AXBOROT TEXNOLOGIYALARI SOHASIDA QO‘LLANILADIGAN ZAMONAVIY KRIPTOGRAFIK ALGORITMLAR TAHLILI

Olimov Iskandar Salimboyevich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
iskandar.olimov@mail.com
Karimov Abduqodir Abdusalomovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
karimovabduqodir041@gmail.com
Bo‘riyev Yusuf Absamat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Soccersppt@gmail.com

Annotatsiya.

Ushbu maqolada axborot texnologiyalari sohasida qo‘llaniladigan zamonaviy kriptografik algoritmlar tasnifi keltirilgan bo‘lib, undan tashqari kriptografik algoritmlar tahlili keltirilgan.

Kalit so‘zlar: AES, RC4, RSA (Rivest-Shamir-Adleman), ChaCha20, Gibrid kriptotizimlar.

Annotation.

This article presents the classification of modern cryptographic algorithms used in the field of information technologies, as well as the analysis of cryptographic algorithms.

Key words: AES, RC4, RSA (Rivest-Shamir-Adleman), ChaCha20, Hybrid cryptosystems.

Аннотация.

В данной статье представлена классификация современных криптографических алгоритмов, используемых в области информационных технологий, а также анализ криптографических алгоритмов.

Ключевые слова: AES, RC4, RSA (Rivest-Shamir-Adleman), ChaCha20, гибридные криптосистемы.

Axborot texnologiyalari sohasida qo‘llaniladigan zamonaviy kriptografik algoritmlarni funksionalligi va foydalaniladigan kalitlar turiga qarab bir necha toifalarga bo‘lish mumkin va quyida batafsil tasniflangan:

Simmetrik kriptografiya. Simmetrik algoritmlarida shifrlash va shifrni ochishda bir xil kalitdan foydaniladi. Ular odatda tezroq va katta hajmdagi ma'lumotlarni shifrlash uchun mos keladi. Zamonaviy simmetrik algoritmlarni quyidagilarga bo‘linadi [1,3,4]:

Mashhur blokli shifrlarga quyidagilar kiradi:

– AES
– 3DES
– Blowfish

– Twofish
– SM4

Mashhur oqim shifrlariga quyidagilar kiradi:

– RC4
– Salsa20
– ChaCha20

Ochiq kalitli shifrlash algoritmlari. Ochiq kalitli algoritmlar shifrlash uchun ochiq kalit va shifrni ochish uchun shaxsiy kalitdan foydaniladi. Ushbu algoritmlar hisoblash qimmati, ko‘pincha kalit almashinuvi va raqamli imzolar uchun ishlatiladi. Umumiy assimetrik algoritmlarga quyidagilar kiradi:

– RSA (Rivest-Shamir-Adleman)
– ECC (elliptik egri kriptografiya)
– DSA (raqamli imzo algoritmi)
– Diffie-Hellman (kalit almashinuvi uchun)

Zamonaviy xesh funksiyalarga quyidagilar kiradi:

– SHA-256 (Secure Hash Algoritm 2).
– SHA-3
– MD5 (Message Digest Algoritm 5)
– RIPEMD (RACE Integrity Primitives Evaluation Message Digest).

Gibrid kriptotizimlar. Gibrid tizimlar simmetrik shifrlash samaradorligini assimetrik shifrlash xavfsizligi bilan birlashtiradi. Odatda, simmetrik kalitni shifrlash uchun assimetrik algoritmdan foydalaniladi, keyinchalik u haqiqiy xabarni shifrlash uchun ishlatiladi. Misol sifatida RSA va AES kombinatsiyasidan foydalaish mumkin [2,4].

Elektron raqamli imzolar. Raqamli imzolar autentifikatsiya va yaxlitlikni ta'minlaydi. Ular assimetrik kriptografiyadan foydalanadilar. Umumiy raqamli imzo algoritmlariga quyidagilar kiradi:

– RSA
– DSA
– ECDSA (elliptik egri raqamli imzo algoritmi).

Kalit almashinuvi algoritmlari. Kalit almashinuvi algoritmlari kriptografik kalitlarni umumiy kanal orqali xavfsiz almashish imkonini beradi. Bunga misol sifatida:

– Diffie-Hellman
– ECDH (elliptik egri Diffie-Hellman).

Kvant kriptografiya. Kvant hisoblashning paydo bo‘lishi va rivojlanishi o‘znavbatida, an'anaviy kriptografik algoritmlarni soya ostida qolishiga sabab bo‘lmoqda [1,3].

Zamonaviy kriptografik algoritmlar bir qator xususiyatlari bo‘yicha tahlili amalga oshiriladi.

1-jadval

Ochiq kalitli algoritmlarining solishtirma tahlili

Algoritm oilalari	Kripto tizim	Xavfsizlik darajasi (bit)				Foydali	Kamchiligi
		80	128	192	256		
Yetarli kata sonni tub ko‘paytiruvchiga ajratish(TKA) murakkabligiga asoslanadi	RSA	1024	3072	7680	15360	Faqat qabul qiluvchi o‘zining maxfiy kaliti bilan xabarni o‘qiy oladi	Maxfiy kalit usullari muhim va tezroq ochiq kalitdan foydalanishidan qaraganda

Xarakteristikasi yetarli kattabo‘lgan chekli maydonda diskret logarifmlash (DL)	El-gamal	1024	3072	7680	15360	Bir xildagi ochiq matn uchun harli shifr ma’lumot to‘g‘ri keladi	Sekinroq tezlik talab etadi shifrlash sharayoni uchun
Elliptik egri chiziq (EECh) nuqtalari asosida sanab o‘tilgan mavjud murakkabliklarni kombinatsiyalashga asoslangan	EECh	160	256	384	512	Kalit uzunligi qisqa va shuning hisobiga tezroq va undan tashqari kompyuterdan katta xarakteristika talab etmidi	Juda qimmat

2.5-jadval

Ochiq kalitli va simmetrik shifrlash algoritmlarining solishtirma tahlili

Xususiyat	*3DES*	*AES*	*RSA*	*El-gamal*	*EECH*
Yaratuvchilar	IBM	Vincent Rijmen	Rivest, Shamir, Adleman	Taher Elgamal	Miller
Yaratilgan yil	1998-yil	1998-yil	1977-yil	1985-yil	1985-yil
Shifrlash turi	Simmetrik	Simmetrik	Asimmetrik	Asimmetrik	Asimmetrik
Raundlar	48	10,12,14 kalit o‘lchamiga	Raund yo‘q	Raund yo‘q	Raund yo‘q
Kalit uzunligi	168,112 yoki 56	128,192,256	1024 dan 4096	>1024	>1024
Blok uzunligi	64 bits	128 bits	Kalitni o‘lchamiga bog‘liq	Kalitni o‘lchamiga bog‘liq	Kalitni o‘lchamiga bog‘liq
Tarmoq turi	Feystal	Feystal emas	Umumiy	Umumiy	Umumiy
Tezlik	DES ga qaraganda tez	3DES ga qaraganda tez	Juda tez	Juda tez	Juda tez
Xavfsizligi	Brute force hujumi	Ishonchli	Xavfsiz	Xavfsiz	Xavfsiz

Javdaldan ko‘rinadiki simmetrik va ochiq kalitli shifrlash algoritmlarining bir biridan farqli tamonlari mavjudligiga va shu bilan bir qatorda ularning ustun va zaif tomonlari ko‘rib chiqilgan.

Xulosa

Axborot texnologiyalari sohasi bugungi kunda tez sur'atlar bilan rivojlanib bormoqda. Ushbu rivojlanish bir nechta asosiy yo‘nalishlarda sun'iy intellekt va mashinani o‘rganish, bulutli hisoblash texnologiyalari, blokcheyn texnologiyalari, kiberxavfsizlik, buyumlar Interneti kabilarda kuzatilmoqda. Axborot texnologiyalari sohasi rivojlanishi iqtisodiyotni o‘sishiga, samaradorlikni oshirishga va kundalik hayotimizni osonlashtirishga xizmat qilish bilan birga ular o’rtasida axborot almashinish jarayonida ularda foydaniladigan kriptografik algoritmlarni e’tibordan chetda qoldirmaslikni talab etmoqda. Ushbu maqolada axborot texnologiyalari

sohasidagi zamonaviy kriptografik algoritmlar haqida ma'lumot berilgan bo'lib, undan tashqari ularni bir qator xususiyatlari bo'yicha tahlili ishlab chiqilgan.

Foydalangan adabiyotlar

1. Kiberxavfsizlik asoslari. S.K.Ganiyev,A.A.Ganiyev, Z.T.Xudoyqulov 2020 yil 4 iyul – sonli bayonnoma.

2. Li, Y., Wu, X., & Bai, G. (2018, October). Implementation of SM4 Algorithm based on Asynchronous Dual-Rail Low-power Design. In *2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)* (pp. 1-3). IEEE.

3. Choudhary A. A Short Survey on Comparative Study of Modern Cryptography Approach //International Conference on Deep Learning, Artificial Intelligence and Robotics. – Cham : Springer Nature Switzerland, 2023. – С. 33-48.

4. Salami Y., Khajevand V., Zeinali E. Cryptographic algorithms: a review of the literature, weaknesses and open challenges //J. Comput. Robot. – 2023. – Т. 16. – №. 2. – С. 46-56.

5. U.M.Yarlakabov Didactic Ways of Forming Students' Technical Thinking.- Eastern European Scientific Journal, 2018 - journale.auris-verlag.de

6. Sharipov Sanjar. Vocational orientation through the development of mathematical competences in the students of technical higher education institutions. CURRENT RESEARCH JOURNAL OF PEDAGOGICS. 3. No. 06 (2022). 58-64. https://doi.org/10.37547/pedagogics-crjp-03-06-10

7. Nadirova-Kazan, H. (2023, November). EXPLORING THE CONTENT OF MEDIA LITERACY: A COMPREHENSIVE REVIEW. In International Scientific and Current Research Conferences (pp. 107-110).

8. Norqo'ziyev, Q., Aynakulov, T., Mahkamov, S., & Sodiqov, D. (2024). IMPLEMENTING MOBILE ROBOT WALKING PATH CONTROL AND TRACKING IN C# WINDOWS FORM APPLICATION. International Journal of scientific and Applied Research, 1(3), 95-99.

9. Ikrom Kulanov, Sneha Latha, Azizbek Uzakboyev, Shakhzoda Burkhanova. Effect of gyrotactic microorganisms on electrically conducting carreau nanofluid flow along an exponentially stretching surface in the presence of chemical reaction. Problems in the textile and light industry in the context of integration of science and industry and ways to solve them: ptlicisiws-2.4–5 may 2023.Namangan, Uzbekistan.AIP Conf. Proc. 3045, 030066 (2024). https://doi.org/10.1063/5.0197498

10. Sanjar Sobirovich Sharipov. IMPLEMENTATION OF SPECIAL AND GENERAL PROFESSIONAL INTEGRATION AS A PEDAGOGICAL PROBLEM Scientific Bulletin of Namangan State University.2020. 2-8. 364-370-p.

11. Abdug'aniyev, B. (2020). Анализ инструментов расследования цифровой криминалистика. Архив Научных Публикаций JSPI.