KRIPTOGRAFIYA FANINI O‘QITISHNING NAZARIY-METODIK ASOSLARI

Choriyev Behruz Shuxrat o‘g‘li
Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti

Annotatsiya. Ushbu maqolada kriptografiya fanini o‘qitishning nazariy-metodik asoslari, axborot xavfsizligi bilan bog‘liq didaktik tamoyillar, psevdotasodifiy sonlar generatorlari hamda oqimli shifrlar mavzusining o‘quv dasturidagi o‘rni tahlil qilinadi. Kriptografiya fani matematik nazariya, algoritmik fikrlash, dasturiy tajriba va xavfsizlik madaniyatini birlashtiruvchi murakkab fan sifatida qaraladi. Maqolada mavzuni raqamli ta’lim texnologiyalari, virtual laboratoriya, simulyatsiya, interaktiv kodlash muhiti va avtomatlashtirilgan baholash vositalari yordamida o‘qitish imkoniyatlari yoritiladi. Shuningdek, talabalar tomonidan tasodifiylik, kalit oqimi, shifrlash jarayoni, sinxronlashuv, statistik testlar va kriptografik barqarorlik tushunchalarini o‘zlashtirishda uchraydigan muammolar hamda ularni bartaraf etish yo‘llari taklif etiladi.

Kalit so‘zlar: kriptografiya, axborot xavfsizligi, psevdotasodifiy sonlar generatori, oqimli shifr, raqamli ta’lim, algoritmik tafakkur, virtual laboratoriya, didaktik tamoyil.

ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВЫ ПРЕПОДАВАНИЯ КРИПТОГРАФИИ

Чориев Бехруз Шухрат угли
Национальный университет Узбекистана имени Мирзо Улугбека

Аннотация. В статье рассматриваются теоретико-методические основы преподавания криптографии, дидактические принципы изучения информационной безопасности, а также место тем псевдослучайных генераторов и потоковых шифров в учебной программе. Криптография представлена как интегративная дисциплина, объединяющая математическую теорию, алгоритмическое мышление, программную практику и культуру безопасной работы с информацией. Особое внимание уделяется возможностям цифровых образовательных технологий, виртуальных лабораторий, интерактивных симуляций и автоматизированной оценки. В работе также определены методические трудности усвоения понятий случайности, ключевого потока, синхронизации и криптографической стойкости, предложены пути их преодоления.

Ключевые слова: криптография, информационная безопасность, псевдослучайный генератор, потоковый шифр, цифровое обучение, алгоритмическое мышление, виртуальная лаборатория, дидактический принцип.

THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF TEACHING CRYPTOGRAPHY

Choriyev Behruz Shuxrat ogli
Mirzo Ulugbek National University of Uzbekistan

Abstract. This article examines the theoretical and methodological foundations of teaching cryptography, the didactic principles of information security education, and the role of pseudorandom number generators and stream ciphers in the curriculum. Cryptography is considered as an integrative discipline that combines mathematical theory, algorithmic reasoning, programming practice and information security culture. The paper discusses the possibilities of teaching cryptographic algorithms through digital educational technologies, virtual laboratories,

simulations, interactive coding environments and automated assessment tools. It also identifies common learning difficulties related to randomness, keystream generation, synchronization, statistical testing and cryptographic strength, and proposes methodological ways to overcome them.

Keywords: cryptography, information security, pseudorandom number generator, stream cipher, digital education, algorithmic thinking, virtual laboratory, didactic principle.

Kirish (Introduction). Raqamli jamiyat sharoitida axborot resurslari, elektron hujjatlar, bulutli xizmatlar, mobil ilovalar, masofaviy ta’lim platformalari va elektron to‘lov tizimlari kundalik faoliyatning ajralmas qismiga aylandi. Bunday muhitda ma’lumotlarning maxfiyligi, yaxlitligi, autentikligi va rad etib bo‘lmasligini ta’minlash axborot xavfsizligining asosiy vazifalaridan biri hisoblanadi. Kriptografiya aynan shu vazifalarni ilmiy asosda hal qiluvchi fan bo‘lib, u nafaqat texnik algoritmlar majmuasi, balki xavfsiz fikrlash, matematik isbot, dasturiy amalga oshirish va mas’uliyatli foydalanish madaniyatini ham shakllantiradi.

Oliy ta’limda kriptografiya fanini o‘qitishning dolzarbligi kiberxavfsizlik, dasturiy injiniring, kompyuter injiniringi va axborot texnologiyalari yo‘nalishlari uchun kasbiy kompetensiyalar bilan bevosita bog‘liq. Talaba simmetrik va assimetrik shifrlash, xesh funksiyalar, elektron raqamli imzo, kalitlarni boshqarish, protokollar xavfsizligi, psevdotasodifiy sonlar generatorlari va oqimli shifrlar kabi tushunchalarni nazariy bilishi bilan birga, ularni dasturiy muhitda modellashtira olishi ham zarur. Chunki amaliy tizimlarda kriptografik xato ko‘pincha algoritm nomini bilmaslikdan emas, balki kalit, nonce, initsializatsiya vektori, tasodifiylik manbasi yoki protokol kontekstini noto‘g‘ri qo‘llashdan kelib chiqadi.

Kriptografiya fanining metodik murakkabligi uning abstrakt matematik apparati, algoritmik bosqichlari va xavfsizlik talablari bir vaqtning o‘zida o‘zlashtirilishini talab qilishi bilan izohlanadi. Masalan, talaba oqimli shifrni tushunishi uchun modulli arifmetika, bitlar ustida amallar, XOR operatsiyasi, kalit oqimi, sinxronlashuv, tasodifiylik va statistik farqlanmaslik kabi tushunchalarni bog‘lay olishi kerak. Shu bois mazkur mavzuni o‘qitishda faqat ma’ruza matni yoki tayyor formulalarni berish yetarli emas; vizual model, algoritmik jadval, bosqichma-bosqich kodlash, testlash va muammoli vaziyatlar asosida o‘qitish zarur.

Ushbu maqolaning maqsadi kriptografiya fanini o‘qitishning nazariy-metodik asoslarini yoritish, psevdotasodifiy sonlar generatorlari va oqimli shifrlar mavzusining o‘quv dasturidagi o‘rnini aniqlash, raqamli ta’lim texnologiyalari yordamida kriptografik algoritmlarni o‘qitish imkoniyatlarini ko‘rsatish hamda mavjud pedagogik muammolarga metodik yechimlar taklif qilishdan iborat.

Tadqiqot metodologiyasi (Research Methodology).

Maqolani tayyorlashda nazariy tahlil, qiyosiy-pedagogik tahlil, didaktik modellashtirish, mavzu mazmunini kompetensiyaviy yondashuv asosida tizimlashtirish hamda kriptografik algoritmlarni o‘qitish jarayonini raqamli ta’lim texnologiyalari bilan bog‘lash usullaridan foydalanildi. Avvalo, axborot xavfsizligi va kriptografiya fanining o‘quv maqsadlari aniqlanib, ular matematik, algoritmik, dasturiy-amaliy va xavfsizlik madaniyati komponentlariga ajratildi. Keyin psevdotasodifiy sonlar generatorlari va oqimli shifrlar mavzusi kriptografiya kursidagi oldingi va keyingi mavzular bilan bog‘liq holda tahlil qilindi.

Metodik tahlilda kriptografiya fanini o‘qitish uchun ilmiylik, tizimlilik, izchillik, ko‘rgazmalilik, amaliy yo‘naltirilganlik, muammoli o‘qitish, xavfsiz tajriba muhiti va reflektiv baholash tamoyillari asos qilib olindi. Raqamli ta’lim vositalari sifatida LMS platformalari, Python yoki JavaScript asosidagi interaktiv kodlash muhiti, Jupyter Notebook, virtual laboratoriya, simulyator, avtomatik testlar, elektron portfoliolar va kriptografik jarayonlarni vizuallashtirish vositalarining

imkoniyatlari ko‘rib chiqildi.

Tadqiqotning metodik modeli quyidagi mantiqqa tayanadi: birinchidan, talabaning nazariy tayyorgarligi diagnostika qilinadi; ikkinchidan, mavzu algoritmik sxema va vizual model orqali tushuntiriladi; uchinchidan, talaba kichik amaliy topshiriqlar orqali generator yoki oqimli shifrning ishlash mexanizmini modellashtiradi; to‘rtinchidan, natija statistik ko‘rsatkichlar, test holatlari va reflektiv izohlar asosida baholanadi; beshinchidan, xatolar tahlili orqali keyingi o‘quv faoliyati moslashtiriladi.

Natijalar va muhokama (Results and Discussions).

Axborot xavfsizligi fanlarida kriptografiya markaziy o‘rin tutadi, chunki u ma’lumotni himoyalashning matematik va algoritmik asoslarini beradi. Maxfiylik shifrlash orqali, yaxlitlik xesh funksiyalar va autentifikatsiya kodlari orqali, autentiklik elektron imzo va sertifikatlar orqali, rad etib bo‘lmaslik esa kriptografik protokollar orqali ta’minlanadi. Shu sababli kriptografiya fanini o‘qitishda talaba nafaqat algoritm ketma-ketligini yod olishi, balki qaysi xavfsizlik xususiyati qaysi kriptografik mexanizm orqali ta’minlanishini tushunishi kerak.

Didaktik jihatdan kriptografiya fanini o‘qitishda ilmiylik tamoyili birinchi o‘rinda turadi. Kriptografik algoritmlar tasodifiy tanlangan amallar yig‘indisi emas, balki matematik isbot, murakkablik nazariyasi, ehtimollar nazariyasi va amaliy xavfsizlik talablariga asoslangan tizimlardir. Shuning uchun o‘qituvchi AES, RSA, ElGamal, elliptik egri chiziqlar, xesh funksiyalar yoki oqimli shifrlarni tushuntirganda ularning umumiy g‘oyasi bilan birga qo‘llanish chegaralari, zaif tomonlari va noto‘g‘ri ishlatilganda yuzaga keladigan xavflarni ham ko‘rsatishi lozim.

Tizimlilik va izchillik tamoyili kriptografiya kursida mavzularning mantiqiy ketma-ketligini to‘g‘ri qurishni talab qiladi. Avval axborot xavfsizligi tushunchalari, xavf modeli, kriptografik maqsadlar va matematik asoslar beriladi. Shundan keyin klassik shifrlar, simmetrik algoritmlar, oqimli shifrlar, psevdotasodifiy sonlar generatorlari, xesh funksiyalar, ochiq kalitli kriptografiya va protokollar ketma-ket o‘rganiladi. Bunday tartib talabaning oldingi bilimlar asosida keyingi murakkab tushunchani tushunishiga yordam beradi.

Amaliy yo‘naltirilganlik tamoyili kriptografiyani o‘qitishda alohida ahamiyatga ega. Talaba XOR amali, modulli qo‘shish, bitlarni siljitish, kalit uzunligi, nonce va initsializatsiya vektori kabi tushunchalarni faqat nazariy ta’rif orqali emas, balki amaliy kod, jadval, vizual oqim va test natijalari orqali anglaganda bilim mustahkamlanadi. Shu sababli har bir nazariy mavzu kichik laboratoriya ishi, tahliliy savol yoki muammoli vaziyat bilan yakunlanishi maqsadga muvofiq.

Ko‘rgazmalilik tamoyili murakkab kriptografik jarayonlarni soddalashtirilgan model orqali tushuntirishga xizmat qiladi. Masalan, oqimli shifrda ochiq matn bitlari kalit oqimi bilan XOR qilinishi natijasida shifrmatn hosil bo‘lishi oddiy jadval, rangli bloklar yoki animatsion ketma-ketlik orqali ko‘rsatilsa, talaba jarayonni tezroq anglaydi. Shu bilan birga, ko‘rgazmalilik ilmiy mazmunni soddalashtirib yubormasligi kerak; har bir modeldan keyin haqiqiy algoritmda mavjud bo‘lgan xavfsizlik talablari izohlanishi zarur.

Kriptografiya fanida etik va xavfsiz foydalanish tamoyili ham muhimdir. Talabalar kriptografik bilimlarni real tizimlarga zarar yetkazish uchun emas, balki ma’lumotlarni himoya qilish, dasturiy mahsulotlarni xavfsiz loyihalash va axborot xavfsizligi siyosatini to‘g‘ri tushunish uchun o‘rganishi kerak. Shu bois laboratoriya topshiriqlari nazorat qilinadigan, o‘quv maqsadiga yo‘naltirilgan va xavfsiz muhitda tashkil etilishi lozim.

Psevdotasodifiy sonlar generatorlari kriptografiya kursining eng muhim mavzularidan biridir. Chunki ko‘plab kriptografik tizimlarda kalit yaratish, nonce hosil qilish, initsializatsiya vektori tanlash, sessiya kalitlarini shakllantirish va oqimli shifrlar uchun kalit oqimini ishlab chiqarish tasodifiylik sifatiga bog‘liq. Oddiy dasturlashdagi tasodifiy son generatori bilan kriptografik

barqaror generator o‘rtasidagi farqni tushunmaslik amaliy xavfsizlik xatolariga olib kelishi mumkin. Shuning uchun talabalarga “tasodifiy ko‘rinadi” degan tushuncha bilan “kriptografik jihatdan bashorat qilib bo‘lmaydi” degan tushuncha o‘rtasidagi farq aniq tushuntirilishi kerak.

O‘quv dasturida psevdotasodifiy sonlar generatorlari mavzusi odatda ehtimollar nazariyasi, algoritmlar, modulli arifmetika va simmetrik kriptografiya asoslaridan keyin joylashtiriladi. Bunday joylashuv metodik jihatdan to‘g‘ri, chunki talaba generatorning davri, urug‘ qiymati, rekurrent formula, statistik xususiyatlar va bashorat qilinmaslik talabini oldingi matematik bilimlar yordamida anglaydi. Masalan, oddiy chiziqli kongruent generator $X(n+1) = (aX(n) + c) \bmod m$ formulasi orqali PRNG tushunchasini soddalashtirib tushuntirish mumkin, biroq keyin bunday generator kriptografik maqsadlar uchun yetarli emasligi albatta muhokama qilinadi.

Oqimli shifrlar mavzusi PRNG bilan bevosita bog‘liq. Oqimli shifrda kalit va boshlang‘ich parametrlar asosida kalit oqimi hosil qilinadi, so‘ng ochiq matn bitlari yoki baytlari ushbu kalit oqimi bilan birlashtiriladi. Eng sodda ko‘rinishda shifrlash $C(i) = P(i)$ XOR $K(i)$, deshifrlash esa $P(i) = C(i)$ XOR $K(i)$ ko‘rinishida ifodalanadi. Bu formula talabalarga oqimli shifrning asosiy g‘oyasini tushuntirish uchun qulay, lekin haqiqiy algoritmlarda kalit oqimini hosil qilish murakkab va xavfsizlikka qat’iy talablar qo‘yilishi alohida ta’kidlanadi.

Oqimli shifrlarni o‘qitishda RC4 tarixi, uning amaliy zaifliklari va zamonaviy algoritmlar, xususan ChaCha20 kabi oqimli shifrlar haqida qisqa tahliliy ma’lumot berish foydali. Bu yondashuv talabaga kriptografiyada algoritmning mashhurligi yoki uzoq yillar qo‘llanilishi uning doimiy xavfsizligini kafolatlamasligini ko‘rsatadi. Shuningdek, nonce qayta ishlatilishi, bir xil kalit oqimidan takror foydalanish, zaif urug‘ qiymati va noto‘g‘ri sinxronlashuv oqimli shifrlarda jiddiy xavf tug‘dirishi tushuntiriladi.

Mazkur mavzuning o‘quv dasturidagi o‘rni nazariy va amaliy kompetensiyalarni bog‘lash imkonini beradi. Talaba bir tomondan tasodifiylik, entropiya, davr, statistik testlar, kalit oqimi va farqlanmaslik tushunchalarini o‘zlashtiradi; ikkinchi tomondan kichik dastur yozish, generator natijasini tekshirish, shifrlash va deshifrlash jarayonini modellashtirish, xatoli holatlarni tahlil qilish kabi amaliy ko‘nikmalarni egallaydi.

1-jadval

Psevdotasodifiy generatorlar va oqimli shifrlarni o‘qitishda kompetensiyaviy bog‘liqlik

Mavzu elementi	Shakllanadigan kompetensiya	Raqamli vosita	Baholash mezoni
Urug‘ qiymati va generator davri	Tasodifiylik manbasini tahlil qilish	Interaktiv jadval, Python modeli	Formula va natijani izohlash
Statistik testlar	Generator chiqishini baholash	Grafik, gistogramma, NIST testlariga kirish	Natija asosida xulosa chiqarish
XOR asosidagi shifrlash	Bitli amallarni algoritmik tushunish	Vizual simulyator, kod muhiti	Shifrlash/deshifrlashni to‘g‘ri bajarish
Nonce va IV	Kalit oqimining takrorlanish xavfini tushunish	Muammoli vaziyat, case-study	Xavf sababini tushuntirish
Oqimli shifrlar	Algoritm bosqichlarini modellashtirish	Virtual laboratoriya	Test holatlarida barqaror ishlash

1-jadvaldan ko‘rinadiki, mavzuni samarali o‘qitish uchun har bir nazariy tushuncha alohida amaliy faoliyat, raqamli vosita va aniq baholash mezoni bilan bog‘lanishi lozim. Bu yondashuv talabaning faqat formulani bilishini emas, balki kriptografik jarayonni tahlil qilish va xavfsizlik xulosasini chiqarish ko‘nikmasini ham rivojlantiradi.

Raqamli ta’lim texnologiyalari kriptografiya fanini o‘qitishda murakkab jarayonlarni ko‘rgazmali, interaktiv va tajribaga asoslangan tarzda tashkil etish imkonini beradi. An’anaviy ma’ruzada oqimli shifrning ishlashini doskada formula orqali tushuntirish mumkin, biroq raqamli muhitda talaba ochiq matn, kalit oqimi va shifrmatn o‘rtasidagi bog‘liqlikni real vaqt rejimida ko‘rishi, parametrlarni o‘zgartirishi, xatoli holatlarni sinashi va natijani tahlil qilishi mumkin. Bu esa mavzuning abstraktligini kamaytiradi.

Virtual laboratoriya kriptografik algoritmlarni o‘qitishda eng samarali vositalardan biri hisoblanadi. Unda talaba oddiy PRNG, kriptografik PRNG, XOR-shifr, oqimli shifr modeli, kalit oqimi, nonce, IV va statistik tekshiruvlarni xavfsiz o‘quv muhitida bajaradi. Laboratoriya topshiriqlari “berilgan algoritmni ishga tushirish” bilan cheklanmasligi kerak; aksincha, talaba parametr o‘zgarganda natija qanday o‘zgarishini tahlil qilishi, zaif generatorni kuchli generator bilan qiyoslashi va xatoli kriptografik dizayn oqibatini tushuntirishi zarur.

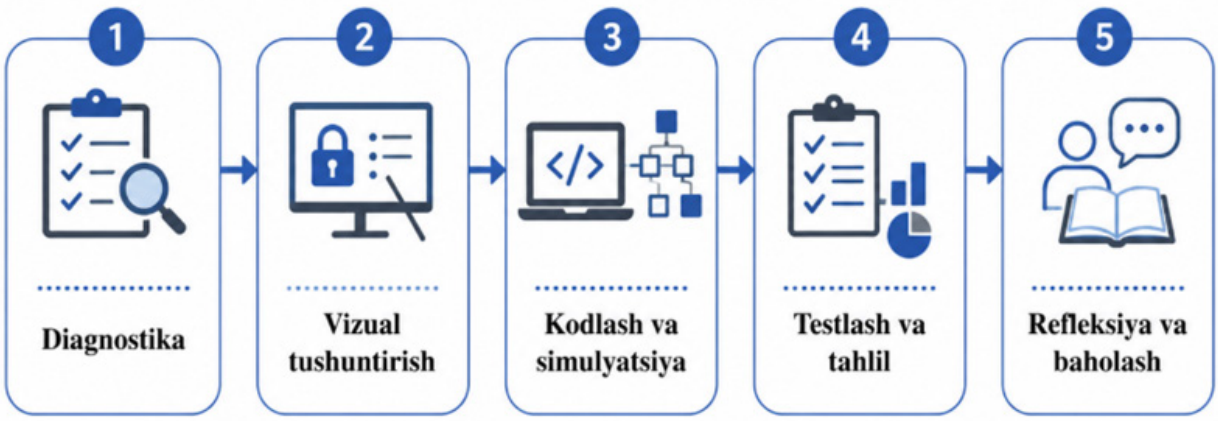
Jupyter Notebook yoki Google Colab kabi interaktiv muhitlar kriptografiya darslarida nazariya va kodni birlashtirishga yordam beradi. Bunday muhitda matnli izoh, formula, jadval, kod va grafik bitta faylda joylashadi. Masalan, talaba LCG generatori natijasini hosil qiladi, uning qiymatlarini grafikda ko‘radi, oddiy chastota tahlilini bajaradi va shu asosda “statistik ko‘rinishda

tekis taqsimlangan natija har doim kriptografik xavfsizlikni anglatmaydi” degan xulosaga keladi. Bu yondashuv ilmiy fikrlashni kuchaytiradi.

LMS platformalari mavzuni modulli tashkil etish, diagnostik test, amaliy topshiriq, kod fayllarini topshirish, forum muhokamasi va reflektiv savollarni boshqarish imkonini beradi. Masalan, “PRNG va oqimli shifrlar” moduli kirish savollari, qisqa videodars, interaktiv simulyatsiya, laboratoriya topshirig‘i, nazorat savollari va yakuniy mini-loyihadan iborat bo‘lishi mumkin. Talabaning urinishlar soni, kod xatolari, test natijalari va izohli javoblari keyingi mashg‘ulotni moslashtirish uchun diagnostik ma’lumot vazifasini bajaradi.

Avtomatlashtirilgan baholash vositalari kriptografiya darslarida ehtiyotkorlik bilan qo‘llanishi kerak. Kodning ishlashi muhim, lekin kriptografiyada natijaning to‘g‘ri chiqishi har doim xavfsiz dizaynni anglatmaydi. Shu sababli baholash mezoni natijaviy testlardan tashqari, algoritm izohi, parametrlar tanlovi, xavfsizlik cheklovlarini tushuntirish va xatoli holatlarni tahlil qilishni ham qamrab olishi lozim. Talaba “kod ishladi” degan xulosadan “kod qaysi xavfsizlik shartlari bajarilganda ishonchli bo‘ladi” degan xulosaga o‘tishi kerak.

Muammoli va loyiha asosida o‘qitish ham kriptografiya fani uchun mos yondashuvdir. Talabalarga oddiy chat ilovasida xabarlarni oqimli shifr modeli bilan himoyalash, generator chiqishini statistik tahlil qilish, nonce takrorlanganda yuzaga keladigan xavfni ko‘rsatish yoki ikki xil generatorni qiyoslash kabi mini-loyihalar berilishi mumkin. Bunday topshiriqlar fanlararo bog‘liqlikni kuchaytiradi: dasturlash, matematik tahlil, axborot xavfsizligi va foydalanuvchi mas’uliyati bir jarayonda namoyon bo‘ladi.



1-rasm. Kriptografik algoritmlarni raqamli muhitda o‘qitishning metodik modeli

1-rasmda kriptografik algoritmlarni raqamli muhitda o‘qitishning umumiy metodik ketma-ketligi aks ettirilgan. Ushbu modelda o‘qitish diagnostikadan boshlanadi, keyin mavzu vizual va algoritmik tushuntiriladi, talaba kodlash va simulyatsiya orqali tajriba o‘tkazadi, natijani testlaydi va yakunda reflektiv izoh asosida bilimini mustahkamlaydi.

Kriptografiya fanini o‘qitishda birinchi muammo talabalarning matematik tayyorgarligi turlicha bo‘lishidir. Modulli arifmetika, ehtimollar nazariyasi, diskret matematika va bitli amallar bo‘yicha bilim yetarli bo‘lmasa, PRNG va oqimli shifrlar mavzusi yuzaki o‘zlashtiriladi. Buni bartaraf etish uchun mavzudan oldin qisqa diagnostik test, tayanch matematik tushunchalar bo‘yicha mikro-ma’ruza va oddiy misollar asosidagi tayyorlov bloki tashkil etish maqsadga muvofiq.

Ikkinchi muammo tasodifiylik va psevdotasodifiylik tushunchalarini chalkashtirish bilan bog‘liq. Ko‘plab talabalar kompyuter yaratgan sonlar avtomatik ravishda “tasodifiy” va xavfsiz deb o‘ylaydi. Dars jarayonida oddiy generator, statistik jihatdan qoniqarli generator va kriptografik barqaror generator o‘rtasidagi farq aniq misollar yordamida ko‘rsatilishi kerak. Masalan, bir

generator natijalari bir qarashda tartibsiz ko‘rinsa-da, urug‘ qiymati ma’lum bo‘lsa, keyingi qiymatlarni bashorat qilish mumkinligi amaliy tajriba orqali tushuntiriladi.

Uchinchi muammo oqimli shifrlar xavfsizligini faqat XOR amalining soddaligi bilan baholashdir. Talaba XOR amali osonligini ko‘rib, oqimli shifr ham oddiy deb xulosa qilishi mumkin. Aslida xavfsizlik kalit oqimining bashorat qilib bo‘lmasligi, nonce va kalitning to‘g‘ri ishlatilishi, sinxronlashuv va protokol shartlariga bog‘liq. Shu sababli o‘qitishda “to‘g‘ri ishlaydigan algoritm” va “xavfsiz ishlatiladigan algoritm” tushunchalari alohida ajratilishi zarur.

To‘rtinchi muammo laboratoriya topshiriqlarining reproduktiv xarakterda qolib ketishidir. Agar talaba faqat tayyor kodni ko‘chirib ishga tushirsa, mavzuning metodik maqsadi amalga oshmaydi. Laboratoriya ishlari tahliliy savollar, parametrlarni o‘zgartirish, xatoli holatni topish, xavfsizlik xulosasi yozish va natijani himoya qilish bilan boyitilishi kerak. Har bir laboratoriya ishi “nima qildim?” savoliga emas, “nima uchun shunday natija chiqdi va xavfsizlik nuqtai nazaridan bu nimani anglatadi?” savoliga javob berishi lozim.

Beshinchi muammo raqamli ta’limda akademik halollik bilan bog‘liq. Talabalar tayyor kod, generator yoki shifr algoritmini internetdan olib, uning ishlash mohiyatini tushunmasdan topshirishi mumkin. Buni kamaytirish uchun topshiriqlarda individual parametrlar, og‘zaki himoya, kod izohi, test natijalarini tahlil qilish, xatolarni tushuntirish va reflektiv savollar qo‘llanilishi kerak. Baholash jarayoni yakuniy natijani emas, balki talabaning fikrlash jarayoni va xavfsizlik xulosasini ham hisobga olishi zarur.

Oltinchi muammo o‘qituvchilar uchun metodik resurslarning yetarli emasligidir. Kriptografik mavzular ko‘pincha matematik yoki dasturiy tomondan alohida yoritiladi, ammo ularni pedagogik ketma-ketlik, raqamli vosita va baholash mezoni bilan bog‘laydigan o‘quv-uslubiy materiallar yetishmaydi. Shuning uchun kriptografiya fani bo‘yicha modul kartalari, laboratoriya ssenariylari, xavfsiz kodlash bo‘yicha yo‘riqnoma, diagnostik testlar va rubrikalar ishlab chiqilishi kerak.

2-jadval

Kriptografiya fanini o‘qitishdagi muammolar va metodik yechimlar

Mavjud muammo	Kutiladigan oqibat	Metodik yechim
Matematik tayyorgarlikning yetarli emasligi	Formula va algoritmlarni yuzaki yodlash	Tayanch matematika bo‘yicha diagnostika va mikro-mashqlar
Tasodifiylikni noto‘g‘ri talqin qilish	Zaif generatorni xavfsiz deb qabul qilish	PRNG, TRNG va CSPRNG farqini tajriba orqali ko‘rsatish
Oqimli shifrlarni haddan tashqari soddalashtirish	Nonce yoki kalit oqimini noto‘g‘ri qo‘llash	Xatoli case-study va xavfsizlik tahlili
Tayyor kodni ko‘chirish	Mustaqil algoritmik fikrlash shakllanmasligi	Individual parametr, kod izohi va og‘zaki himoya
Laboratoriya vositalarining cheklanganligi	Nazariya-amaliyot uzilishi	Virtual laboratoriya, simulyator va avtomatik testlar

Xulosa va takliflar (Conclusion and Suggestions).

Kriptografiya fanini o‘qitish axborot xavfsizligi kompetensiyalarini shakllantirishning muhim

tarkibiy qismidir. Ushbu fan talabalarda matematik asoslangan fikrlash, algoritmik tahlil, xavfsiz dasturiy yechim yaratish, kriptografik mexanizmlarni to‘g‘ri qo‘llash va axborot xavfsizligi madaniyatini rivojlantiradi. Psevdotasodifiy sonlar generatorlari va oqimli shifrlar mavzusi esa kriptografiya kursida nazariya bilan amaliyot bog‘lanadigan muhim bo‘g‘in hisoblanadi.

Tahlillar shuni ko‘rsatadiki, mazkur mavzuni samarali o‘qitish uchun ilmiylik, tizimlilik, izchillik, ko‘rgazmalilik, amaliy yo‘naltirilganlik, xavfsiz tajriba muhiti va reflektiv baholash tamoyillariga tayanish zarur. Raqamli ta’lim texnologiyalari bu jarayonda o‘quv materialini soddalashtirish emas, balki murakkab kriptografik jarayonlarni ko‘rinarli, tajribaviy va tahliliy shaklda o‘zlashtirishga xizmat qilishi kerak.

Maqola natijalaridan kelib chiqib quyidagi takliflar ilgari suriladi: kriptografiya fanida PRNG va oqimli shifrlar bo‘yicha alohida virtual laboratoriya ishlab chiqish; har bir laboratoriya ishiga xavfsizlik tahlili va reflektiv savollarni kiritish; talabalarning matematik tayyorgarligini aniqlash uchun diagnostik blok yaratish; LMS platformasida mavzuni modul ko‘rinishida tashkil etish; baholashda kod natijasi bilan birga algoritm izohi, parametrlar tanlovi va xavfsizlik xulosasini ham hisobga olish.

Shunday qilib, kriptografiya fanini raqamli ta’lim texnologiyalari asosida o‘qitish talabalarning nazariy bilimini amaliy kompetensiyaga aylantirish, xavfsiz fikrlashni shakllantirish va kiberxavfsizlik sohasida malakali mutaxassis tayyorlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1996.

2. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. CRC Press, 2020.

3. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2023.

4. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.

5. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2010.