O‘ZBEKISTON MILLIY UNIVERSITETI XABARLARI, 2026, [14]
ISSN 2181-7324(Print)

IJTIMOIY FANLAR
http://journals.nuu.uz
ISSN 3093-8996(Onlayn)

UDK: 004.056.55:378.147

Azamat I.TILLAYEV,
PhD, dotsent v.b.., O‘zbekiston Milliy Universiteti, Toshkent, O‘zbekiston
E-mail: tillayev1@mail.ru, ORCI: 0000-0003-2018-7012

Dotsent, PhD K.Raximov taqrizi asosida

KRIPTOGRAFIYA FANINING “KLASSIK SHIFRLASH ALGORITMLARI” BO‘LIMINI O‘QITISHNI SUN’IY INTELLEKTGA ASOSLANGAN SIMULYATOR ISHLANMALARDAN FOYDALANISH ORQALI TAKOMILLASHTIRISH

Annotatsiya

Maqolada kriptografiya fanining “Klassik shifrlash algoritmlari” bo‘limini o‘qitishda sun’iy intellektga asoslangan simulyatordan foydalanish metodikasi taklif etilgan. Simulyatorning arxitekturasi, shifrlash va kriptotahlil modullari, talaba modeli, adaptiv topshiriq generatori va SI-tutor funksiyalari yoritilgan. Simulyator yordamida o‘tkaziladigan amaliy mashg‘ulotning tuzilmasi hamda metodikaning samaradorligini baholash uchun pedagogik tajriba dizayni asoslab berilgan.

Kalit so‘zlar: Kriptografiya, klassik shifrlar, Sezar shifri, Vijener shifri, kriptotahlil, simulyator, sun’iy intellekt, adaptiv ta’lim, intellektual o‘qitish tizimi.

УЛУЧШЕНИЕ ПРЕПОДАВАНИЯ РАЗДЕЛА «КЛАССИЧЕСКИЕ АЛГОРИТМЫ ШИФРОВАНИЯ» В КРИПТОГРАФИИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ СИМУЛЯТОРОВ, ОСНОВАННЫХ НА ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ

Аннотация

В статье предложена методика преподавания раздела «Классические алгоритмы шифрования» дисциплины «Криптография» с использованием симулятора на основе искусственного интеллекта. Описаны архитектура симулятора, модули шифрования и криптоанализа, модель обучающегося, адаптивный генератор заданий и функции ИИ-тьютора. Обоснованы структура практического занятия и дизайн педагогического эксперимента для оценки эффективности методики.

Ключевые слова: Криптография, классические шифры, шифр Цезаря, шифр Виженера, криптоанализ, симулятор, искусственный интеллект, адаптивное обучение.

IMPROVING THE TEACHING OF THE "CLASSICAL ENCRYPTION ALGORITHMS" SECTION OF CRYPTOGRAPHY THROUGH THE USE OF AI-BASED SIMULATORS

Annotation

The article proposes a methodology for teaching the “Classical Encryption Algorithms” section of the Cryptography course using an artificial intelligence-based simulator. The simulator architecture, encryption and cryptanalysis modules, learner model, adaptive task generator and AI tutor functions are described. The structure of a practical session and the design of a pedagogical experiment for evaluating the methodology are substantiated.

Key words: Cryptography, classical ciphers, Caesar cipher, Vigenère cipher, cryptanalysis, simulator, artificial intelligence, adaptive learning.

Kirish. Raqamli iqtisodiyot va elektron hukumat tizimlarining jadal rivojlanishi axborot xavfsizligi sohasida yuqori malakali kadrlar tayyorlash masalasini dolzarb vazifalar qatoriga olib chiqdi. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi hamda 2021-yil 17-fevraldagi PQ-4996-son “Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida”gi qarori ta’lim jarayoniga raqamli va intellektual texnologiyalarni keng joriy etishni ustuvor yo‘nalish sifatida belgilaydi [1; 2].

Kriptografiya fanining “Klassik shifrlash algoritmlari” bo‘limi butun kursning poydevori hisoblanadi. Aynan shu bo‘limda talabalar ochiq matn, shifrmatn, kalit, kalitlar fazosi, almashtirish va o‘rin almashtirish, kriptobardoshlilik va kriptotahlil kabi tayanch tushunchalarni ilk bor o‘zlashtiradilar. K. Shennon tomonidan asoslangan konfuziya va diffuziya tamoyillari [3] ham klassik shifrlarning tahlilidan kelib chiqqan bo‘lib, zamonaviy blokli shifrlarning tuzilishini tushunish uchun zarur nazariy asos bo‘lib xizmat qiladi.

Amaliyot shuni ko‘rsatadiki, ushbu bo‘limni an’anaviy usulda o‘qitishda bir qator muammolar yuzaga keladi. Birinchidan, shifrlash va deshifrlashni qo‘lda bajarish ko‘p vaqt talab etadi, natijada talaba e’tibori algoritm mohiyatidan mexanik hisoblashga ko‘chadi. Ikkinchidan, kriptotahlil usullari — chastotaviy tahlil, Kasiski usuli, moslik indeksini hisoblash — katta hajmdagi hisob-kitoblarni talab qiladi va ularni auditoriyada qo‘lda to‘liq bajarish deyarli imkonsiz. Uchinchidan, guruhdagi talabalarning matematik tayyorgarligi turlicha bo‘lib, o‘qituvchi har bir talabaga tezkor individual qayta aloqa bera olmaydi.

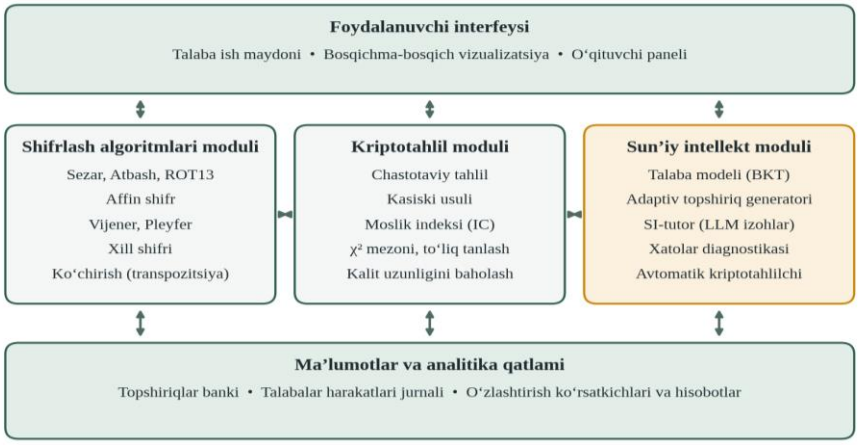
Ushbu muammolarni hal etishning istiqbolli yo‘li — o‘quv simulyatorlari va sun’iy intellekt (SI) texnologiyalarini uyg‘unlashtirishdir. Simulyator algoritmning har bir qadamini ko‘rgazmali tarzda namoyish etib, talabaga parametrlarni o‘zgartirib tajriba o‘tkazish imkonini beradi, SI moduli esa talabaning bilim darajasini baholab, o‘quv jarayonini individual moslashtiradi.

Mavzuga oid adabiyotlar tahlili va tadqiqot metodologiyasi. Klassik shifrlarning tarixi va kriptotahlil

usullari D. Kan va S. Singx [6] asarlarida keng yoritilgan. V. Stallings, K. Paar va Ya. Pelsl, J. Kats va Ye. Lindell [7] darsliklarida klassik shifrlar zamonaviy kriptografiyaga kirish sifatida qaraladi va ularning matematik modellari modul arifmetikasi asosida bayon etiladi. Polialfavit shifrlarni tahlil qilishning asosiy usullari — F. Kasiski usuli [9] va V. Fridmanning moslik indeksi [8] — hozirgi kunda ham o‘quv kurslarida asosiy tahliliy vosita sifatida o‘rganiladi.

Kriptografiyani o‘qitishda eng keng tarqalgan dasturiy vositalardan biri — ochiq kodli CrypTool loyihasidir [10]. U klassik va zamonaviy algoritmlarni vizuallashtirish hamda kriptotahlil vositalarini taqdim etadi. Biroq bunday vositalar asosan namoyish va tahlil uchun mo‘ljallangan bo‘lib, talabaning bilim darajasini modellashtirish va o‘quv trayektoriyasini individual moslashtirish funksiyalari ularda ko‘zda tutilmagan. Tahlil shuni ko‘rsatadiki, klassik shifrlarni o‘qitish uchun simulyatsiya imkoniyatlarini SI asosidagi adaptiv yo‘naltirish bilan birlashtirgan, o‘zbek tilida va o‘zbek alifbosi xususiyatlarini hisobga olgan holda ishlab chiqilgan metodik ishlanmalar yetarli emas. Ushbu maqola shu bo‘shliqni to‘ldirishga qaratilgan.

Natijalar va muhokama. 1.Simulyatorning arxitekturasi. Ishlab chiqilgan simulyator besh qatlamli modulli arxitekturaga ega (1-rasm). Foydalanuvchi interfeysi qatlami talabaning ish maydoni, algoritm qadamlarining vizualizatsiyasi va o‘qituvchi panelini o‘z ichiga oladi. Markaziy qatlamda uchta o‘zaro bog‘langan modul joylashgan: shifrlash algoritmlari moduli, kriptotahlil moduli va sun’iy intellekt moduli. Quyi qatlam topshiriqlar banki, talaba harakatlari jurnali va o‘zlashtirish ko‘rsatkichlarini saqlaydi.



1-rasm. SI ga asoslangan kriptografik simulyatorning arxitekturasi

Simulyatorda o‘rganiladigan klassik algoritmlar va ularga mos vizualizatsiya hamda kriptotahlil vositalari 1-jadvalda keltirilgan.

1-jadval. Simulyatordagi klassik shifrlash algoritmlari

Algoritm	Shifr turi	Simulyatordagi vizualizatsiya	Kriptotahlil usuli
Sezar, ROT13	Monoalfavit almashtirish	Alifbo diskining aylanishi	To‘liq tanlash, chastotaviy tahlil
Affin shifr	Monoalfavit almashtirish	x → ax + b moslik jadvali	Chastotaviy tahlil, chiziqli tenglamalar tizimi
Vijener	Polialfavit almashtirish	Vijener jadvali, kalitning takrorlanishi	Kasiski usuli, moslik indeksi
Pleyfer	Bigrammali almashtirish	5×5 kalit matritsasi	Bigrammalar chastotasi
Xill	Chiziqli poligramma shifr	Matritsaviy ko‘paytma	Ma’lum ochiq matn hujumi
Ustunli ko‘chirish	O‘rin almashtirish	Jadval ustunlarining qayta tartiblanishi	Ustunlar tartibini tanlash, anagramma

Algoritmlarning matematik modellari. Simulyatorda har bir algoritm alifbo quvvati n ga nisbatan modul arifmetikasi asosida amalga oshirilgan. Bu esa bitta dasturiy yadroda 26 harfli lotin alifbosi bilan bir qatorda o‘zbek lotin alifbosidan ham foydalanish imkonini beradi: o‘zbek alifbosidagi o‘, g‘, sh, ch va ng harf birikmalari bitta belgi sifatida qaraladi. Harflar 0 dan n − 1 gacha bo‘lgan sonlar bilan kodlanadi. Sezar shifrida shifrlash va deshifrlash quyidagicha ifodalanadi:

$$E(x) = (x + k) \bmod n,\quad D(y) = (y - k) \bmod n, \qquad (1)$$

bu yerda x — ochiq matn harfining kodi, y — shifrmatn harfining kodi, k — kalit. Affin shifr Sezar shifrining umumlashmasi hisoblanadi:

$$E(x) = (a \cdot x + b) \bmod n,\quad D(y) = a^{-1} \cdot (y - b) \bmod n,\quad \text{EKUB}(a, n) = 1. \qquad (2)$$

Simulyator talabaga a parametrini n bilan o‘zaro tub bo‘lmagan qiymatga o‘zgartirib ko‘rish imkonini beradi: bu holda shifrlash akslantirishi o‘zaro bir qiymatli bo‘lmay qolishini talaba ekranda bevosita kuzatadi. Masalan, n = 26 da a uchun 12 ta ruxsat etilgan qiymat mavjud bo‘lib, kalitlar fazosi 12·26 = 312 ga teng. Vijener shifrida m uzunlikdagi kalit davriy takrorlanadi:

$$y_i = (x_i + k_{i \bmod m}) \bmod n. \qquad (3)$$

Xill shifrida ochiq matn d uzunlikdagi bloklarga bo‘linadi va har bir blok kalit matritsasiga ko‘paytiriladi:

$$Y = K \cdot X \bmod n,\quad \text{EKUB}(\det K, n) = 1. \qquad (4)$$

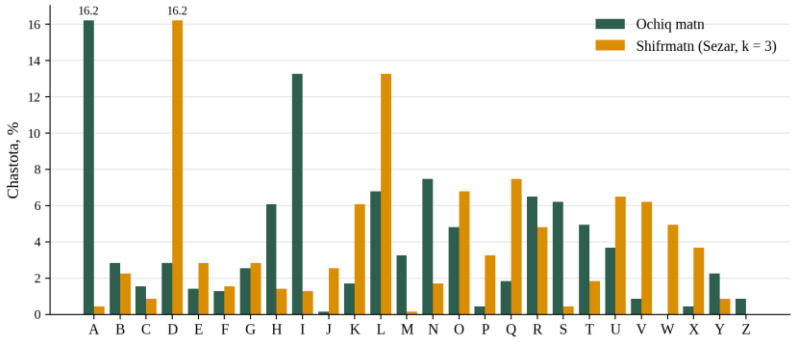
Polialfavit shifrlarni tahlil qilishda moslik indeksi muhim ahamiyatga ega:

$$IC = \sum f_i(f_i - 1) / (N(N - 1)), \qquad (5)$$

bu yerda f_i — i-harfning matndagi soni, N — matndagi harflarning umumiy soni. Ingliz tilidagi mazmunli matn uchun IC ≈ 0,066, tasodifiy 26 harfli matn uchun esa IC ≈ 1/26 ≈ 0,038 ga teng [9].

Kriptotahlilni vizuallashtirish. Simulyatorning muhim didaktik imkoniyati — kriptotahlil jarayonini ko‘rgazmali qilishdir. 2-rasmda maqola muallifi tomonidan tayyorlangan 709 harfdan iborat o‘zbekcha o‘quv matni va uning k = 3 kalit

bilan Sezar shifri yordamida olingan shifrmatnidagi harflar chastotasi keltirilgan (tahlil soddalik uchun 26 harfli lotin alifbosida bajarilgan, tutuq belgisi hisobga olinmagan).



2-rasm. Ochiq matn va Sezar shifrmatnidagi harflar chastotasi (k = 3)

Grafikdan ko‘rinib turibdiki, ochiq matndagi eng ko‘p uchraydigan “A” harfi (16,2 %) shifrmatnda “D” harfiga, ikkinchi o‘rindagi “I” harfi (13,3 %) esa “L” harfiga o‘tgan.

4. Sun’iy intellekt modulining funksiyalari. SI moduli simulyatorni oddiy namoyish vositasidan intellektual o‘qitish tizimiga aylantiradi. Uning asosiy funksiyalari 2-jadvalda keltirilgan.

2-jadval. Sun’iy intellekt modulining funksiyalari

Funksiya	Texnologik asos	Pedagogik vazifasi
Talaba modeli	Bayes bilimlarni kuzatish (BKT) modeli	Har bir ko‘nikmaning o‘zlashtirilganlik ehtimolini baholash
Adaptiv topshiriq generatori	Talaba modeli va qiyinlik darajalariga asoslangan tanlash qoidalari	Topshiriqni talabaning “yaqin rivojlanish zonasi”da tanlash
SI-tutor	Katta til modeli (LLM), mavzu konteksti bilan cheklangan	Tayyor javob bermasdan yo‘naltiruvchi savollar va bosqichma-bosqich izohlar
Xatolar diagnostikasi	Tipik xatolar namunalari bo‘yicha klassifikator	Mod amali, kalitni indekslash, teskari elementni topishdagi xatolarni aniqlash
Avtomatik kriptotahlilchi	χ^2 mezoni, moslik indeksi, “tepalikka chiqish” (hill climbing) evristikasi	Talaba yechimini tekshirish, namunaviy tahlil yo‘lini ko‘rsatish

Talaba modeli har bir ko‘nikmani — masalan, “modul bo‘yicha qo‘shish”, “affin shifrda teskari elementni topish”, “Kasiski usulida kalit uzunligini aniqlash” — alohida kuzatadi. Talaba topshiriqni bajargan har safar ko‘nikmaning o‘zlashtirilganlik ehtimoli qayta hisoblanadi [3].

5. Amaliy mashg‘ulotni tashkil etish metodikasi. Simulyatordan foydalangan holda o‘tkaziladigan 80 daqiqalik amaliy mashg‘ulot tajribaviy o‘rganish tsikli asosida quriladi (3-jadval).

3-jadval. Simulyator asosidagi amaliy mashg‘ulotning tuzilmasi

Bosqich	Vaqt	O‘qituvchi va talaba faoliyati	Simulyator funksiyasi
1. Motivatsiya	5 daq.	Tarixiy keys: shifrlangan xabarni ochish muammosi qo‘yiladi	Shifrlangan xabarni namoyish etish
2. Nazariy asos	15 daq.	Algoritmning matematik modeli muhokama qilinadi	Qadamlarni bosqichma-bosqich vizuallashtirish
3. Tadqiqot	20 daq.	Talabalar parametrlarni o‘zgartirib, qonuniyatlarni aniqlaydi	Interaktiv tajriba maydoni, SI-tutor izohlari
4. Kriptotahlil topshirig‘i	25 daq.	Talaba “kriptotahlilchi” rolida shifrmatnni ochadi	Adaptiv topshiriq, xatolar diagnostikasi
5. Refleksiya va baholash	15 daq.	Natijalar muhokamasi, xulosalar	Individual hisobot, o‘qituvchi paneli

Topshiriqlar Blum taksonomiyasining qayta ko‘rib chiqilgan varianti asosida uch darajada tuziladi: reproduktiv daraja (berilgan kalit bilan shifrlash va deshifrlash), qo‘llash va tahlil darajasi (kalit noma’lum bo‘lganda kriptotahlil qilish) hamda baholash va yaratish darajasi (algoritmning zaif tomonlarini asoslash va uni kuchaytirish yo‘lini taklif etish). O‘qituvchi paneli guruh bo‘yicha qaysi ko‘nikmalar sust o‘zlashtirilganini real vaqt rejimida ko‘rsatadi va o‘qituvchiga mashg‘ulot davomida tezkor tuzatish kiritish imkonini beradi [5].

Olingan natijalar simulyatsiya va adaptiv qayta aloqani uyg‘unlashtirish talabalarning klassik shifrlarni o‘zlashtirishiga ijobiy ta’sir ko‘rsatishi haqidagi xalqaro tadqiqotlar xulosalari bilan mos keladi [3].

Shu bilan birga, SI texnologiyalaridan foydalanishda bir qator xavflarni hisobga olish zarur. Birinchidan, talaba SI-tutorga haddan tashqari tayanib, mustaqil fikrlash ko‘nikmasini yo‘qotishi mumkin; shu sababli tutor javob bermaydigan, faqat yo‘naltiradigan rejimda ishlashi lozim. Ikkinchidan, til modellari noto‘g‘ri ma’lumot generatsiya qilishi mumkin, shuning uchun hisoblashga oid barcha javoblar deterministik modul tomonidan tekshiriladi. Uchinchidan, nazorat topshiriqlarida simulyatorning yordamchi funksiyalari

cheklanishi, talabaning qo‘lda bajariladigan asosiy ko‘nikmalari esa alohida baholanishi kerak [4].

Taklif etilgan yondashuvni “Zamonaviy simmetrik shifrlar” va “Ochiq kalitli kriptotizimlar” bo‘limlariga ham kengaytirish mumkin. Masalan, simulyatorning modulli arxitekturasi Feystel tarmog‘i raundlarini yoki RSA algoritmidagi modul bo‘yicha darajaga ko‘tarish amallarini vizuallashtiruvchi yangi modullarni qo‘shish imkonini beradi. Tadqiqot ishi AL-9624115223-sonli “Kriptografiya fani bo‘yicha elektron o‘quv qo‘llanma yaratish” mavzusidagi amaliy loyiha doirasida bajarildi.

Xulosa va tavsiyalar. Tadqiqot natijalari asosida quyidagi xulosalarga kelindi. Birinchidan, kriptografiya fanining “Klassik shifrlash algoritmlari” bo‘limini an’anaviy usulda o‘qitish mexanik hisoblashlarga ortiqcha vaqt sarflanishi va individual qayta aloqaning yetishmasligi bilan bog‘liq cheklovlarga ega. Ikkinchidan, shifrlash, kriptotahlil va sun’iy intellekt modullaridan iborat simulyator bu cheklovlarni bartaraf etish imkonini beradi: u algoritmlarni vizuallashtiradi, kriptotahlilni amalda bajarishga sharoit yaratadi va talaba modeli asosida o‘quv jarayonini individuallashtiradi. Uchinchidan, tajribaviy o‘rganish tsikli asosida qurilgan amaliy mashg‘ulot tuzilmasi va Blum taksonomiyasiga muvofiq ko‘p darajali topshiriqlar tizimi talabalarning reproduktiv faoliyatdan tahliliy va ijodiy faoliyatga o‘tishini ta’minlaydi.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son ““Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni. — www.lex.uz.
2. O‘zbekiston Respublikasi Prezidentining 2021-yil 17-fevraldagi PQ-4996-son “Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida”gi qarori. — www.lex.uz.
3. Tillayev A.I. Oliy ta’limda videoma’ruzalar tayyorlashning umumiy qoidalari. “Ilm sarchashmalari” UrDU ilmiy jurnali, 2025 №12/2, 138–141 b.
4. Tillayev A.I., Ishmuratova L.A. Zamonaviy interaktiv talimiy veb-saytlarni yaratishda texnologik va pedagogik yondashuvlar. O‘zMU xabarlari, 2026 №2, 197–200 b.
5. Azamat Tillaev. Development of An Electronic Training Manual on Cryptographic Methods Using Modern Multimedia and Artificial Intelligence Technologies. International Journal of Pedagogics, 6(05), USA, 2026, P.463–466.
6. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. — Pearson, 2017. — 767 p.
7. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. — Boca Raton: CRC Press, 2020. — 648 p.
8. VanLehn K. The Relative Effectiveness of Human Tutoring, Intelligent Tutoring Systems, and Other Tutoring Systems // Educational Psychologist. — 2011. — Vol. 46, No. 4. — P. 197–221.
9. Kasneci E. et al. ChatGPT for Good? On Opportunities and Challenges of Large Language Models for Education // Learning and Individual Differences. — 2023. — Vol. 103. — Article 102274.
10. CrypTool: e-learning platform for cryptography and cryptanalysis [Elektron resurs]. — URL: https://www.cryptool.org.