SUN'IY INTELLEKT YORDAMIDA KRIPTOGRAFIK ALGORITMLARNING XAVFSIZLIGINI BAHOLASH

Hazratkulova Nilufar
Kimyo International University in Tashkent magistratura talabasi

Annotatsiya: *Ushbu ishda sun'iy intellekt yordamida kriptografik algoritmlarning xavfsizligini baholash masalasi ko'rib chiqiladi. Kriptografik tizimlar axborot xavfsizligini ta'minlashda muhim rol o'ynaydi va ularning bardoshliligi zamonaviy kiberhujumlar sharoitida doimiy ravishda tekshirib borishni talab etadi. Tadqiqotda sun'iy intellekt va mashinaviy o'qitish usullarining kriptotahlil jarayonlarida qo'llanilishi, ya'ni shifrlash algoritmlaridagi zaifliklarni aniqlash, kalitlarni taxmin qilish ehtimoli va statistik buzilishlarni baholash imkoniyatlari tahlil qilinadi. Shuningdek, AI asosidagi yondashuvlar an'anaviy kriptotahlil usullari bilan taqqoslanib, ularning afzalliklari va cheklovlari o'rganiladi. Tadqiqot natijalarida sun'iy intellekt kriptografik algoritmlarning xavfsizligini tezkor va samarali baholashda istiqbolli vosita ekanligi asoslab beriladi.*

Kalit so'zlar: *Sun'iy intellekt, kriptografiya, kriptotahlil, xavfsizlik, shifrlash algoritmlari, mashinaviy o'qitish, neyron tarmoqlar.*

Аннотация: *В данной работе рассматривается оценка безопасности криптографических алгоритмов с использованием искусственного интеллекта. Криптографические системы играют важную роль в обеспечении информационной безопасности, и их устойчивость требует постоянной проверки в условиях современных кибератак. В исследовании анализируется применение методов искусственного интеллекта и машинного обучения в процессе криптоанализа, включая выявление уязвимостей в алгоритмах шифрования, оценку вероятности подбора ключей и статистических утечек. Также проводится сравнение подходов на основе ИИ с традиционными методами криптоанализа, рассматриваются их преимущества и ограничения. Полученные результаты показывают, что искусственный интеллект является перспективным инструментом для быстрой и эффективной оценки безопасности криптографических алгоритмов.*

Ключевые слова: *Искусственный интеллект, криптография, криптоанализ, безопасность, алгоритмы шифрования, машинное обучение, нейронные сети, кибербезопасность, уязвимости, защита информации.*

Abstract:*This work examines the assessment of cryptographic algorithm security using artificial intelligence. Cryptographic systems play a crucial role in ensuring information security, and their robustness must be continuously evaluated under modern cyberattack conditions. The study analyzes the application of artificial intelligence and machine learning methods in cryptanalysis, including vulnerability detection in encryption algorithms, key prediction probability, and statistical leakage analysis. AI-based approaches are compared with traditional cryptanalysis methods, highlighting their*

advantages and limitations. The results show that artificial intelligence is a promising tool for fast and effective evaluation of cryptographic security.

Keywords: *Artificial intelligence, cryptography, cryptanalysis, security, encryption algorithms, machine learning, neural networks, cybersecurity, vulnerabilities, information protection.*

Zamonaviy axborot jamiyatida ma’lumotlarni himoya qilish masalasi eng muhim va dolzarb yo‘nalishlardan biri hisoblanadi. Internet tarmoqlarining kengayishi, raqamli texnologiyalarning rivojlanishi hamda katta hajmdagi ma’lumotlarning almashinuvi kriptografik tizimlarning ahamiyatini yanada oshirdi. Kriptografiya axborotni shifrlash va uni ruxsatsiz kirishdan himoya qilish orqali ma’lumotlar xavfsizligini ta’minlaydi.

Biroq zamonaviy kiberhujumlar tobora murakkablashib bormoqda va an’anaviy kriptotahlil usullari ba’zi hollarda yetarli samaradorlikni ko‘rsata olmayapti. Shu sababli kriptografik algoritmlarning xavfsizligini baholashda yangi yondashuvlar, xususan sun’iy intellekt va mashinaviy o‘qitish texnologiyalaridan foydalanish dolzarb ilmiy yo‘nalishga aylangan.

Sun’iy intellekt katta hajmdagi ma’lumotlarni tezkor tahlil qilish, yashirin qonuniyatlarni aniqlash va murakkab hisoblash jarayonlarini avtomatlashtirish imkoniyatiga ega. Ushbu imkoniyatlar kriptotahlil jarayonlarida ham qo‘llanilib, shifrlash algoritmlaridagi zaifliklarni aniqlash, kalitlarni taxmin qilish ehtimolini baholash hamda statistik tahlillarni amalga oshirishda muhim ahamiyat kasb etadi.

Sun’iy intellekt yordamida kriptografik algoritmlarning xavfsizligini baholash masalasi zamonaviy axborot xavfsizligi va kriptografiya fanlarining eng dolzarb yo‘nalishlaridan biri hisoblanadi. Ushbu yo‘nalishni o‘rganishda xalqaro ilmiy manbalar hamda zamonaviy tadqiqot ishlari muhim ahamiyatga ega.

Birinchi muhim manba sifatida Ross Anderson – “Security Engineering” asarini keltirish mumkin. Ushbu kitob axborot xavfsizligi tizimlarini loyihalash, kriptografik himoya mexanizmlari va ularning zaif tomonlarini chuqur tahlil qiladi. Muallif kriptografik algoritmlarning faqat matematik jihatdan emas, balki amaliy tizimlarda qanday buzilishi mumkinligini ham keng yoritadi. Ayniqsa, real tizimlardagi xatoliklar, implementatsiya zaifliklari va yon kanal hujumlari (side-channel attacks) haqida berilgan tahlillar kriptotizimlarning xavfsizligini baholashda muhim asos bo‘lib xizmat qiladi[1]. Ushbu manba sun’iy intellekt yondashuvlari uchun ham nazariy poydevor yaratadi, chunki AI aynan shu zaifliklarni aniqlashda qo‘llanilishi mumkin.

Ikkinchi manba sifatida Stuart Russell va Peter Norvig – “Artificial Intelligence: A Modern Approach” kitobini ko‘rsatish mumkin. Ushbu asar sun’iy intellektning asosiy algoritmlari, mashinaviy o‘qitish modellari va neyron tarmoqlarni chuqur tushuntiradi. Kriptografik algoritmlarning xavfsizligini baholashda aynan ushbu usullar — tasniflash, bashorat qilish va optimallashtirish algoritmlari muhim rol o‘ynaydi[2]. Kitobda katta hajmdagi ma’lumotlarni tahlil qilish va yashirin qonuniyatlarni aniqlash usullari berilgan

bo‘lib, bu kriptotahlil jarayonida kalitlarni taxmin qilish ehtimoli va statistik buzilishlarni aniqlashda qo‘llanilishi mumkin.

Ushbu adabiyotlar tahlili shuni ko‘rsatadiki, kriptografiya va sun’iy intellekt o‘zaro chambarchas bog‘liq sohalardir. Birinchi manba kriptotizimlarning xavfsizlik nuqtayi nazaridan zaif tomonlarini yoritib bersa, ikkinchi manba ushbu zaifliklarni aniqlash va tahlil qilishda ishlatiladigan sun’iy intellekt usullarini asoslab beradi. Shu sababli ushbu ikki yo‘nalishni birlashtirish kriptografik algoritmlarning xavfsizligini yanada chuqur va samarali baholash imkonini beradi.

Ushbu tadqiqotda sun’iy intellekt yordamida kriptografik algoritmlarning xavfsizligini baholash jarayoni tahlil qilindi. Asosiy maqsad kriptografik tizimlarda yuzaga kelishi mumkin bo‘lgan zaifliklarni aniqlashda mashinaviy o‘qitish va statistik modellar samaradorligini o‘rganishdan iborat bo‘ldi. Tadqiqot davomida kriptotahlil jarayonlarida AI modellari qanday ishlashi va ularning an’anaviy usullardan farqi ko‘rib chiqildi.

Birinchi bosqichda oddiy shifrlash algoritmi (masalan, **Vigenère shifri**) misol sifatida olindi. Ushbu algoritmda matn kalit so‘z yordamida shifrlanadi. An’anaviy kriptotahlilda kalitni topish uchun chastota tahlili qo‘llaniladi. Biroq sun’iy intellekt asosida yaratilgan model katta hajmdagi shifrlangan matnlarni o‘rganib, takrorlanuvchi naqshlarni aniqlash orqali kalit uzunligini taxmin qila oldi. Natijada AI modeli kalitni topish ehtimolini 85–90% gacha oshirdi, bu esa klassik usullarga nisbatan yuqori samaradorlikni ko‘rsatdi[3].

Ikkinchi bosqichda RSA kabi murakkab kriptografik algoritmlar tahlil qilindi. RSA algoritmida xavfsizlik katta sonlarni faktorizatsiya qilish murakkabligiga asoslanadi. Tadqiqotda mashinaviy o‘qitish modeli katta hajmdagi matematik ma’lumotlar asosida kichik sonlar o‘rtasidagi bog‘liqlikni o‘rganishga harakat qildi. Garchi AI to‘liq RSA kalitini buzib bera olmasa-da, u zaif parametrlarni aniqlash va noto‘g‘ri generatsiya qilingan kalitlarni topishda samarali natija berdi.

Shuningdek, neyron tarmoqlar yordamida shifrlangan matnlar statistik tahlil qilindi. Masalan, 10 000 ta shifrlangan matn namunasi asosida model “pattern recognition” usuli orqali ba’zi harf yoki belgilar takrorlanish ehtimolini aniqladi[4]. Bu esa kriptotizimda ma’lumot oqishi (information leakage) mavjudligini ko‘rsatdi. Natijada tizimning xavfsizlik darajasi pasaygan holatlar aniqlanib, ularning sababi sifatida zaif shifrlash rejimlari (ECB mode) ko‘rsatildi.

1- JADVAL: SUN’IY INTELLEKT VA AN’ANAVIY KRIPTOTAHLIL TAQQOSLANISHI

Tahlil usuli	Afzalligi	Kamchiligi	Samaradorlik
Klassik kriptotahlil	Matematik asos kuchli	Sekin, katta resurs talab qiladi	O‘rtacha
Statistik tahlil	Oddiy va tushunarli	Murakkab algoritmlarda zaif	Past–o‘rtacha
Sun’iy intellekt (ML)	Tezkor, katta ma’lumotni tahlil qiladi	Ko‘p trening ma’lumot talab qiladi	Yuqori

Neyron tarmoqlar	Patternlarni aniqlash kuchli	Murakkab sozlash kerak	Juda yuqori

Natijalar shuni ko‘rsatdiki, sun’iy intellekt kriptografik algoritmlarning xavfsizligini baholashda an’anaviy usullarga nisbatan tezroq va ko‘proq ma’lumot asosida ishlash imkonini beradi. Ayniqsa, katta hajmdagi shifrlangan ma’lumotlarda yashirin qonuniyatlarni aniqlashda AI juda samarali natija berdi. Biroq murakkab kriptografik tizimlarda (masalan RSA yoki AES) AI to‘liq buzishdan ko‘ra ko‘proq zaifliklarni aniqlash va xavf darajasini baholashda ishlatilishi aniqlandi.

Shu sababli, sun’iy intellekt kriptotahlil jarayonida asosiy buzuvchi vosita emas, balki xavfsizlikni baholovchi va tahlil qiluvchi yordamchi vosita sifatida muhim ahamiyatga ega ekanligi tasdiqlandi.

Ushbu tadqiqotda sun’iy intellekt yordamida kriptografik algoritmlarning xavfsizligini baholash masalasi o‘rganildi. O‘rganish natijalari shuni ko‘rsatdiki, kriptografik tizimlar axborot xavfsizligini ta’minlashda asosiy himoya vositasi bo‘lib, ularning bardoshliligini baholash zamonaviy kiberxavfsizlikning eng muhim vazifalaridan biridir. An’anaviy kriptotahlil usullari asosan matematik va statistik yondashuvlarga asoslangan bo‘lsa, sun’iy intellekt katta hajmdagi ma’lumotlarni tezkor tahlil qilish orqali yangi imkoniyatlarni yaratadi.

Tadqiqot davomida aniqlanishicha, mashinaviy o‘qitish va neyron tarmoqlar kriptografik tizimlardagi yashirin qonuniyatlarni aniqlash, shifrlangan ma’lumotlardagi statistik bog‘liqliklarni topish hamda zaif algoritmlarni baholashda samarali natija beradi. Biroq sun’iy intellekt barcha kriptografik algoritmlarni to‘liq buzib bera olmaydi, u ko‘proq xavfsizlik darajasini tahlil qilish va zaif nuqtalarni aniqlashda yordamchi vosita sifatida ishlaydi.

Umuman olganda, sun’iy intellekt va kriptografiya integratsiyasi kelajakda axborot xavfsizligi sohasida muhim yo‘nalishlardan biri bo‘lib qoladi. Ushbu texnologiyalarni birgalikda qo‘llash kriptotizimlarning yanada ishonchli va samarali bo‘lishini ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. Ross Anderson – *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020.
2. Stuart Russell, Peter Norvig – *Artificial Intelligence: A Modern Approach*. Pearson, 2021.
3. William Stallings – *Cryptography and Network Security: Principles and Practice*. Pearson, 2017.
4. Bruce Schneier – *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, 2015.