E CONF SERIES

International Conference on Medical Science, Medicine and Public Health
Hosted online from Jakarta, Indonesia
Website: econfseries.com 30th September, 2025

KRIPTOGRAFIK ALGORITMLARNING MATEMATIK VA ALGORITMIK ASOSLARINI O‘RGANISHNING DIDAKTIK JIHATLARI VA ULARNING TA’LIMIY DASTURIY VOSITALAR ORQALI O‘QITISH METODIKASI

Sadinov Otabek Baxodirovich
Navoiy Davlat Universiteti Aniq Fanlar Fakulteti Talabasi

Annotatsiya:
Maqolada kriptografik algoritmlarning nazariy va amaliy asoslarini o‘rganishning didaktik tahlili ilmiy tahlil, ushbu algoritmlarning matematik asoslari – son nazariyasi, modulli arifmetika, kombinatorik tuzilmalar va algoritmik ishlab chiqarishlarning ta'lim jarayonidagi o‘rni asoslab berilgan. Kriptografik masalalarni o‘rganishda o‘quvchilarning mantiqiy tafakkurini rivojlantirish, algoritmik madaniyatini yanada amaliy qo‘llash ko‘rinishida muhim ahamiyat kasb etishi ko‘rsatib o‘tilgan. Kriptografiyani o‘qitishda ta'limiy yordamni yuklashdan yuklashning didaktik tahlilni o‘rnatish. Interaktiv vosita yordamida tajriba algoritmlarini vizual modellashtirish, o‘tkazish va o‘quvchilarning mustaqil ta'limini ta'minlash omili sifatida qaraladi. Tadqiqot asosidagi kriptografik bilimlarni o‘qitish metodikasini ta'minlashga oid ilmiy-amaliy tavsiyalar berilgan.

Kalit so‘zlar: aqlli tizimlar, sun’iy intellekt, kiberfizik, axborot xavfsizligi, modul arifmetikasi.

Kirish:

Zamonaviy raqamli texnologiyalar taraqqiyoti axborot xavfsizligi masalasini dolzarb muammolardan biriga aylantirdi. Ayniqsa, turli sohalarda axborot almashinuvi, elektron imzo, onlayn tranzaksiyalar va raqamli identifikatsiya kabi xizmatlarning keng qo‘llanilishi kriptografiyaning o‘rni va ahamiyatini orttirmoqda. Raqamli texnologiyalar shu qadar shiddat bilan rivojlanmoqdaki, inson turmush tarzi va hatto tafakkurini ham butunlay o‘zgartirib yubormoqda. Endilikda, bu texnologiyalarni kundalik ishlarda, ish o‘rnida va ishlab chiqarishda qo‘llanilishi insoniyatni to‘rtinchi sanoat inqilobiga olib keldi. Bu sanoat inqilobi ishlab

chiqarishni aqlli tizimlar, sun'iy intellekt, kiberfizik texnologiyalarga asoslangan butunlay avtomatlashtirilgan tizimga o'tish deganidir. Ushbu sanoat inqilobining mahsuli bo'lgan texnologiyalar raqamli iqtisodiyotni ham rivojlantirishga asos bo'lib hisoblanadi. Rivojlangan raqamli iqtisodiyot esa, o'z navbatida davlat taraqqiyotini belgilab beradi. O'z taraqqiyot yo'lini tanlagan jamiyatimiz uchun raqamli bilimlarga, tafakkurga ega, strategik fikrlay oladigan [1], zamonaviy bilim va tajribalar, milliy va umumbashariy qadriyatlar asosida mustaqil va mantiqiy fikrlaydigan yoshlami tarbiyalash [1] ustuvor yo'nalishlardan biridir. Raqamli dunyo talablariga javob bera oladigan yoshlar qanday bilim va malakalarga ega bo'llishi kerak degan masala butun dunyo oldidagi dolzarb masaladir, chunki, jahonda raqamli texnologiyalardan nafaqat foydalanuvchi, balki ishlab chiqaruvchi tomonidan ham yuqori malakali mutaxassislarga talab juda katta.

Shu bois, bugungi kunda axborot texnologiyalari, kompyuter injiniringi va matematika fanlari bilan integratsiyalashgan holda **kriptografik algoritmlarni o'rgatish** – ta'lim tizimining muhim yo'nalishlaridan biriga aylandi. Ushbu maqolada kriptografik algoritmlarning **matematik va algoritmik asoslari**, ularni **ta'lim jarayonida o'qitish metodikasi** hamda **ta'limiy dasturiy vositalar yordamida tushuntirish usullari** tahlil qilinadi.

Mavzuga oid adabiyotlarning tahlili (Literature reviyew)

Kriptologiya(grekchada kryptos-"sirli" va logos-"xabar") deganda aloqa xavfsizligi haqidagi fan tushuniladi. U aloqa kanallari orqali axborotning xavfsizligini ta'minlab saqlash hamda uzatish tizimlarini yaratish va tahlillash to'g'risidagi fandir. Kriptologiyaikki ilmiy irmoqqa ajraladi. Bular kriptografiya va kriptotahlildir.[2] Dastlabki kriptografiya davriga oid shifrlar haqida gap borganda Yevropa fani tarixidan o'rin olgan Plutarx, Aristotel (miloddan avvalgi IVasr), Yuliy Sezar (miloddan avvalgi 100-44 yy.), R.Bekon (1214-1294 yy.) shifrlarini aytib o'tish joiz [3-6].

Axborot xavfsizligining zamonaviy yo'nalishlaridan biri sifatida kriptografiya fanining o'rganilishi so'nggi yillarda ilmiy va pedagogik nuqtai nazardan dolzarb mavzuga aylangan. Ushbu soha bo'yicha xorijiy va mahalliy adabiyotlar mazmunan turlicha yondashuvlarni o'z ichiga olgan bo'lsa-da, ularning umumiy yo'nalishi

kriptografik algoritmlarning matematik asoslarini o‘rganish, ularni dasturlash tilida realisatsiya qilish hamda o‘quv jarayoniga tatbiq etishga qaratilgan.

Xususan, Menezes, van Oorschot va Vanstone tomonidan yaratilgan “Applied Cryptography” qo‘llanmasida kriptografik tizimlarning nazariy poydevori, matematik modeli hamda ularning zamonaviy IT infratuzilmadagi roli yoritilgan. Asarda algoritmlarning tahliliy ifodasi bilan bir qatorda, xavfsizlik darajasi, kalitlar uzunligi va murakkablik nazariyasi bo‘yicha fundamental tushunchalar asoslangan. Ushbu ish nazariy jihatdan boy manba bo‘lib, o‘qitish strategiyalarini ishlab chiqishda muhim ilmiy asos vazifasini o‘taydi.

W. Stallings tomonidan yozilgan “Cryptography and Network Security” nomli asarda esa algoritmlarning amaliy tomoniga e’tibor qaratilgan. Muallif ma’lumotlarni shifrlash va autentifikatsiyalash algoritmlarining tuzilmasini batafsil ochib bergan. Bu manbadan o‘qitish jarayonida algoritmlarning ishlash mexanizmini bosqichma-bosqich tushuntirish uchun foydalanish mumkin.

Yuqoridagi tahlildan kelib chiqadiki, mavjud adabiyotlar kriptografiyaning nazariy va amaliy jihatlarini yoritish bilan shug‘ullangan, biroq ta’lim tizimiga tatbiq qilish imkoniyatlarini to‘liq ochib berilmagan. Shu bois, ushbu adabiyotlar negizida yangi didaktik yondashuvlar ishlab chiqish, metodik qo‘llanmalar yaratish va o‘quv jarayonini interaktiv platformalarga asoslash muhim vazifa sanaladi.

Tadqiqot metodologiyasi (Research Methodology)

Kriptografik algoritmlar kuchli matematik asosga ega bo‘lib, quyidagi sohalarga tayanadi:

- **Modul arifmetikasi** – kriptografiyada ko‘pincha modul bo‘yicha bo‘lish, ko‘paytirish va eksponenta kabi operatsiyalar qo‘llaniladi (masalan, RSA algoritmi).
- **Son nazariyasi** – tub sonlar, Eylor funksiyasi, Fermat va Euler teoremalari orqali maxfiy kalitlar generatsiyasi amalga oshiriladi.
- **Diskret logarifmlar** – Diffie-Hellman va ElGamal kabi algoritmlarning matematik asosini tashkil etadi.
- **Matematik mantiq va guruhlar nazariyasi** – algoritmik jarayonlarning izchil tuzilishini ta’minlaydi.

Mazkur matematik bilimlar o‘quvchilarda abstrakt fikrlashni shakllantirish bilan birga, ularni real hayotdagi muammolarni hal qilishga tayyorlaydi. Kriptografik algoritmlar o‘z algoritmik strukturasi bilan turli fanlar kesishmasida joylashgan bo‘lib, ularni o‘rganish uchun:

- **Blok-sxemalar** yordamida vizual yondashuv;
- **Psevdokod** asosida algoritmni tahlil qilish;
- **Soddalashtirilgan o‘quv versiyalari** orqali murakkab algoritmlarning mohiyatini tushuntirish;

katta ahamiyatga ega. Masalan, RSA algoritmini o‘rgatishda oddiy sonlar ustida kalit generatsiyasi, shifrlash va deshifrlash bosqichlari o‘quvchilar tomonidan mustaqil bajarilishi mumkin.

Ta’lim jarayonida kriptografik algoritmlarni **mantiqiy, matematik va algoritmik fikrlashni rivojlantirish** vositasi sifatida qo‘llash pedagogik maqsadlarga xizmat qiladi. Kriptografik algoritmlarni o‘qitishda interaktiv dasturiy vositalardan foydalanish o‘quvchilarning bilim olish jarayonini soddalashtiradi. Bu vositalar orqali o‘quvchilarda, Amaliy ko‘nikmalar, mustaqil fikrlash, muammoni algoritmik yechish kompetensiyalari shakllanadi.

Tajriba va metodik tavsiyalar

Tajriba shuni ko‘rsatadiki, kriptografiya elementlarini o‘rgatishda quyidagi metodik yondashuvlar yuqori samaradorlik beradi:

- **Problemali ta’lim**: O‘quvchiga muammo qo‘yiladi (masalan, maxfiy xabarni shifrlash), va u algoritmik yechimni topadi.
- **Loyiha asosida ta’lim**: O‘quvchilar mustaqil yoki guruhda kichik kriptografik tizim yaratadi.
- **Bosqichma-bosqich murakkablashtirish**: Dastlab sodda algoritmlar (Caesar), keyinchalik murakkabrog‘i (RSA) o‘rgatiladi.

Xulosa

Kriptografik algoritmlarni o‘rganish va o‘rgatish, nafaqat IT sohasiga qiziqqan yoshlarni tayyorlash, balki ularning matematik va mantiqiy fikrlashini rivojlantirish,

axborot xavfsizligining asosiy tamoyillarini tushunish, hamda dasturlash kompetensiyalarini oshirishda muhim rol o‘ynaydi.

Ushbu maqolada ko‘rib chiqilgan matematik asoslar, algoritmik strukturani tushuntirish metodikasi, va ta’limiy dasturiy vositalardan foydalanish bo‘yicha tavsiyalar O‘zbekiston Milliy universiteti kabi oliy ta’lim muassasalarida bu sohani o‘qitishda samarali bo‘lishi mumkin.

Foydalanilgan adabiyotlar (namunaviy ro‘yxat)

1. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*. CRC Press.
2. Stallings, W. (2017). *Cryptography and Network Security*. Pearson Education.
3. Гусев, В. Б. (2020). *Криптография для начинающих*. Москва: БХВ-Петербург.
4. Namozov, O., Raximov, A. (2021). *Dasturlash asoslari va algoritmik tafakkur*. Toshkent.
5. O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi. (2023). *Axborot xavfsizligi bo‘yicha o‘quv dasturi*.
6. X.E.XOLMIRZAYEV, M.N.IKROMOVA, M.M.BAHROMOVA - ALGORITMIK TILLAR VA DASTURLASH OlQUV QO'LLANMA Toshkent 2023
7. Akbarov Davlatali Yegitaliyevich, XasanovPo‘latFattoxovich, Xasanov Xislat Po‘latovich, Axmedova Oydin Po‘latovna, Xolimtayeva Iqbol Ubaydullayevna“Kriptografiyaning matematik asoslari”.O‘quv qo‘llanma. – Toshkent. TATU.2018 –208bet