ҒТАМР 14.25.09

ҚЫСҚА МЕРЗІМДІ ЭЛЕКТИВТІ КУРС ТӘЖІРИБЕСІНДЕ КРИПТОГРАФИЯ ЭЛЕМЕНТТЕРІ АРҚЫЛЫ ГАУСС ӘДІСІН ОҚЫТУ ӘДІСТЕМЕСІ

МЕТОДИКА ОБУЧЕНИЯ МЕТОДУ ГАУССА С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ КРИПТОГРАФИИ В ПРАКТИКЕ КРАТКОСРОЧНОГО ЭЛЕКТИВНОГО КУРСА

METHODOLOGY FOR TEACHING THE GAUSS METHOD USING CRYPTOGRAPHY ELEMENTS IN A SHORT-TERM ELECTIVE COURSE

Б.Б. Сағынтаева [1]*, **Н.Д. Мархабатов** [2]
[1] Шәкәрім университеті КеАҚ, Семей, Казақстан
[2] Л.Н. Гумилев атындағы Еуразия ұлттық университеті Астана қаласы, Қазақстан
*Жауапты-автор: Сағынтаева Бақытжан Бауыржанқызы, e-mail: kbskyt@mail.ru

Ключевые слова:
криптография, метод Гаусса, системы линейных уравнений, алгоритмическое и логическое мышление, методика обучения математике, элективный курс.

АННОТАЦИЯ

В условиях стремительного развития цифровых технологий особую значимость приобретает проблема информационной безопасности. Криптография рассматривается как эффективный научный инструмент защиты информации — одного из важнейших ресурсов современного общества. В то же время в образовательной практике, особенно в школьном курсе математики, наблюдаются трудности в усвоении абстрактных тем. В этой связи использование элементов криптографии может рассматриваться как один из эффективных способов решения данной проблемы. Иными словами, возрастает значение обучения математике на основе прикладного содержания. Включение элементов криптографии способствует формированию более глубокого понимания изучаемого материала.

Целью исследования является разработка эффективной методики обучения методу Гаусса на основе элементов криптографии для решения систем линейных уравнений, а также определение её влияния на развитие познавательных способностей учащихся.

В ходе исследования использовались теоретические методы (анализ, моделирование) и эмпирические методы, включая педагогический эксперимент. Эксперимент был проведён в средней общеобразовательной школе №45 города Семей. В исследовании приняли участие 22 учащихся 9 класса. В процессе реализации элективного курса рассматривалось преобразование задач криптографического содержания в системы линейных уравнений. Полученные системы решались с использованием метода Гаусса.

Результаты проведённого исследования показали, что использование элементов криптографии способствует развитию алгоритмического и логического мышления учащихся. Кроме того, это помогает более глубоко понять математические понятия и повышает интерес к изучению предмета.

С практической точки зрения предложенная методика может быть внедрена в школьный курс математики в формате элективного предмета. Также она способствует усилению межпредметных связей.

Түйінді сөздер:
криптография, Гаусс әдісі, сызық теңдеулер жүйесі, алгоритмдік және логикалық ойлау, математиканы оқыту әдістемесі, элективті курс.

ТҮЙІНДЕМЕ

Қазіргі цифрлы технологиялар дамыған заманда ақпараттық қауіпсіздік мәселесі орасан маңызға ие. XXI ғасырда адамзат үшін маңызды активтердің бірі – ақпарат, дерек болып табылады. Сол активтерді қорғауда ғылыми құрал негізінде криптография пайдаланылады. Криптография ғылыми құрал ретінде қолданылу аясы кең. Әрбір күнделікті көптеген алмасып жатқан ақпаратты шифрлау, қорғаумен қатар математиканың мектеп бағдарламасында да өзекті болады. Мысалы, оқушыларға кейбір абстрактілі тақырыптарды игеру қиынға соғады. Сондай тақырыптарды қызық әрі жеңіл түрде криптография элементтері арқылы түсіндіре аламыз.

Зерттеудің негізгі мақсаты – сызықтық теңдеулер жүйесін криптография элементтерін кіріктіре отырып, Гаусс әдісі арқылы шешуді оқушыларға үйрету. Оқыту процесін оңтайландыратын әдістеме ұсыну. Ұсынылған әдістеме нәтижесіне байланысты оқушылардың танымдық қабілеттерін де дамыту.

Зерттеу жұмысы барысында теориялық талдау, модельдеу және педагогикалық эксперимент әдістері қолданылды. Эксперимент Семей қаласындағы №45 жалпы білім беретін мектепте ұйымдастырылды. Тәжірибелік жұмысқа 9-сыныптан 22 оқушы қатысты. Элективті курсты өткізу кезінде криптологиялық мазмұндағы есептерді сызықтық теңдеулер жүйесіне келтіру көзделді. Ал алынған сызықтық теңдеулер жүйесін Гаусс әдісімен шешуге арналған тапсырмалар пайдаланылды.

Криптография элементтерін пайдалану элективті курсы барысында оқушыларға оң әсер ететіндігі анықталды. Оқушылардың алгоритм бойынша жұмыс жасауы, логикалық ойтізбегін дұрыс құруы жақсаруы көрсетілді. Сонымен қатар, жалпы математика пәніне деген қызығушылық артқаны байқалды.

Жүргізілген зерттеу аясында криптография элементтерін пайдалану оқушылардың алгоритмдік және логикалық ойлау дағдыларын дамытуға ықпал ететіндігі анықталды. Сондай-ақ,математикалық ұғымдарды тереңірек түсінуге көмектесіп, пәнге деген қызығушылықтарын арттырды.

Практикалық тұрғыдан алғанда, ұсынылған әдістеме мектептің математика бағдарламасында элективті пән ретінде қолданыла алады. Сонымен қатар, пәнаралық байланысты күшейтуге мүмкіндік береді.

keywords:

ABSTRACT

cryptography, Gauss method, systems of linear equations,

algorithmic and logical thinking, mathematics teaching methodology, elective course.

In the context of the rapid development of digital technologies, the issue of information security is becoming increasingly important. Cryptography is considered an effective scientific tool for protecting information, which is one of the most valuable resources of modern society. At the same time, in educational practice, particularly in school mathematics, students often face difficulties in understanding abstract concepts. In this regard, the use of cryptography elements can be seen as an effective way to address this problem. In other words, there is a growing need to teach mathematics through applied content. The integration of cryptography elements contributes to a deeper understanding of mathematical concepts.

The aim of this study is to develop an effective methodology for teaching the Gauss method based on cryptography elements for solving systems of linear equations, as well as to assess its impact on the development of students' cognitive abilities.

The study employed both theoretical methods (analysis, modeling) and empirical methods, including a pedagogical experiment. The experiment was conducted at Secondary School No. 45 in the city of Semey and involved 22 ninth-grade students. During the implementation of the elective course, tasks of a cryptographic nature were transformed into systems of linear equations. These systems were then solved using the Gauss method.

The results of the study showed that the use of cryptography elements contributes to the development of students' algorithmic and logical thinking. In addition, it facilitates a deeper understanding of mathematical concepts and increases students' interest in the subject.

From a practical perspective, the proposed methodology can be implemented in the school mathematics curriculum as an elective course. It also promotes the strengthening of interdisciplinary connections.

КІРІСПЕ

Қазіргі ақпараттық қоғамда деректерді сақтау мен қорғау мәселесі бұрынғыдан да маңызды бола түсті. Цифрлық технологиялар күн сайын дамып, интернет арқылы ақпарат алмасу көлемі үнемі артып келеді. Осындай жағдай негізінде ақпараттың қауіпсіздігін қамтамасыз ету қажеттілігі айқын сезіледі. Өз кезегінде, бұл үдеріс криптографияның рөлін бұрынғыдан да күшейтіп отыр.

Криптография негізінен ақпаратты құпиялау және сыртқы әсерлерден қорғау жолдарын зерттейтін ғылым болып табылады. Криптография тек техникалық салалармен ғана емес, сонымен қатар математикамен де тығыз байланысты. Әсіресе алгебра, дискретті математика және ықтималдық теориясы криптографиялық тәсілдердің негізін құрайды [1].

Заманауи криптографиялық жүйелерді қарастыру көбіне олардың алгебралық модельдерін құрудан басталады. Себебі, көптеген криптографиялық алгоритмдер Буль функциялары арқылы немесе бірнеше айнымалысы бар күрделі теңдеулер жүйесі түрінде беріледі [2], [3]. Көп жағдайда мұндай жүйелер сызықтық емес сипатқа ие болады, нәтижесінде бірден шешімін табу қиындық тудырады. Осыған байланысты криптоанализде жүйені ықшамдау, қарапайым түрге келтіру тәсілдері жиі қолданылады. Ұсынылған тәсіл бойынша негізгі мақсат – күрделі құрылымды барынша жеңіл әрі түсінікті деңгейге жеткізу. Сол себепті, теңдеулерді сызықтық жүйеге айналдыру әдістері кеңінен пайдаланылады. Осындай тәсілдердің бірі – Extended Linearization (XL) әдісі. Аталған әдіс қосымша айнымалылар енгізу арқылы бастапқы жүйені қайта құруға мүмкіндік береді [4].

Ал, алынған сызықтық теңдеулер жүйесін шешуде классикалық тәсілдер қолданылады. Солардың ішінде Гаусс әдісі қарапайымдылығы мен тиімділігіне байланысты ерекше орын алады [5]. Бұл әдіс тек ғылыми еспетерді шешуде ғана емес, сонымен қатар оқыту процесінде де өте қолайлы болып табылады. Өйткені, Гаусс әдісінің қадамдары нақты әрі жүйелі түрде орындалады.

Сонымен қатар, криптографияда Буль функциялары теориясының маңызы ерекше. Себебі, көптеген шифрлау алгоритмдері дәл осы функцияларға сүйенеді [6]. Криптографиялық примитивтерді алгебралық түрде көрсету оларды тереңірек талдауға және беріктік деңгейін бағалауға жол ашады. Өз кезегінде мұндай тәсіл күрделі процестерді жүйелі түрде түсінуге мүмкіндік береді.

Ал білім беру саласына келсек, математика пәнін оқытуда абстрактілі ұғымдарды меңгеру әлі де өзекті мәселелердің бірі болып отыр. Кейбір зерттеулерде оқушылардың сызықтық теңдеулер жүйесін шешу алгоритмдерін жаттап алғанымен, оның мәнін толық түсіне бермейтіні атап көрсетіледі [7]. Сондықтан, оқыту барысында тек формальды тәсілмен шектелмей, мазмұнды терең ашуға бағытталған әдістерді қолдану қажеттігі айқындалады. Осы тұрғыдан алғанда, қолданбалы және пәнаралық бағыттағы тәсілдерді енгізу маңызды рөл атқарады.

Математика сабақтарына криптография элементтерін енгізу оқушылардың пәнге деген қызығушылығын арттыруға ықпал етеді. Сонымен бірге мұндай тапсырмалар білімалушылардың алгоритмдік ойлауын дамытып, логикалық пайымдау қабілеттерін күшейтеді [8], [9]. Нақты мазмұнмен байланысқан тапсырмалар оқушыларға күрделі тақырыптарды жеңілірек қабылдауға көмектеседі.

Оқыту барысында схемалар мен модельдерді қолдану да өз нәтижесін береді. Бұл тәсілдер ақпаратты реттеп, түсінікті түрде ұсынуға мүмкіндік жасайды. Соның нәтижесінде материалды меңгеру жеңілдей түседі [10].

Жалпы алғанда, криптография элементтері арқылы Гаусс әдісін оқыту тиімді бағыттардың бірі деп қарастыруға болады. Алайда, осы саладағы әдістемелік мәселелер толық зерттелді деген тұжырым жасау қиын. Сол себепті, бұл бағытта арнайы әдістемелік негіздерді дамыту қажет. Сондықтан аталған тақырыптың өзектілігі айқын көрінеді.

ӘДЕБИЕТТЕРГЕ ШОЛУ

Криптографияны математикалық білім беруге енгізу мәселесі соңғы жылдары зерттеушілердің назарын барған сайын көбірек аударып отыр. Arifin (2025) матрица теориясы мен деректерді шифрлау арасындағы байланысты талдай отырып, криптографиялық ұғымдарды мектептегі математика сабақтарына интеграциялаудың білім алушылардың цифрлық сауаттылығын арттыруға тікелей ықпал ететінін дәлелдейді [8]. Зерттеуші цифрлық дәуірде математикалық модельдеу дағдыларын дамыту үшін қолданбалы криптографиялық есептердің маңызды педагогикалық құрал екенін атап өтеді.

Dewi et al. (2021) болашақ математика мұғалімдерінің сызықтық теңдеулер жүйесін шешудегі концептуалды түсінік деңгейін зерттеген. Олар оқушылардың алгоритмді механикалық жаттап орындайтынын, бірақ математикалық мазмұнды терең ұғынбайтынын анықтаған [7]. Бұл тұжырым ұсынылған зерттеудің негізгі проблемасымен тікелей сәйкес келеді және криптографиялық мазмұн арқылы абстрактілі ұғымдарды нақтылаудың қажеттігін растайды.

Krishnan & Eng (2024) сызықтық алгебраны оқытудағы шығармашылық тәсілдерді зерттей отырып, практикалық бағытта берілген есептердің оқушылардың математикалық ойлауын дамытуға қомақты үлес қосатынын дәлелдеген [10]. Ұсынылып отырған зерттеу де осы бағытта жасалған болса да, ерекшелігі мынада: криптографиялық есептер арнайы

элективті курс шеңберінде кезең-кезеңімен күрделендірілетін жүйемен беріледі, бұл бұрынғы зерттеулерде сирек кездесетін дидактикалық нақтылық болып табылады.

Алгебралық криптоанализ саласындағы зерттеулер де (Horáček, 2019; Ünal, 2024) сызықтық теңдеулер жүйесінің шифрлауды талдаудағы орталық рөлін айқындайды [5, 6]. Сондай-ақ Попов & Яковлева (2020) схемалау тәсілдері арқылы оқушылардың математикалық түсінігін тереңдетуге болатынын дәлелдейді [9]. Осы зерттеулерді жинақтай келе, криптография элементтерін Гаусс әдісімен оқытуды біріктіретін тұтас дидактикалық модель туралы жарияланған жұмыстардың жеткіліксіздігі анық байқалады — дәл осы олқылық ұсынылып отырған зерттеудің ғылыми жаңалығын негіздейді.

ЗЕРТТЕУ МАТЕРИАЛДАРЫ МЕН ӘДІСТЕРІ

Мақалада әртүрлі ғылыми-педагогикалық тәсілдер өзара үйлестіріліп қолданылды. Жұмыс барысында теориялық және эмпирикалық әдістер қатар пайдаланылды. Зерттеудің теориялық негізі ретінде криптография, сызықтық алгебра және математиканы оқыту әдістемесіне қатысты отандық және шетелдік еңбектер қарастырылды.Әдебиеттерді талдау кезінде салыстыру, жүйелеу, қорытындылау тәсілдері қолданылды [1-6]. Сонымен бірге криптографиялық есептерді сызықтық теңдеулер жүйесіне айналдыру процесі арнайы модельдеу арқылы қарастырылды. Мұндай тәсіл зерттеліп отырған тақырыпты тереңірек түсінуге мүмкіндік береді.

Эмпирикалық кезеңде зерттеу педагогикалық эксперимент түрінде жүргізілді. Тәжірибелік жұмыс Семей қаласындағы №45 жалпы орта білім беретін мектепте ұйымдастырылды. Экспериментке 9-сыныпта оқитын 22 оқушы қатысты. Эксперименттің мақсаты криптография элементтерін қолдана отырып, Гаусс әдісін оқытудың қаншалықты тиімді екенін анықтауға бағытталды.

Зерттеу аясында педагогикалық эксперимент үш кезең бойынша ұйымдастырылды: диагностикалық, қалыптастырушы және бақылау.

Диагностикалық кезеңде оқушылардың сызықтық теңдеулер жүйесін шешу бойынша бастапқы деңгейі анықталды. Эксперимент қатысушыларына дәстүрлі форматтағы 5 тапсырмадан тұратын бақылау жұмысы берілді. Ұсынылған тапсырмалар екі және үш айнымалысы бар сызықтық теңдеулер жүйесін шешуге бағытталды. Оқушылар берілген сызықтық теңдеулер жүйесін матрицалық түрде жазып, шешу барысында белгілі алгоритмдерді қолданды. Әр тапсырма 0-ден 2 ұпайға дейін бағаланды. Әр толық дұрыс жауап – 2 ұпай, жартылай дұрыс жауап – 1 ұпай, қате жауап үшін 0 ұпай тиесілі болды. Жалпы ең жоғарғы ұпай саны 10-ға тең болды. Жиналған ұпайлар негізінде оқушылардың деңгейі үш топқа бөлінді: 0 мен 4 ұпай аралығында төмен, 5 пен 7 ұпай аралығында орта және 8 бен 10 ұпай аралығында жоғары. Нәтижелерді талдау барысында оқушылардың басым бөлігі есеп шығару қадамдарын орындағанымен, оның мәнін толық түсіне бермейтіні байқалды. Бұл жағдай оқушылардың әрекетінде жаттау элементтерінің басым екенін көрсетеді.

Қалыптастырушы кезеңде оқыту процесі қысқа мерзімді элективті курс ретінде ұйымдастырылды. Курс бағдарламасы криптография элементтеріне негізделе құрылды. Ұсынылған тапсырмалар біртіндеп күрделеніп отырды.

Оқушыларға сабақ барысында алдымен қарапайым шифрлау тапсырмалары берілді. Келесі кезеңде XOR операциясына байланысты логикалық есептер қарастырылды. Одан кейін криптографиялық өрнектерді сызықтық теңдеулер жүйесіне айналдыру және есептерді Гаусс әдісімен шешу тапсырмалары ұсынылды.

Оқыту кезінде көрнекі құралдар, модельдеу тәсілдері және алгоритмдік амалдар қолданылды. Практикалық бағытқа да ерекше көңіл бөлінді. Сонымен қатар, оқушылардың оқу нәтижелері ағымдағы тапсырмалар арқылы үнемі бақылауда болды.

Бақылау кезеңінде оқушылардың оқу нәтижелері қайта тексерілді. Бұл жолы берілген тапсырмалар құрылымы жағынан бастапқы кезеңге ұқсас болды, бірақ мазмұны сәл күрделірек жасалды. Оқушылар криптография элементтері енгізілген есептерді орындап, сызықтық теңдеулер жүйесін Гаусс әдісі арқылы шешті. Кейін алынған нәтижелер бастапқы көрсеткіштермен салыстырылды. Жасалған салыстыру негізінде оқыту тәсілінің тиімділігі бағаланды.

Зерттеу барысында педагогикалық бақылау, тестілеу және салыстырмалы талдау әдістері қолданылды. Сонымен қатар алынған нәтижелер сапалық тұрғыдан қарастырылды. Жиналған деректер оқушылардың математикалық ұғымдарды қаншалықты түсінетінін, алгоритмдік ойлау деңгейінің қалай өзгергенін және пәнге деген қызығушылығының артқанын бағалауға мүмкіндік берді. Жалпы алғанда, қолданылған әдістер жиынтығы криптография элементтері арқылы Гаусс әдісін оқытудың тиімділігін жан-жақты қарастыруға жағдай жасады.

Криптографияның математикалық негіздері. Қазіргі цифрлық қоғам жағдайында криптография ақпараттық қауіпсіздікті қамтамасыз етудің маңызды ғылыми бағыттарының бірі ретінде қарастырылады. Ол ақпаратты қорғауға арналған математикалық әдістер жүйесін құрай отырып, алгебра, дискретті математика және ықтималдық теориясы сияқты іргелі ғылым салаларына сүйенеді [1]. Осыған байланысты заманауи криптографиялық алгоритмдер ақпаратты түрлендіру барысында күрделі алгебралық құрылымдарды кеңінен қолданады.

Булев функциялар екілік айнымалыларға тәуелді болып, логикалық амалдар - AND, OR, XOR арқылы анықталады. Аталған функциялар криптографиялық примитивтердің теориялық негізін құрайды және шифрлау алгоритмдерінің ішкі құрылымын сипаттауда маңызды рөл атқарады [6]. Әсіресе, XOR операциясының маңызы ерекше, себебі ол екілік өрістегі қосу амалына сәйкес келеді және сызықтық қасиеттерімен сипатталады. Бұл қасиеттер криптографиялық процестерді алгебралық тұрғыдан модельдеуге, сондай-ақ оларды теңдеулер жүйесі түрінде өрнектеуге мүмкіндік береді [1].

Сонымен қатар, криптографиялық алгоритмдерді алгебралық тәсілмен сипаттау криптоанализдің жетекші бағыттарының бірі болып табылады. Мұндай жағдайда шифрлау үдерісі көп айнымалысы бар теңдеулер жүйесі ретінде қарастырылады. Ал осы жүйені шешу арқылы құпия кілтті немесе бастапқы ақпаратты анықтауға мүмкіндік туындайды [2].

Гаусс әдісінің криптологиядағы қолданылуы. Алгебралық криптоанализ шеңберінде криптографиялық алгоритмдер, әдетте, сызықтық емес теңдеулер жүйесі түрінде қарастырылады [2], [4]. Аталған жүйелерді тікелей шешу едәуір күрделі болғандықтан, оларды қарапайым әрі есептеуге ыңғайлы түрге келтіру қажеттілігі туындайды. Осыған байланысты зерттеулерде теңдеулер жүйесін сызықтық түрге келтіру әдістері кеңінен қолданылады.

Сызықтық түрлендірудің мәні – сызықтық емес мүшелерді жаңа айнымалылармен алмастыру арқылы бастапқы жүйені сызықтық теңдеулер жүйесіне келтіру болып табылады [4]. Бұл тәсіл, әсіресе, Extended Linearization (XL) әдісінде тиімді жүзеге асырылады және криптоанализде практикалық маңызы жоғары құралдардың бірі ретінде қарастырылады.

Алынған сызықтық теңдеулер жүйесін шешуде классикалық әрі тиімді тәсілдердің бірі – Гаусс әдісі. Бұл әдіс матрицаны сатылы немесе қысқартылған сатылы түрге келтіру арқылы айнымалылардың мәндерін кезең-кезеңімен анықтауға мүмкіндік береді және есептеу тиімділігімен ерекшеленеді [5]. Сызықтық жүйенің жалпы түрі келесідей өрнектеледі:

$$Ax = b$$

мұндағы

A - коэффициенттер матрицасы, x - айнымалылар векторы, ал b - бос мүшелер векторы.

Жалпы алғанда, криптографиялық есептерді алгебралық әдістер арқылы шешу үдерісі бірнеше өзара байланысты кезеңдерден тұрады: алдымен криптографиялық модель құрылады, кейін ол теңдеулер жүйесі түрінде сипатталады, одан соң сызықтық теңдеулер жүйесіне түрлендіріледі және соңғы кезеңде алынған жүйе Гаусс әдісі арқылы шешіледі. Мұндай кезеңдік құрылым тек есепті шешудің тиімді жолын қамтамасыз етіп қана қоймай, сонымен қатар күрделі криптографиялық есептерді жүйелі түрде талдауға мүмкіндік береді.

Гаусс әдісін оқытудың дидактикалық моделі. Жоғарыда қарастырылған теориялық негіздерге сүйене отырып, криптография элементтері арқылы Гаусс әдісін оқыту арнайы құрастырылған дидактикалық модель негізінде ұйымдастырылады. Аталған модель оқыту процесін жүйелі түрде құрылымдауға, сондай-ақ оқушылардың күрделі математикалық ұғымдарды бірізді және саналы түрде меңгеруіне жағдай жасайды.

Ұсынылып отырған дидактикалық модель үш өзара байланысты кезеңнен тұрады: модельдеу, сызықтандыру және Гаусс әдісі арқылы шешу. Бірінші кезеңде криптографиялық есеп математикалық модель түрінде сипатталады, келесі кезеңде ол сызықтық теңдеулер жүйесіне келтіріледі, ал соңғы кезеңде алынған жүйе Гаусс әдісі арқылы шешіледі.

Осы кезеңдердің әрқайсысы оқушылардың алгоритмдік ойлауын дамытуға, математикалық модельдеу дағдыларын қалыптастыруға және күрделі есептерді кезең-кезеңімен шешу қабілетін жетілдіруге бағытталған. Сонымен қатар, бұл тәсіл теориялық білім мен практикалық қолданудың өзара байланысын қамтамасыз етеді, нәтижесінде оқу материалының мазмұны терең әрі түсінікті меңгеріледі.

Криптография элементтері негізінде есептер жүйесі. Ұсынылған дидактикалық модельді тиімді жүзеге асыру мақсатында оқушыларға криптография элементтеріне негізделген, мазмұны жағынан біртіндеп күрделенетін есептер жүйесі әзірленді. Аталған есептер жүйесі оқушылардың бастапқы қарапайым ұғымдарды меңгеруінен бастап, күрделі математикалық модельдерді түсінуіне дейін кезең-кезеңімен дамуын қамтамасыз етеді.

Бұл жүйе оқыту үдерісінің логикасына сәйкес төрт деңгей бойынша құрылды. Әрбір деңгей алдыңғы кезеңде қалыптасқан білім мен дағдыларға сүйене отырып, келесі деңгейге өтуді қамтамасыз етеді.

Бірінші деңгейде қарапайым шифрлау тапсырмалары ұсынылады, бұл оқушыларды криптографияның негізгі ұғымдарымен таныстыруға бағытталған. Екінші деңгейде XOR операциясына негізделген логикалық есептер қарастырылады, мұнда оқушылар екілік амалдардың қасиеттерін тәжірибе жүзінде меңгереді. Үшінші деңгейде криптографиялық өрнектерді сызықтық теңдеулер жүйесіне келтіру дағдылары қалыптастырылады. Ал төртінші, қорытынды деңгейде алынған сызықтық теңдеулер жүйесін Гаусс әдісі арқылы шешу жүзеге асырылады.

Ұсынылған есептер жүйесі оқушылардың логикалық және алгоритмдік ойлау қабілеттерін дамытуға, сондай-ақ математикалық білімдерін практикалық тұрғыда қолдану дағдыларын қалыптастыруға мүмкіндік береді.

Қарапайым шифрлау тапсырмалары білім алушыларды криптографияның бастапқы ұғымдарымен таныстыруға және ақпаратты түрлендірудің элементар алгоритмдерін меңгертуге бағытталған. Бұл деңгейде оқушылар символдарды кодтау, шифрлау және кері шифрлау үдерістерінің мәнін түсініп, олардың өзара байланысын анықтайды. Сонымен

қатар, белгілі бір ережелерге сәйкес әріптердің өзгеруін бақылау арқылы олар математикалық заңдылықтарды байқауға дағдыланады.

Аталған кезеңде негізінен классикалық криптографияға тән алмастыру және орын ауыстыру әдістері қарастырылады. Солардың бірі - Полибий квадраты әдісі. Бұл тәсілде әрбір әріп арнайы кестедегі координаталар арқылы кодталады, яғни символдық ақпарат сандық формаға түрлендіріледі. Мұндай түрлендіру білім алушыларға кодтау үдерісінің мәнін көрнекі түрде түсінуге мүмкіндік береді.

Мысалы, Полибий квадраты негізінде сөзді шифрлау тапсырмаларын орындау барысында оқушылар координаталық жүйемен жұмыс істеу дағдыларын дамытады. Әріптердің кестедегі орнын анықтау кезінде олар жол мен баған ұғымдарын нақты қолданады. Нәтижесінде әріптер екі таңбалы сандар арқылы өрнектеліп, шифрмәтін құрылады. Бұл үдеріс білім алушылардың логикалық ойлау қабілетін жетілдіріп, ақпаратты құрылымдау дағдыларын қалыптастырады.

Сонымен қатар, қарапайым шифрлау тапсырмалары құрамына орын ауыстыру әдістері де енгізіледі. Мұндай тапсырмаларда мәтіндегі символдардың орны өзгергенімен, олардың мағынасы сақталады. Бұл тәсіл білім алушыларға ақпараттың мазмұны мен оның берілу формасының айырмашылығын түсінуге мүмкіндік береді.

Осы деңгейдегі тапсырмалардың маңызды ерекшеліктерінің бірі олардың қолжетімділігі мен көрнекілігі. Қарапайым алгоритмдерге негізделген мұндай есептер оқушылардың пәнге деген қызығушылығын арттырып, оларды күрделірек тапсырмаларды меңгеруге біртіндеп дайындайды. Нәтижесінде білім алушылар криптография элементтерін тек теориялық тұрғыда ғана емес, практикалық деңгейде де саналы түрде игере бастайды.

Жоғарыда баяндалғандарды нақтылау мақсатында білім алушыларға қарапайым шифрлау әдістерін қолдануға негізделген келесі есеп ұсынылады.

Мысал 1.

Полибий квадраты (5×5, ағылшын алфавиті, I және J бір ұяшықта):

Кесте 1 – Полибий квадраты (5×5)

№	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

«DATA» сөзін латын квадраты (Полибий квадраты) арқылы шифрлайық. Әр әріптің кестедегі орнын табамыз:

D әріпі бірінші жолдың төртінші бағанында орналасқан, сондықтан ол 14 деп белгіленеді. A әріпі бірінші жол мен бірінші бағанның қиылысында тұр — 11.

T әріпі төртінші жолдың төртінші бағанында — 44.

Соңғы A әріпі қайтадан 11 болады.

Осылайша, шифрланған түрі: 14 11 44 11.

Жауабы да сол: 14 11 44 11.

Бұл тапсырма қарапайым көрінгенімен, бірнеше маңызды дағдыны қалыптастырады. Оқушылар кестемен жұмыс істейді, жол мен бағанды шатастырмай анықтауға үйренеді. Сонымен қатар, әріптерді сандарға айналдыру арқылы ақпаратты кодтаудың қалай жүретінін түсінеді. Ең бастысы әрекеттерді ретімен орындауға дағдыланады.

Осындай қарапайым тапсырмалар кейінгі, күрделірек есептерге жақсы негіз болады. Алдымен оқушылар ақпаратты координаталар арқылы кодтауды меңгереді. Кейін біртіндеп екілік форматқа өтеді.

Бұл өте маңызды кезең болып табылады, себебі қазіргі ақпараттық жүйелерде барлық мәліметтер екілік — 0 және 1 — форматта ұсынылады.

Сол себепті келесі қадамда криптографияда жиі қолданылатын XOR операциясымен таныстыру орынды болады. Бұл операция хабарламаның әрбір битін кілттің сәйкес битімен салыстыру арқылы жұмыс істейді және ағынды шифрларда кеңінен қолданылады.

Полибий квадраты арқылы әріптерді санға айналдыру оқушыларды дәл осы екілік әрекеттерді түсінуге дайындайтын алғашқы қадамдардың бірі.

Мысал 2.

Берілген 6-биттік хабарлама: M = 101101.

Кілт: K = 110011.

Осы кілт арқылы хабарламаны шифрлау керек.

Шешуі:

XOR операциясы екілік қосуға ұқсас амал, яғни mod 2 бойынша қосу. Қарапайым тілмен айтқанда, екі битті салыстырамыз: егер екеуі бірдей болса нәтиже 0, ал әртүрлі болса 1 шығады.

Мысалы:

$0 \oplus 0 = 0$

$1 \oplus 1 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

Енді хабарлама мен кілттің биттерін бір-бірімен кезекпен қосайық:

1-бит: $1 \oplus 1 = 0$

2-бит: $0 \oplus 1 = 1$

3-бит: $1 \oplus 1 = 0$

4-бит: $1 \oplus 1 = 0$

5-бит: $0 \oplus 1 = 1$

6-бит: $1 \oplus 1 = 0$

Нәтижесінде шифрланған хабарлама: 011110.

Бұл есепті орындау кезінде оқушылар екілік сандармен жұмыс істеуді үйренеді. Сонымен қатар, логикалық амалдардың қалай жұмыс істейтінін өздері көріп түсінеді. Әр қадамды ретімен орындау арқылы алгоритмдік ойлау да біртіндеп қалыптасады.

Мұндай тапсырмалар бастапқыда жеңіл көрінуі мүмкін, бірақ олар кейінгі күрделі тақырыптарға жақсы дайындық болады. Мысалы, теңдеулер жүйесіне келтіру немесе Гаусс әдісін қолдану сияқты бөлімдерге өту әлдеқайда жеңілдейді.

Криптографиядағы есептер тек осындай қарапайым амалдармен шектелмейді. Көп жағдайда олар күрделі алгебралық өрнектер түрінде беріледі; мұндай есептерді тікелей шешу едәуір күрделілік тудырады.

Осыған байланысты аталған есептерді сызықтық теңдеулер жүйесіне келтіру тәсілі қолданылады: күрделі өрнектер жаңа айнымалылар арқылы ауыстырылып, есеп қарапайым сызықтық жүйеге түрленеді.

Бұл тәсілдің мәні мынада: сызықтық емес мүшелер (мысалы, айнымалылардың көбейтіндісі) жаңа айнымалылармен ауыстырылады, соның нәтижесінде бастапқы есеп сызықтық теңдеулер жүйесіне айналады. Алынған сызықтық жүйені классикалық Гаусс әдісі арқылы тиімді шешуге болады.

Мысал 3.

Келесі криптографиялық өрнекті қарастырайық:

$x_1x_2 \oplus x_2x_3 \oplus x_1 = 1$

Бұл жерде x_1x_2 және x_2x_3 - сызықтық емес мүшелер. Осындай өрнектермен жұмыс істеу бірден оңай емес, сондықтан оны қарапайымдау тәсілін қолданамыз.

Ол үшін жаңа айнымалылар енгіземіз: $u_1 = x_1x_2$, $u_2 = x_2x_3$.

Сонда бастапқы өрнек былай жазылады:

$u_1 \oplus u_2 \oplus u_3 = 1$

Екілік өрісте бұл:

$u_1 + u_2 + u_3 = 1 \pmod 2$

Яғни, күрделі көрінген өрнек енді қарапайым сызықтық теңдеуге айналды.

Көрсетілген тәсіл оқушыларға жақсы көмектеседі. Олар есепті бөліктерге бөлуді үйренеді, қажет жерде жаңа айнымалы енгізеді. Біртіндеп есептің құрылымын түсіне бастайды.

Сызықтық теңдеулер жүйесін шешуде жиі қолданылатын тиімді тәсілдердің бірі - Гаусс әдісі. Бұл әдіс теңдеулер жүйесін біртіндеп түрлендіру арқылы белгісіз айнымалыларды табуға мүмкіндік береді. Яғни, бастапқы жүйе қарапайым әрі есептеуге қолайлы түрге келтіріледі.

Гаусс әдісін қолданғанда матрицамен жұмыс жүргізіледі. Осы үдерісте бірнеше негізгі түрлендірулер орындалады: жолдардың орнын ауыстыру, жолды нөлден өзге санға көбейту немесе бөлу, сондай-ақ бір жолға екінші жолды қосу немесе азайту. Осындай амалдардың нәтижесінде жүйе ықшам әрі түсінікті түрге келеді.

Шешу барысы екі негізгі кезеңге бөлінеді. Алдымен тура жүріс орындалады: матрица сатылы түрге келтіріліп, негізгі диагональдың астындағы элементтер нөлге айналады. Одан кейін кері жүріс жүзеге асырылады - соңғы теңдеуден бастап айнымалылардың мәндері біртіндеп анықталады.

Мысал 4.

Үш компоненттен тұратын құпия кілтті (x, y, z) табу үшін келесі теңдеулер жүйесін қарастырайық:

$$\begin{cases} x + y + z = 6 \\ 2x - y + z = 3 \\ x + 2y - z = 2 \end{cases}$$

Алдымен жүйені кеңейтілген матрица түрінде жазамыз:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 6 \\ 2 & -1 & 1 & 3 \\ 1 & 2 & -1 & 2 \end{array}\right)$$

Енді біртіндеп түрлендіреміз.

Екінші жолдан бірінші жолдың екі есесін аламыз:

$R_2 = R_2 - 2R_1$

Нәтижесінде: $\left(\begin{array}{ccc|c} 0 & -3 & -1 & -9 \end{array}\right)$

Үшінші жолдан бірінші жолды азайтамыз:

$R_3 = R_3 - 2R_1$

Аламыз: $\left(\begin{array}{ccc|c} 0 & 1 & -2 & -4 \end{array}\right)$

Осыдан кейін матрица келесі түрде болады:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 6 \\ 0 & -3 & -1 & -9 \\ 0 & 1 & -2 & -4 \end{array}\right)$$

Есептеуді жеңілдету үшін екінші және үшінші жолдардың орнын ауыстырамыз:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 6 \\ 0 & 1 & -2 & -4 \\ 0 & -3 & -1 & -9 \end{array}\right)$$

Келесі қадамда үшінші жолдағы екінші бағанды нөлге келтіреміз. Ол үшін:

$R_3 = R_3 + 3R_2$

Сәйкесінше: $\left(0 \quad 0 \quad -7 \middle| -21\right)$

Матрица сатылы түрге келеді:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 6 \\ 0 & 1 & -2 & -4 \\ 0 & 0 & -7 & -21 \end{array}\right)$$

Енді кері бағытта шешеміз.

Соңғы теңдеуден:

$-7z = -21, z = 3$

Оны екінші теңдеуге қоямыз:

$y - 2\square 3 = -4, y = 2$

Соңында бірінші теңдеу:

$x + 2 + 3 = 6, x = 1$

Жауабы: $(x, y, z) = (1, 2, 3)$

Бұл мысалда жүйені бірден шешпей, оны ретімен жеңілдету тиімді екені көрінеді. Алдымен түрлендіріп аламыз, содан кейін ғана айнымалыларды табамыз.

Осындай тәсіл оқушыларға есепті кезең-кезеңімен қарастыруға көмектеседі. Сонымен бірге, олар модель құру, логикалық талдау жасау және алгоритм бойынша жұмыс істеу дағдыларын біртіндеп меңгереді.

Бұл бөлім алдыңғы қарастырылған тақырыптармен де байланысты. Мысалы, шифрлау немесе XOR амалдары арқылы алынған өрнектерді кейін осындай теңдеулер жүйесіне келтіруге болады. Соның арқасында білім алушылар криптографияны бөлек-бөлек емес, өзара байланысқан жүйе ретінде қабылдай бастайды.

НӘТИЖЕЛЕР ЖӘНЕ ОЛАРДЫ ТАЛҚЫЛАУ

Педагогикалық эксперимент барысында білім алушылардың оқу көрсеткіштерінде оң өзгерістер байқалды. Экспериментке дейінгі бастапқы нәтижелер мен кейінгі қорытынды деректер өзара салыстырылып, талданды.

Алынған мәліметтер негізінде білім алушылардың деңгейі үш санат бойынша қарастырылды: төмен, орта және жоғары. Әр деңгейдің үлесі пайыздық көрсеткіштер арқылы анықталып, нәтижелер жүйелі түрде көрсетілді.

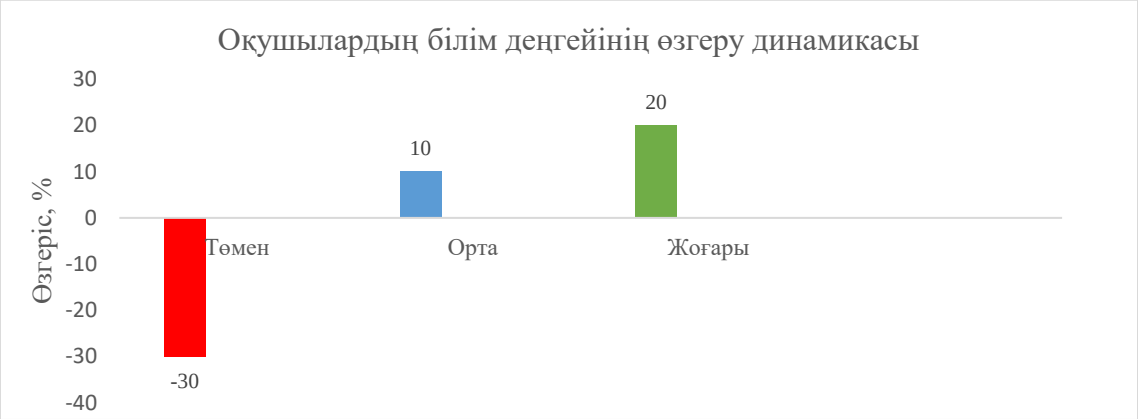
Кесте 2 – Оқушылардың білім деңгейінің өзгеруі

Деңгей	**Экспериментке дейін (%)**	**Эксперименттен кейін (%)**
Төмен	45%	15%
Орта	40%	50%
Жоғары	15%	35%

Кесте 2 мәліметтеріне назар аударсақ, эксперименттен кейін білім алушылардың оқу нәтижелерінде оң өзгерістер байқалады. Әсіресе деңгейлер бойынша айырмашылық анық

көрінеді: төмен деңгейдегі оқушылардың үлесі 45%-дан 15%-ға дейін қысқарған. Ал жоғары деңгейге жеткен оқушылар саны, керісінше, 15%-дан 35%-ға дейін өскен.

Бұл көрсеткіштер қолданылған әдістеменің нәтижелі болғанын аңғартады. Сонымен бірге, білім алушылардың математикалық дайындығының жақсарғанын байқауға болады.



Сурет 1 – Оқушылардың білім деңгейінің өзгеру динамикасы

Диаграммаға қарасақ, білім алушылардың оқу нәтижелеріндегі өзгерістер анық көрінеді. Эксперимент барысында төмен деңгейдегі оқушылар саны едәуір азайып, шамамен 30%-ға қысқарған. Бұл олардың бастапқы қиындықтарды біртіндеп жеңіп, оқу материалын жақсырақ меңгере бастағанын аңғартады.

Орта деңгейдегі көрсеткіш те өзгеріссіз қалмаған, бұл топтағы оқушылардың үлесі 10%-ға артқан. Мұны негізгі ұғымдарды түсіну деңгейінің тұрақтана бастағанымен түсіндіруге болады.

Ең айқын өзгеріс жоғары деңгейде байқалады. Бұл санаттағы оқушылар саны 20%-ға өскен, яғни олардың бір бөлігі есептерді өз бетінше талдап, математикалық модельдерді қолдана алатын деңгейге жеткен.

Жалпы алынған нәтижелер криптография элементтеріне негізделген элективті курстың пайдалы болғанын көрсетеді. Сонымен қатар, ұсынылған әдістеменің оқушылардың танымдық белсенділігіне және алгоритмдік ойлауына оң әсер еткенін байқауға болады. Алынған нәтижелердің статистикалық сенімділігін дәлелдеу мақсатында Стьюдент t-критерийі қолданылды. Эксперимент алдындағы орташа ұпай: $M_1 = 5{,}1$ ($SD_1 = 1{,}8$), ал эксперименттен кейінгі орташа ұпай: $M_2 = 7{,}4$ ($SD_2 = 1{,}5$). Есептелген t-мәні: $t = 4{,}23$, бостандық дәрежесі $df = 21$, маңыздылық деңгейі $p < 0{,}01$. Бұл нәтиже оқу көрсеткіштерінің өсуі кездейсоқ емес, статистикалық тұрғыдан мәнді екенін растайды.

Талқылау. Алынған нәтижелер криптография элементтерін қолдана отырып ұйымдастырылған оқытудың тиімді болғанын көрсетеді. Эксперимент барысында байқалған өзгерістер ұсынылған дидактикалық модельдің педагогикалық тұрғыдан негізді құрылғанын аңғартады.

Төмен деңгейдегі оқушылар санының азаюы ерекше назар аудартады. Бұл білім алушылардың бастапқы қиындықтарды біртіндеп еңсеріп, оқу материалын жақсырақ түсіне бастағанын білдіреді. Мұндай өзгерісті криптографиялық тапсырмалардың практикалық сипатымен түсіндіруге болады. Абстрактілі ұғымдар нақты мысалдар арқылы берілген кезде оларды қабылдау жеңілдей түседі.

Орта және жоғары деңгейдегі көрсеткіштердің өсуі де маңызды нәтиже болып табылады. Бұл білім алушылардың логикалық және алгоритмдік ойлауының дамығанын көрсетеді. Әсіресе, криптографиялық өрнектерді теңдеулер жүйесіне келтіру және оларды шешу кезеңдері олардың модель құру дағдыларына оң әсер еткенін байқауға болады.

Тапсырмалардың біртіндеп күрделенуі де өз нәтижесін берді. Алдымен қарапайым шифрлау, кейін XOR операциялары, одан соң алгебралық модельдерге көшу — осындай ретпен жұмыс істеу білімді жүйелі меңгеруге көмектесті. Бұл тәсіл оқу барысында шамадан тыс қиындықтың алдын алып, материалды біртіндеп игеруге мүмкіндік берді.

ҚОРЫТЫНДЫ

Жүргізілген зерттеу криптография элементтерін пайдалану арқылы Гаусс әдісін оқытудың тиімді тәсілін құруға мүмкіндік бергенін көрсетті. Ұсынылған дидактикалық модель білім алушылардың сызықтық теңдеулер жүйесін түсінуін жақсартып, оларды алгоритм негізінде шешуге дағдыландырады.

Эксперимент нәтижелері оқу көрсеткіштеріндегі өзгерістерді айқын байқатты. Төмен деңгейдегі оқушылар саны азайып, ал жоғары деңгейге жеткендердің үлесі артты. Мұны қолданылған әдістеменің нәтижелі болғанымен байланыстыруға болады. Криптография элементтері арқылы берілген тапсырмалар математикалық ұғымдарды нақты әрі түсінікті түрде қабылдауға көмектесті.

Зерттеу барысында қолданылған тапсырмалар бірден күрделенбей, біртіндеп енгізілді. Осындай тәсіл оқушылардың қызығушылығын сақтап, олардың ойлау белсенділігін арттырды. Әсіресе, өрнектерді теңдеулер жүйесіне келтіру және оларды Гаусс әдісімен шешу кезеңдері математикалық модельдеуді түсінуге ықпал етті.

Ұсынылған әдістеменің практикалық жағы да маңызды. Оны мектеп курсында элективті пән ретінде қолдануға болады, сондай-ақ басқа пәндермен байланыстыра оқытуға мүмкіндік бар. Соның нәтижесінде математиканы оқыту мазмұны қазіргі талаптарға жақындай түседі және білім алушылардың заманауи дағдыларын дамытуға жағдай жасалады.

Зерттеудің шектеулері. Жүргізілген зерттеу бірқатар шектеулер аясында орындалғанын атап өту қажет. Біріншіден, тәжірибелік жұмысқа 22 оқушы ғана қатысты, бұл іріктеменің шағын екенін білдіреді. Екіншіден, зерттеуде бақылаушы топ (контрольная группа) қолданылмады, бұл нәтижелердің тек ұсынылған әдістеменің ықпалымен байланыстылығын толық дәлелдеуді қиындатады. Алынған нәтижелерді жалпылауды тереңдету үшін болашақта кеңірек іріктememен және бақылаушы топпен бірге жүргізілетін зерттеу жүргізу ұсынылады. Сондай-ақ, ұзақ мерзімді оқыту нәтижелерін бақылау (longitudinal study) ұсынылған дидактикалық модельдің тұрақты тиімділігін растауға мүмкіндік берер еді.

МҮДДЕЛЕР ҚАЙШЫЛЫҒЫ: Автор(лар) мүдделер қайшылығы жоқ екенін мәлімдейді.

ДЕРЕКТЕРДІҢ ҚОЛЖЕТІМДІЛІГІ: Зерттеуде қолданылған деректер авторларға жазбаша сұраным жолдау арқылы қолжетімді болады.

АЛҒЫС: Авторлар тәжірибелік жұмысты жүргізуге мүмкіндік берген Семей қаласындағы №45 жалпы орта білім беретін мектептің директоры мен математика мұғалімдеріне, зерттеуге белсене қатысқан 9-сынып оқушыларына шын жүректен алғыс білдіреді.

ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫ ТУРАЛЫ ХАБАРЛАМА: Мақаланы дайындау барысында жасанды интеллект технологиялары қолданылған жоқ.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

Токарева Н.Н. Симметричная криптография. – Новосибирск: НГТУ, 2012. – 312 с. ISBN 978-5-7782-1887-6

Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Cryptography and Coding: Lecture Notes in Computer Science. – Berlin: Springer, 2007. – Vol. 4887. – P. 152–169. https://doi.org/10.1007/978-3-540-77272-9_10

Calderini M. On Boolean functions, symmetric cryptography and algebraic coding theory: PhD Thesis. – Trento: University of Trento, 2015. – 147 p. URL: http://eprintsphd.biblio.unitn.it/1501/

Ishchukova E., Maro E., Pristalov P. Algebraic Analysis of a Simplified Encryption Algorithm GOST R 34.12-2015 // Computation. – 2020. – Vol. 8, № 2. – Article 51. https://doi.org/10.3390/computation8020051

Horáček J. Algebraic and Logic Solving Methods for Cryptanalysis: Dissertation. – Passau: University of Passau, 2019. – 162 p. URL: https://opus4.kobv.de/opus4-uni passau/frontdoor/index/index/docId/679

Ünal A. Cryptanalysis by Algebraic Relations: Doctoral Thesis. – Zurich: ETH Zurich, 2024. – 249 p. https://doi.org/10.3929/ethz-b-000679381

Dewi I.L.K., Zaenuri, Dwijanto, Mulyono. Identification of mathematics prospective teachers' conceptual understanding in determining solutions of linear equation systems // European Journal of Educational Research. – 2021. – Vol. 10, № 3. – P. 1157–1170. https://doi.org/10.12973/eu-jer.10.3.1157

Arifin S. The Use of Matrix Theory in Data Encryption: A Literature Review and Its Implications for Mathematics Education in the Digital Era // Journal of Data Science and Education. – 2025. – P. 1–11. https://doi.org/10.56452/jdse.v3i1.119

Попов Н.И., Яковлева Е.В. Использование метода схематизации при обучении студентов и школьников математике // Вестник Сыктывкарского университета. – 2020. – № 4 (37). – С. 74–85. URL: https://cyberleninka.ru/article/n/ispolzovanie-metoda- shematizatsii-pri-obuchenii-studentov-i-shkolnikov-matematik

Krishnan S., Eng F.K. Creative Teaching in Mathematics: An Example in Linear Algebra // International Journal of Academic Research in Progressive Education and Development. – 2024. – Vol. 13, № 3. – P. 726–737. https://doi.org/10.6007/IJARPED/v13-i3/22494

Ünal A. Algebraic relations in cryptanalysis and their applications // ETH Zurich Research Collection [Электронный ресурс]. – 2024. – URL: https://doi.org/10.3929/ethz-b- 000679381 (дата обращения: 21.02.2026).

Meidl W., Niederreiter H. Introduction to Finite Fields and Their Applications in Cryptography // Finite Fields and Their Applications. – Cambridge: Cambridge University Press, 2021. – 432 p. ISBN 978-1-108-49371-6

Mullen G.L., Panario D. Handbook of Finite Fields. – Boca Raton: CRC Press, 2013. – 1068 p. ISBN 978-1-4398-7378-6

Даулетбаева Д.А., Байсалова Г.Т. Математика сабақтарында STEM-тәсілін пайдалану мүмкіндіктері // ҚазҰПУ Хабаршысы. Педагогика сериясы. – 2022. – № 3 (75). – Б. 105–114. [Dauletbayeva D.A., Baisalova G.T. Vozmozhnosti ispol'zovaniya STEM-podkhoda na urokakh matematiki [Possibilities of Using STEM Approach in Mathematics Lessons] // Vestnik KazNPU. Seriya pedagogika [KazNPU Bulletin. Pedagogy Series]. – 2022. – No. 3 (75). – P. 105–114. In Kazakh]

Jupri A., Drijvers P., van den Heuvel-Panhuizen M. Difficulties in initial algebra learning in Indonesia // Mathematics Education Research Journal. – 2014. – Vol. 26, № 4. – P. 683–710. https://doi.org/10.1007/s13394-013-0097-0

Авторлар туралы мәліметтер
Информация об авторах
Information about authors

Сағынтаева Бақытжан Бауыржанқызы – магистрант 2 курс, "Шәкәрім университеті" КеАҚ , Семей, Қазақстан
Сагынтаева Бакытжан Бауыржановна – магистрант 2 курс, "Университет Шакарим" НАО, г. Семей, Казахстан
Sagyntayeva Bakytzhan Bauyrzhanovna – 2nd-year Master's student, "Shakarim University" JSC, Semey, Kazakhstan,
e-mail: kbskyt@mail.ru,
ORCID: https://orcid.org/0009-0003-8618-7004,

Мархабатов Нурлан Дарханұлы – ф.-м.ғ.к. , PhD докторы, "Л.Н. Гумилев атындағы евразия ұлттық университеті" КеАҚ , Астана, Қазақстан
Мархабатов Нурлан Дарханович – к.ф.-м.н., доктор PhD, JSC "Евразийский национальный университет имени Л.Н. Гумилева" НАО, Астана, Казахстан
Markhabatov Nurlan Darkhanovich – cand. Sci. (phys.-math.), doctor PhD, JSC "L.N. Gumilyov Eurasian National University", Astana, Kazakhstan
e-mail: *Nur_24.08.93@mail.ru*,
ORCID: https://orcid.org/0000-0002-5088-0208