашып көрсеткен. Оның пікірінше, дайындықтың негізін жалпы математика курсы қалайды, демек ол «ядро» болып табылады, ал «сыртқы қабатын» жоғары математикадан арнайы кафедралармен бірлесе оттырып жазылған арнайы курстар, курстық жобалар мен дипломдық жұмыстардың математикалық модельдері құрайды.

Жоғары оқу орындарындағы студенттерді математикалық даярлау мәселесін шешудің бір жолы ретінде кәсіби бағдарланған оқыту деп айтады [14].

Ақпараттық қауіпсіздік саласындағы студенттердің математикалық дайындығы маңызды рөл атқарады, өйткені криптография, шифрлау алгоритмдері және осалдықтарды талдау терең математикалық түсінікті қажет етеді. Ақпараттық қауіпсіздік саласындағы студенттердің математикалық дайындығы мен күткен нәтижелері арасындағы алшақтықты талдайды. Бұл мәселені шешу үшін докторантура деңгейінде арнайы математикалық курстар енгізілген, ал магистратура бағдарламасында талаптарды қайта қарау керек. Мақсат – білім берудің қатаңдығын сақтай отырып, оны барлық студенттер үшін қолжетімді ету деп айтады [15].

**Қорытынды**

Іздеу және шығармашылық типтегі есептерді шешуге үйрету ақпараттық қауіпсіздік саласындағы мамандардың математикалық дайындығының қолданбалы бағытын жүзеге асырудың маңызды бағыттарының бірі. Мұнда қолданбалы есептер ерекше рөл атқаруы керек.

Ақпараттық қауіпсіздік саласының болашақ мамандарының математикалық дайындығы аясында қолданбалы есептерге қойылатын талаптары нақтыланды:

- есептерде зерттелетін математикалық аппаратты кәсіби тәжірибеде қолдану мүмкіндіктерін көрсететін нақты мазмұны болуы керек;

- есептер жалпы техникалық және арнайы пәндерді оқу кезінде математикалық аппараттың қолданылуын, оқытылатын пәндердің өзара байланысын көрсету керек;

- есептерді шешу студенттердің математикалық дайындығын күшейтуге бағытталуы керек, оның басты міндеті кәсіби маман даярлау сапасын арттыру болып табылады;

- ақпараттық қауіпсіздік саласының болашақ мамандарын дайындайтын жоғары оқу орындары үшін дәстүрлі оқыту түрлерімен қатар (дәрістер, практикалық сабақтар) компьютерді практикалық сабақтарда қолданып өткізуді енгізу қажет.

Артықшылықтары мен кемшіліктері:

- Хилл шифрінің негізгі артықшылықтарының бірі - оның кейбір басқа шифрлау әдістерімен салыстырғанда салыстырмалы қарапайымдылығы мен тиімділігі. Ол «жиіліктік талдау» шабуылдарына жақсы қарсылықты қамтамасыз етеді, онда қарсылас шифрлық мәтінде әріптер мен биграммалардың пайда болу жиілігін талдайды.

- Хилл шифрінде кейбір кемшіліктер бар. Олардың бірі - белгілі бір өлшемдегі шаршы матрицаларды пайдалану қажеттілігі, бұл кілттерді таңдауды шектейді. Оған қоса, толық шифрлау қауіпсіздігі үлкен кілттерді пайдалануды талап етеді, бұл әдіс кейбір қолданбалар үшін тиімсіз болуы мүмкін.

Қорытындылай келе, студенттерге матрицаның көмегімен кілттерді генерациялауды, құпия мәтінді шифрлауды, шифрланған мәтінді кері шифрлау әдістерін оқуды оңтайландыру және қолданбалы есептерді шешуге әдістемелік нұсқаулықтар көрсетіліп, Хилл алгоритмі блок-схемасы құрылып, MS Excel-де нақты уақытта есептелді. Нәтижесінде мақалада ұсынылған әдіс шамамен 4,2 есе жылдам орындалды.

Студенттерге мұндай қолданбалы есептерді шығаруды үйретудің дұрыс ұйымдастырылуы, оларды сәйкесінше берілген формулалар, анықтамалар мен алдыңғы дәлелденген теоремалар арқылы толықтай түсінуге мүмкіндік береді.

Студенттер тапсырмаларды орындау барысында зерттеу жүргізу тәжірибесін, атап айтқанда жоспарлауды, болжауды, аналитикалық модельдер құруды, эксперимент нәтижелерін өңдеуді игереді. Мұның бәрі студенттердің математикалық, жалпы кәсіби және арнайы пәндерге деген қызығушылығының артуына ықпал етеді. Ақпаратты қорғау саласындағы кәсіби құзыретті маман дайындауда, студенттерге математикадан қолданбалы есептерді тиімді әдістермен шығаруды үйретудің маңызы зор.

Зерттеу жұмысы Абай атындағы Қазақ Ұлттық педагогикалық университетінің ғылыми жоба есебінен қаржыландырып отыр (14.05.2024 ж., бұйрық No05-04/329).

## ӘДЕБИЕТ

[1]. Кадирбаева Р.И.,Әтірбек Қ.Е. Болашақ математика мұғалімдерін даярлау процесінде аралас оқыту технологиясын қолданудың ерекшеліктері // «Абылай хан атындағы ҚазХҚжәнеӘТУ Хабаршысы» журналы, «Педагогика ғылымдары» сериясы. – 2024. - No4(75).- 415-437 б. – Кіру

режимі: URL: https://doi.org/10.48371/PEDS.2024.75.4.026 [Қаралған күні 14.09.2024]

[2] A.P.U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," Int. J. Adv. Appl. Sci., vol. 6, no. 4, 2017. – pp. 313-318.

[3] F.H. Khan, R. Shams, F. Qazi, dan D.-E.-S. Agha, "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix," Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, 2015. – 5-7 p.

[4] A.P.U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," Int. J. Sci. Res., vol. 5, no. 7, 2016. – pp. 1149-1152.

[5] W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005. - 328 p.

[6] Temirbekova Zh.E., Pyrkova A.Yu. "Improving teachers' skills to integrate the microcontroller technology in computer engineering education", Education and information technology, 2022. – pp. 8381-8412. doi:10.1007/s10639-021-10875-8

[7] *Брюс Шнайер*. *Прикладная криптография*. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: «Триумф». – 2002. - 816 с.

[8] Абылкасымова А.Е., Молдабекова М.С., Тыныбекова С.Д. Вопросы профессионально-педагогической направленности обучения в вузе. - Алматы, 1999. - 130 с.

[9] Лесгафт П.Ф. Избранные педагогические сочинения / сост. И.Н. Решетель – М.: Педагогика 1988. - 345 с.

[10] Об обучении математике в университетах и педвузах на рубеже двух тысячелетий / Б. В. Гнеденко, Д. Б. Гнеденко. - 3-е изд., испр. и доп. - М.: Ком-Книга, 2006. - 160 с. - (Психология, педагогика, технология обучения: математика).

[11] Столяр А. А. Педагогика математики. Учеб. пособие для студентов физико-математического факультета педагогических вузов – Минск: Вышэйшая школа, 1986. - 414 с.

[12] Махмутов М.И., Власенков А.М. Принципы профессиональной направленности преподавания в среднем ПТУ // Принципы обучения в среднем ПТУ: сб. научн. трудов / под ред. А.А. Кирсанова – М: изд-во АПН СССР, 1986. – С.50-53.

[13] Тыныбекова С.Ж. Профессионально-педагогическая направленность математической подготовки студентов технических вузов: Дисс.докт.пед.наук. А.: 2001. – 230 с.

[14] Toktarova, V.I. Professionally Oriented Mathematical Training of Students in Higher Educational Institutions /V.I. Toktarova // Proceedings of ADVED 2018 - 4th International Conference on Advances in Education and Social Sciences. – 2018. – pp. 402-406.

[15] Wolthusen, S. in IFIP International Federation for Information Processing, Volume 237. Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer). – 2007. – pp. 129-136.

## REFERENCES

[1] Kadirbaeva R.İ., Ätırbek Q.E. Bolaşaq matematika mūğalımderın daiarlau prosesında aralas oqytu tehnologiasyn qoldanudyñ erekşelıkterı (Features of the application of blended learning technology in the process of training future mathematics teachers) // «Abylai han atyndağy QazHQjäneÄTU Habarşysy» jurnaly, «Pedagogika ğylymdary» seriasy. – 2024. – No4 (75). - 415-437 bb. – Kiru rezhimi URL: https://doi.org/10.48371/PEDS.2024.75.4.026 [Qaralğan küni 14.09.2024] [in Kaz.]

[2] A.P.U. Siahaan, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” Int. J. Adv. Appl. Sci., vol. 6, no. 4, 2017. – pp. 313-318 [in Eng.]

[3] F.H. Khan, R. Shams, F. Qazi, dan D.-E.-S. Agha, “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix,” Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, 2015. – pp. 5-7 [in Eng.]

[4] A.P.U. Siahaan, “Three-Pass Protocol Concept in Hill Cipher Encryption Technique,” Int. J. Sci. Res., vol. 5, no. 7, 2016. – pp. 1149-1152. [in Eng.]

[5] W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005. - 328 p. [in Eng.]

[6] Temirbekova Zh.E., Pyrkova A.Yu. “Improving teachers’ skills to integrate the microcontroller technology in computer engineering education”, Education and information technology, 2022. – pp. 8381-8412. doi:10.1007/s10639-021-10875-8 [in Eng.]

[7] Bryus Shnaier. Prikladnaya kriptografiya Protokoly, algoritmy, iskhodnye teksty na yazyke Si (Applied cryptography. Protocols, algorithms, and source texts in C.). - M.: “Triumf”, 2002. - 816 s. [in Rus.]

[8] Abylkasymova A.E., Moldabekova M.S., Tynybekova S.D. Voprosy professional’no-pedagogicheskoi napravlennosti obucheniya v vuze (Issues of professional and pedagogical orientation of higher education education.). – Almaty, 1999. - 130 s. [in Rus.]

[9] Lesgaft P.F. Izbrannye pedagogicheskie sochineniya (Selected pedagogical writings) / sost. I.N. Reshetel’ – M.: Pedagogika 1988. - 345 s. [in Rus.]

[10] Ob obuchenii matematike v universitetakh i pedvuzakh na rubezhe dvukh tysyacheletii (About teaching mathematics at universities and colleges at the turn of two millennia) / B. V. Gnedenko, D. B. Gnedenko. - 3-e izd., ispr. i dop. - M.: Kom-Kniga, 2006. - 160 s. - (Psikhologiya, pedagogika, tekhnologiya obucheniya: matematika). [in Rus.]

[11] Stolyar A. A. Pedagogika matematiki (The pedagogy of mathematics.).

Ucheb. posobie dlya studentov fiziko-matematicheskogo fakul'teta pedagogicheskikh vuzov – Minsk: Vysheishaya shkola, 1986. - 414 s. [in Rus.]

[12] Makhmutov M.I., Vlasenkov A.M. Printsipy professional'noi napravlennosti prepodavaniya v srednem PTU (Principles of professional orientation of teaching in secondary vocational schools)// Printsipy obucheniya v srednem PTU: sb. nauchn. trudov / pod red. A.A. Kirsanova – M: izd-vo APN SSSR, 1986. – S.50-53. [in Rus.]

[13] Tynybekova S.Zh. Professional'no-pedagogicheskaya napravlennost' matematicheskoi podgotovki studentov tekhnicheskikh vuzov: Diss.dokt. ped.nauk. (Professional and pedagogical orientation of mathematical training of students of technical universities: Dissertation of Doctor of pedagogical sciences.). A.: 2001. - 230 s. [in Rus.]

[14] Toktarova, V.I. Professionally Oriented Mathematical Training of Students in Higher Educational Institutions /V.I. Toktarova // Proceedings of ADVED 2018 - 4th International Conference on Advances in Education and Social Sciences. – 2018. – pp. 402-406. [in Eng]

[15] Wolthusen, S. in IFIP International Federation for Information Processing, Volume 237. Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer). – 2007. – pp. 129-136 [in Eng.]

## МЕТОД ВЫЧИСЛЕНИЯ АЛГОРИТМА ХИЛЛА С ПОМОЩЬЮ MS EXCEL

Абылкасымова А.Е.[1], Жадраева Л.У.[2], *Урстемова Г.К.[3], Темирбекова Ж.Е.[4]
[1,2,*3]Казахский национальный педагогический университет им. Абая, Алматы, Казахстан
[4]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

**Аннотация.** В статье рассматривается необходимость обучения студентов технических вузов решению задач прикладной направленности в обучении математике, а в частности, изучение матричной темы с помощью прикладных задач. Особое место в повышении интереса студентов к математике, будущей профессиональной профессии занимают прикладные задачи. Большое значение имеет использование компьютерных технологий при решении задач математической и прикладной направленности с помощью специальных программ. Чтобы защитить конфиденциальную информацию от угроз, ее необходимо зашифровать. Одним из алгоритмов шифрования является криптосистема Хилла. В криптосистеме Хилла для шифрования и обратного шифрования конфиденциальных данных используется матрица размера ($n \times n$) в качестве секретного ключа. В целях обеспечения

согласованности информации используется MS Excel с целью повышения скорости шифрования и обратного шифрования конфиденциальных данных в режиме реального времени с помощью криптосистемы Хилла. Расчет больших по размеру матриц в прикладных задачах, представленных в статье, в MS Excel вычислялся примерно в 4,2 раза быстрее. Уточнены требования будущих специалистов в области информационной безопасности к прикладным задачам в рамках математической подготовки. Хилл описал основные преимущества и недостатки криптосистемы. С помощью матрицы были продемонстрированы методические рекомендации по оптимизации генерации секретных ключей, шифрования секретного текста, считывания методов обратного шифрования зашифрованного текста и решения прикладных задач, создана блок-схема криптосистемы Хилла и реализована в MS Excel. Обучение студентов технического вуза решению профессиональных задач прикладной направленности по курсу математики открывает большой путь к их профессиональному становлению компетентным, квалифицированным специалистом. По этой причине эта статья имеет большое значение.

**Ключевые слова:** матрица, обратная матрица, криптография, зашифрованный текст, шифрования, генерация ключей, криптосистема, криптографический алгоритм

## THE METHOD OF CALCULATING HILL'S ALGORITHM THROUGH A MS EXCEL

Abylkassymova A.[1], Zhadraeva L.[2], *Urstemova G.[3], Temirbekova Zh.[4]
[1,2,*3]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[4]Al-Farabi Kazakh National University, Almaty, Kazakhstan

**Abstract.** The article considers the need to teach students of technical universities to solve problems of an applied orientation in teaching mathematics, and in particular, the study of a matrix topic using applied problems. Applied tasks occupy a special place in increasing students' interest in mathematics, the future professional profession. The use of computer technology in solving mathematical and applied problems with the help of special programs is of great importance. To protect confidential information from threats, it must be encrypted. One of the encryption algorithms is Hill's cryptosystem. Hill's cryptosystem uses a matrix of size ($n \times n$) as a secret key to encrypt and reverse encrypt confidential data. In order to ensure the consistency of information, MS Excel is used to increase the encryption speed and reverse encryption of confidential data in real time using the Hill cryptosystem. The calculation of large matrices in the applied problems presented in the article in MS Excel was calculated about 4.2 times faster. The requirements of future information security specialists for applied

tasks within the framework of mathematical training have been clarified. Hill described the main advantages and disadvantages of the cryptosystem. Using the matrix, methodological recommendations were demonstrated for optimizing the generation of secret keys, encryption of secret text, reading methods of reverse encryption of encrypted text and solving applied problems, a block diagram of the Hill cryptosystem was created and implemented in MS Excel. Teaching students of a technical university to solve professional problems of an applied orientation in the course of mathematics opens a great way to their professional development as a competent, qualified specialist. For this reason, this article is of great importance.

**Key words:** matrix, inverse matrix, cryptography, ciphertext, encryption, secret keys generation, cryptosystem, cryptographic algorithm

*Мақала түсті: 13 маусым 2024*

**Авторлар туралы мәлімет**

Әбілқасымова Алма Есімбекқызы - педагогика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, РБА академигі, Абай атындағы Қазақ Ұлттық педагогикалық университеті, e-mail: aabylkassymova@mail.ru

Жадраева Лариса Уштановна – педагогика ғылымдарының докторы, қауымдастырылған профессор, Абай атындағы Қазақ Ұлттық педагогикалық университеті, e-mail: lari_6308@mail.ru

Урстемова Гульмира Кабылбековна – Абай атындағы Қазақ Ұлттық педагогикалық университеті докторанты, e-mail: gulmira_7008@mail.ru

Темирбекова Жанерке Ерлановна – PhD, доцент м.а, әл-Фараби атындағы Қазақ Ұлттық университеті, e-mail: temyrbekovazhanerke2@gmail.com

**Информация об авторах**

Абылкасымова Алма Есимбековна - доктор педагогических наук, профессор, академик НАН РК, академик РАО, Казахский национальный педагогический университет им.Абая e-mail: aabylkassymova@mail.ru

Жадраева Лариса Уштановна – доктор педагогических наук, ассоциированный профессор Казахский национальный педагогический университет им. Абая, e-mail: lari_6308@mail.ru

Урстемова Гульмира Кабылбековна – докторант Казахский национальный педагогический университет им. Абая, e-mail: gulmira_7008@mail.ru

Темирбекова Жанерке Ерлановна – PhD, и.о. доцента Казахский национальный университет им. аль-Фараби, e-mail: temyrbekovazhanerke2@gmail.com

**Information about authors**

Abylkassymova Alma Yessimbekovna – Doctor of Pedagogical Sciences, professor, Academician of the National Academy of Sciences of the Republic of Kazakhstan, Academician of the Russian Academy of Education, Kazakh National Pedagogical University named after Abai, e-mail: aabylkassymova@mail.ru

Zhadraeva Larisa Ushtanovna – Doctor of Pedagogical Sciences, Associate Professor Kazakh National Pedagogical University named after Abai, e-mail: lari_6308@mail.ru

Urstemova Gulmira Kabylbekovna – doctoral student Kazakh National Pedagogical University named after Abai, e-mail: gulmira_7008@mail.ru

Temirbekova Zhanerke Erlanovna – PhD, Acting Associate Professor Al-Farabi Kazakh National University, e-mail: temyrbekovazhanerke2@gmail.com