Вып. 70 Методические и практические проблемы надежности систем энергетики. В 2хКнигах. / Книга2 / Отв. ред. Н.И. Воропай – ИСЭМ СО РАН, 2019 г.- С.361-366.

9. Akhmetbaev D.S., Dzhandigulov A.R. Development of algorithms for a new topological method for calculating current distribution coefficients in complex electrical networks//Eurasian journal of mathematical and computer applications. ISSN 2306–6172,Volume 7, Issue 3 (2019) 4 – 12

КРИПТОГРАФИЯНЫҢ МАТЕМАТИКАЛЫҚ НЕГІЗДЕРІ

Жетпісов Қ., Мусабеков А.К.

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан

E-mail: zhetpissov_k@enu.kzmussabekov_ak_1@enu.kz

Криптографиялық алгоритмдер және шифрлау теориясы пәнін оқып игеруде ақырлы өрістер теориясын меңгеру өте маңызды.

Шифрлау платформасындағы әріптерді цифрлаудан бастап, мәтінді шифрлауда, ақпаратты сақтауда, өңдеуде, таратуда және оны компьютерлік тілге ауыстыруда (кодтауда) толығымен осы ақырлы өрістердің негізгі ұғымдары мен тұжырымдары қолданылады.

Қазіргі заманауи шифрлау платформаларындағы ақпаратты тарату процессін оқып-үйренуде үлкен құрама n – санын таңдаудың ерекшелігіне тоқталғымыз келеді. Класикалық шифрлау алгоритмдерінде (Эль-Гамаль, Шамир, RSA, DES) осы үлкен санды таңдаудағы ерекшелікке көңіл аударған жөн.

Егер n – құрама сан болса, онда Z_n – айырмалар сақинасының өріс болмайтыны түсінікті. Ашық кілтті криптожүйелерде абоненттің құпия кілтін таңдауда осы санның жай көбейткіштерін таңдайтындығы белгілі, яғни, $n = p \cdot q$ және p, q әртүрлі жай сандар болса, онда p – бірінші абоненттің құпия кілті, q – екінші абоненттің құпия кілті болады. Z_p және Z_q сақиналары өріс болғандықтан ақпаратты жолдау және қабылдау (жауап жазу) бірмәнді анықталатындығы түсінікті. Алгоритмдердегі осы n, p, q – сандарының қалай сәйкестендірілетіндігін студенттерге түсіндіру өте маңызды. Шын мәнісінде, Z_n сақинасы Z_p және Z_q сақиналарының декарттық көбейтіндісі болатын $Z_p \times Z_q$ сақинасымен ауыстырылады.

Онда $Z_p \times Z_q$ сақинасы шифрлау процесінде қалай жұмыс істейді?

Z_n және $Z_p \times Z_q$ изоморфты сақиналар. n – құрама сан болғандықтан Z_n сақинасында нөлдің бөлгіштерінің кері элементтері жоқ. Яғни, бұл ақпараттың дұрыс және толық жолдануына және қабылдануына кедергі жасайды. Егер Z_n сақинасын $Z_p \times Z_q$ сақинасымен ауыстырсақ, онда нөлдің бөлгіштерін «айналып өтуге» болады.

Ол үшін ақпарат жолдаушы (1 – абонент) Z_p – өрісінде барлық ақпаратты жолдайды. Ақпаратты қабылдаушы (2 – абонент) оны p – лық санау жүйесінен q – лік санау жүйесіне ауыстырып оқиды. Екінші абонент (қабылдаушы) Z_q – өрісінде өз ақпаратын жолдайды. Ал, бірінші абонент бұл ақпаратты q – лік санау жүйесінен p – лық санау жүйесіне ауыстырып оқиды. $Z_p \times Z_q$ сақинасының әрбір элементінің бірінші компонентін бірінші абонент қолданса, екінші компонентін екінші абонент қолданады.

Үлкен n – саны бірнеше жай сандарға жіктелсе, сонша абонент құпия ақпараттармен алмаса алады.

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ болса, онда

$$Z_n \cong Z_{p_1} \times Z_{p_2} \times \ldots \times Z_{p_k}$$

Шифрлау алгоритміндегі осындай түрлендірулердің орындалатынын жақсы түсіне білу әріректе кодтау теориясы пәнін оқып-үйренуде көп септігін тигізеді.

Кодтау – ақпаратты екілік санау жүйесіне ауыстыру болып табылады.

Бұл процестегі негізгі сұрақтар түзелетін және түзелмейтін қателерге қатысты туындайды. Атап айтқанда, «синдромдар» көпшілік жағдайда жоғарыда айтылған шифрлау

алгоритмдеріндегі санау жүйесіне көшу кезеңдеріндегі әртүрлі қателердің нәтижесінде пайда болады.

Сондықтан криптографиялық алгоритмдер және шифрлау теориясы пәні мен кодтау теориясы пәндерінің арасындағы сабақтастықты ұштастыруда студенттерге ақырлы өрістердің негізгі қасиеттерін және оларды қолданудағы сақинадан ақырлы өріске өту жолдарын нақты айқындап, оларды тәжірибелік мысалдармен толықтыра отыра оқып-үйрену өте маңызды.

Қолданылған әдебиеттер тізімі

1. Қ. Жетпісов., Ж.А. Түсіпов., Т.Т. Оспанова., Н.Д. Мархабатов. Криптографияның математикалық негіздері. Оқу құралы. – Астана: СКАМАДИ баспасы, 2018. – 143 бет.

2. Қ. Жетпісов., Б.Н. Рахымжанов., А.О. Башеева., А.К. Мусабеков. Дискретті математика пәнінен лабораториялық жұмыстар практикумы. Оқу – әдістемелік құрал. – Нұр-Сұлтан: «Печатный мир» баспасы, 2021. – 104 бет.

ЭКОЛОГИЯЛЫҚ ҮДЕРІСТЕРДІ МОДЕЛЬДЕУ МЕН ТАЛДАУДЫҢ НЕГІЗГІ ӘДІСТЕРІ

Кервенев Қ.Е., Естаев Д.Е., Жанузакова Д.Б.

Академик Е.А.Бөкетов атындағы Қарағанды университеті, Қарағанды, Қазақстан;
Ә.Бөкейханов атындағы №1 гимназия, Тараз, Қазақстан;
Ө.Жолдасбеков атындағы №50 орта мектеп, Тараз, Қазақстан
E-mail: kervenev@bk.ru, d.estaev3092@list.ru

Модельдеу-әртүрлі оқу пәндерінен білімді біріктіруге мүмкіндік беретін тиімді құрал. Жалпы модельдеу және компьютерлік модельдеу маңызды гуманистік функцияны орындай алады, өйткені белгілі бір антропогендік факторлардың салдарын болжау мүмкіндігі тіпті жаһандық масштабта (планетаның климатының өзгеруі, ядролық қыс және т.б.) қауіпті және жағымсыз құбылыстарды болдырмауға мүмкіндік береді. Демек, ол қазіргі қоғамдағы саяси ойлаудың мазмұны мен стилін қалыптастыра алады. Зерттеу мақсатына байланысты кез-келген объект үшін көптеген түрлі модельдер жасалуы мүмкін. Мысалы, егер біз жануарлардың популяциясы сияқты күрделі жүйені алсақ, онда тіршілік процестерін сипаттау үшін биологиялық объект ретінде жеке жануарлардың моделі қолданылады, зерттеуші жануарлар тобының тіршілігін модельдеу үшін басқа, этологиялық (тіршілік) модельді қолданады, ал жеке адамдар санының өзгеру динамикасын болжау үшін мүлдем басқа экологиялық модель жасалады. Содан кейін бір модельді құру кезінде маңызды объектінің қасиеттері басқасына мүлдем елеусіз болуы мүмкін. Зерттеушінің мақсаты-орта деңгей табу: процестің моделін оны негізгі белгілерінен айырмай жасау.

Жеке популяциялар мен олардың қауымдастықтарының санының динамикасын сипаттаудың алғашқы әрекеттері 18 ғасырға жатады. Қазіргі математикалық экология біздің ғасырдың 20 - жылдарында пайда болды-дәл осы кезде математика әдістері мен модельдеу идеялары биологияға ене бастады. Математикалық экология-бұл тиісті математикалық модельдерді зерттеу негізінде өсімдіктер мен жануарлар организмдерінің және олар құрған қауымдастықтардың өздері мен қоршаған орта арасындағы байланысы туралы ғылым. Қазіргі экологияның алдында көптеген проблемалар бар, бірақ олардың негізгілері, біздің ойымызша, мыналар: - антропогендік факторлардың әсерінен экожүйенің жай-күйін болжау; - әр түрлі қалпына келтірілетін табиғи ресурстарды пайдаланудың оңтайлы стратегиясын таңдау; - дақылдарды зиянкестермен күресу үшін популяциялар мен олардың қауымдастықтарын басқару пестицидтерді қолдану арқылы емес, олармен байланысты құралдармен зиянкестердің табиғи жауларын қолдану.Біз экологиядағы математикалық модельдеудің бірнеше мысалын қарастырамыз, олардың көмегімен біз осы ғылымның ерекшеліктерінен туындайтын жаңа тәсілдер мен идеялармен танысамыз. Сонымен қатар,