C# MUHITIDA AES ALGORITMI YORDAMIDA MA’LUMOTLARNI SHIFRLASH VA TIKLASH TIZIMINI YARATISH

Shervayev Abdurahmon Maxammadjon o‘g‘li
Guliston davlat universiteti
Axborot texnologiyalari va fizika-matematika fakulteti, 3-bosqich talabasi
E-mail: abdurahmonsherboyev17@gmail.com

*DOI: **https://doi.org/10.5281/zenodo.20215892***

Annotatsiya: *Ushbu maqolada C# dasturlash muhiti yordamida AES algoritmi asosida ma’lumotlarni shifrlash va deshifrlash tizimini yaratish masalasi ko‘rib chiqiladi. Zamonaviy axborot texnologiyalari rivojlanishi sharoitida ma’lumotlar xavfsizligini ta’minlash muhim vazifalardan biri hisoblanadi. Shu sababli maqolada simmetrik kriptografik algoritmlardan biri bo‘lgan, AES algoritmining ishlash prinsipi, afzalliklari va qo‘llanilish sohalari tahlil qilinadi. Amaliy qismda C# dasturlash tilida Windows Forms muhitida foydalanuvchi uchun qulay interfeysga ega bo‘lgan dasturiy vosita ishlab chiqildi. Ushbu dastur orqali foydalanuvchi matnli ma’lumotlarni maxfiy kalit yordamida shifrlashi hamda ularni qayta tiklashi mumkin. Dasturda AES algoritmi asosida shifrlash va deshifrlash jarayonlari implementatsiya qilinib, ularning samaradorligi va ishonchliligi ta’minlandi.Maqolani yozish natijasida ishlab chiqilgan dasturiy ta’minot ma’lumotlarni himoyalashda samarali vosita sifatida xizmat qilishi mumkin. Mazkur ish axborot xavfsizligi sohasida zamonaviy kriptografik usullardan foydalanishning amaliy ahamiyatini ko‘rsatadi.*

Kalit so‘zlar: *AES algoritmi, C# dasturlash tili, kriptografiya, ma’lumotlarni shifrlash, deshifrlash, axborot xavfsizligi, simmetrik shifrlash, Windows Forms, dasturiy ta’minot, maxfiy kalit.*

Аннотация: *В данной статье рассматривается вопрос создания системы шифрования и дешифрования данных на основе алгоритма AES с использованием среды программирования C#. Обеспечение безопасности данных является одной из важных задач в контексте развития современных информационных технологий. Поэтому в статье анализируются принцип работы, преимущества и области применения алгоритма AES, являющегося одним из симметричных криптографических алгоритмов. В практической части разработан программный инструмент с удобным пользовательским интерфейсом на языке программирования C# в среде Windows Forms. С помощью этой программы пользователь*

может шифровать и восстанавливать текстовые данные, используя секретный ключ. В программе реализованы процессы шифрования и дешифрования на основе алгоритма AES, обеспечивающие их эффективность и надежность. Разработанное в результате написания статьи программное обеспечение может служить эффективным инструментом защиты данных. Данная работа демонстрирует практическую значимость использования современных криптографических методов в области информационной безопасности.

Ключевые слова: *алгоритм AES, язык программирования C#, криптография, шифрование данных, дешифрование, информационная безопасность, симметричное шифрование, Windows Forms, программное обеспечение, секретный ключ.*

Abstract*: This article examines the development of a data encryption and decryption system based on the AES algorithm using the C# programming environment. Data security is a key issue in the context of modern information technology development. Therefore, this article analyzes the operating principle, advantages, and applications of the AES algorithm, a symmetric cryptographic algorithm. In the practical section, a software tool with a user-friendly interface is developed in the C# programming language within the Windows Forms environment. This program enables the user to encrypt and decrypt text data using a secret key. The program implements encryption and decryption processes based on the AES algorithm, ensuring their efficiency and reliability. The software developed as a result of this article can serve as an effective data protection tool. This work demonstrates the practical significance of using modern cryptographic methods in the field of information security.*

Keywords: *AES algorithm, C# programming language, cryptography, data encryption, decryption, information security, symmetric encryption, Windows Forms, software, secret key*

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi natijasida turli sohalarda katta hajmdagi ma’lumotlar almashinuvi amalga oshirilmoqda. Shu bilan birga, ma’lumotlarning maxfiyligi, yaxlitligi va ishonchliligini ta’minlash masalasi dolzarb ahamiyat kasb etmoqda. Ayniqsa, internet tarmoqlari orqali uzatilayotgan axborotlarni ruxsatsiz kirishdan himoya qilish zarurati kriptografik usullardan keng foydalanishni talab etadi.

Kriptografiya axborotni himoyalashning muhim vositalaridan biri bo‘lib, u ma’lumotlarni shifrlash va deshifrlash orqali ularning xavfsizligini ta’minlaydi. Zamonaviy kriptografik algoritmlar orasida AES (Advanced Encryption Standard) algoritmi o‘zining yuqori darajadagi ishonchliligi,

tezkorligi va samaradorligi bilan ajralib turadi. Ushbu algoritm simmetrik shifrlash turiga mansub bo‘lib, bir xil kalit yordamida ma’lumotlarni kodlash va qayta tiklash imkonini beradi.

Mazkur maqolaning asosiy maqsadi C# dasturlash muhiti yordamida AES algoritmi asosida ma’lumotlarni shifrlash va deshifrlash tizimini yaratishdan iborat. Ushbu jarayonda Windows Forms texnologiyasi asosida foydalanuvchi uchun qulay interfeysga ega dastur ishlab chiqilib, uning yordamida matnli ma’lumotlarni xavfsiz tarzda himoyalash va tiklash imkoniyati yaratildi.

Maqola ishini yozish vazifalari sifatida AES algoritmining nazariy asoslarini o‘rganish, uni dasturiy jihatdan amalga oshirish hamda ishlab chiqilgan tizimning funksional imkoniyatlarini tahlil qilish belgilandi. Ushbu ish natijalari axborot xavfsizligini ta’minlashda zamonaviy dasturiy vositalardan foydalanishning ahamiyatini ko‘rsatadi.

Kriptografiya axborotni himoyalashning muhim yo‘nalishlaridan biri bo‘lib, u ma’lumotlarni ruxsatsiz kirishdan saqlash, uzatilayotgan axborotning maxfiyligi va yaxlitligini ta’minlashga xizmat qiladi. Kriptografik usullar asosan ikki turga bo‘linadi: simmetrik va assimetrik shifrlash algoritmlari. Simmetrik shifrlash algoritmlarida ma’lumotni shifrlash va deshifrlash uchun bitta umumiy kalitdan foydalaniladi, assimetrik algoritmlarda esa ikki xil – ochiq va yopiq kalitlar qo‘llaniladi.

Simmetrik kriptografik algoritmlar orasida AES (Advanced Encryption Standard) algoritmi keng tarqalgan bo‘lib, u hozirgi kunda eng ishonchli va samarali shifrlash standartlaridan biri hisoblanadi. AES algoritmi 2001-yilda AQShning Milliy standartlar va texnologiyalar instituti (NIST) tomonidan rasmiy standart sifatida qabul qilingan. Ushbu algoritm blokli shifrlash prinsipiga asoslanib, 128 bitli bloklar ustida ishlaydi hamda 128, 192 va 256 bit uzunlikdagi kalitlardan foydalanish imkoniyatiga ega.

AES algoritmi o‘rniga qo‘yish va aralashtirish (substitution-permutation network) tamoyiliga asoslangan bo‘lib, bir nechta iteratsion bosqichlardan (round) iborat. Har bir bosqich quyidagi asosiy amallarni o‘z ichiga oladi: SubBytes (baytlarni o‘zgartirish), ShiftRows (qatorlarni siljitish), MixColumns (ustunlarni aralashtirish) va AddRoundKey (kalit bilan qo‘shish). Ushbu amallar ketma-ket bajarilishi natijasida boshlang‘ich ma’lumot murakkab ko‘rinishga keltiriladi va uni kalitsiz tiklash deyarli imkonsiz bo‘ladi.

AES algoritmining asosiy afzalliklari sifatida uning yuqori tezkorligi, kriptotahlilga chidamliligi va turli platformalarda samarali ishlash imkoniyati keltiriladi. Ayniqsa, katta hajmdagi ma’lumotlarni qayta ishlashda AES algoritmi boshqa ko‘plab algoritmlarga nisbatan ustunlikka ega.

Shu sababli u bank tizimlari, elektron tijorat, ma’lumotlar bazalari va tarmoq xavfsizligi sohalarida keng qo‘llaniladi.

Mazkur ishda AES algoritmining aynan simmetrik xususiyatidan foydalanilib, ma’lumotlarni shifrlash va deshifrlash jarayonlari C# dasturlash muhiti orqali amaliy jihatdan realizatsiya qilindi. Natijada foydalanuvchi kiritgan matnli ma’lumotlar maxfiy kalit yordamida shifrlanib, faqat shu kalit orqali qayta tiklanishi ta’minlandi. Bu esa axborot xavfsizligini ta’minlashda AES algoritmining samaradorligini yana bir bor tasdiqlaydi.

Mazkur ishda AES algoritmi asosida ma’lumotlarni shifrlash va deshifrlash tizimini ishlab chiqish uchun C# dasturlash tili hamda Windows Forms texnologiyasidan foydalanildi. Dastur foydalanuvchi uchun qulay, sodda va intuitiv interfeys asosida loyihalashtirildi.

Dastur interfeysi bir nechta asosiy komponentlardan tashkil topgan. Jumladan, foydalanuvchi tomonidan matn kiritish uchun maxsus maydon (textBoxInput), maxfiy kalitni kiritish uchun maydon (textBoxKey) hamda natijani aks ettirish uchun alohida maydon (textBoxOutput) mavjud. Bundan tashqari, dasturda “Shifrlash” (Encrypt), “Deshifrlash” (Decrypt), “Nusxa olish” (Copy) va “Tozalash” (Clear) kabi boshqaruv tugmalari joriy etilgan.

Dasturda xavfsizlikni oshirish maqsadida kalit kiritish maydonida kiritilayotgan belgilar maxfiy ko‘rinishda, ya’ni yulduzcha (*) belgisi orqali aks ettiriladi. Bu esa foydalanuvchi kiritayotgan maxfiy ma’lumotni tashqi kuzatuvchilardan himoya qilish imkonini beradi.

Dasturiy realizatsiyada AES simmetrik shifrlash algoritmidan foydalanildi. Shifrlash jarayonida foydalanuvchi tomonidan kiritilgan matn va maxfiy kalit asosida ma’lumotlar baytlar ketma-ketligiga o‘tkazilib, maxsus kriptografik o‘zgartirishlar amalga oshiriladi. Natijada ma’lumotlar shifrlangan ko‘rinishga keltiriladi va Base64 formatda foydalanuvchiga taqdim etiladi.

Deshifrlash jarayonida esa aksincha, shifrlangan matn va mos kalit yordamida dastlabki ma’lumot qayta tiklanadi. Agar noto‘g‘ri kalit kiritilsa yoki ma’lumot buzilgan bo‘lsa, dastur foydalanuvchiga xatolik haqida xabar beradi.

Dasturiy ta’minotda .NET platformasining System.Security.Cryptography kutubxonasi imkoniyatlaridan foydalanildi. AES algoritmini amalga oshirishda Aes sinfi, ma’lumotlar oqimini qayta ishlashda esa MemoryStream va CryptoStream obyektlari qo‘llanildi. Bu esa dastur samaradorligi va ishlash tezligini ta’minlashga xizmat qiladi.

Qo‘shimcha funksiyalar sifatida natijani tezkor nusxalash (Copy) hamda barcha maydonlarni tozalash (Clear) imkoniyatlari joriy etildi. Ushbu funksiyalar dasturdan foydalanishni yanada qulaylashtiradi.

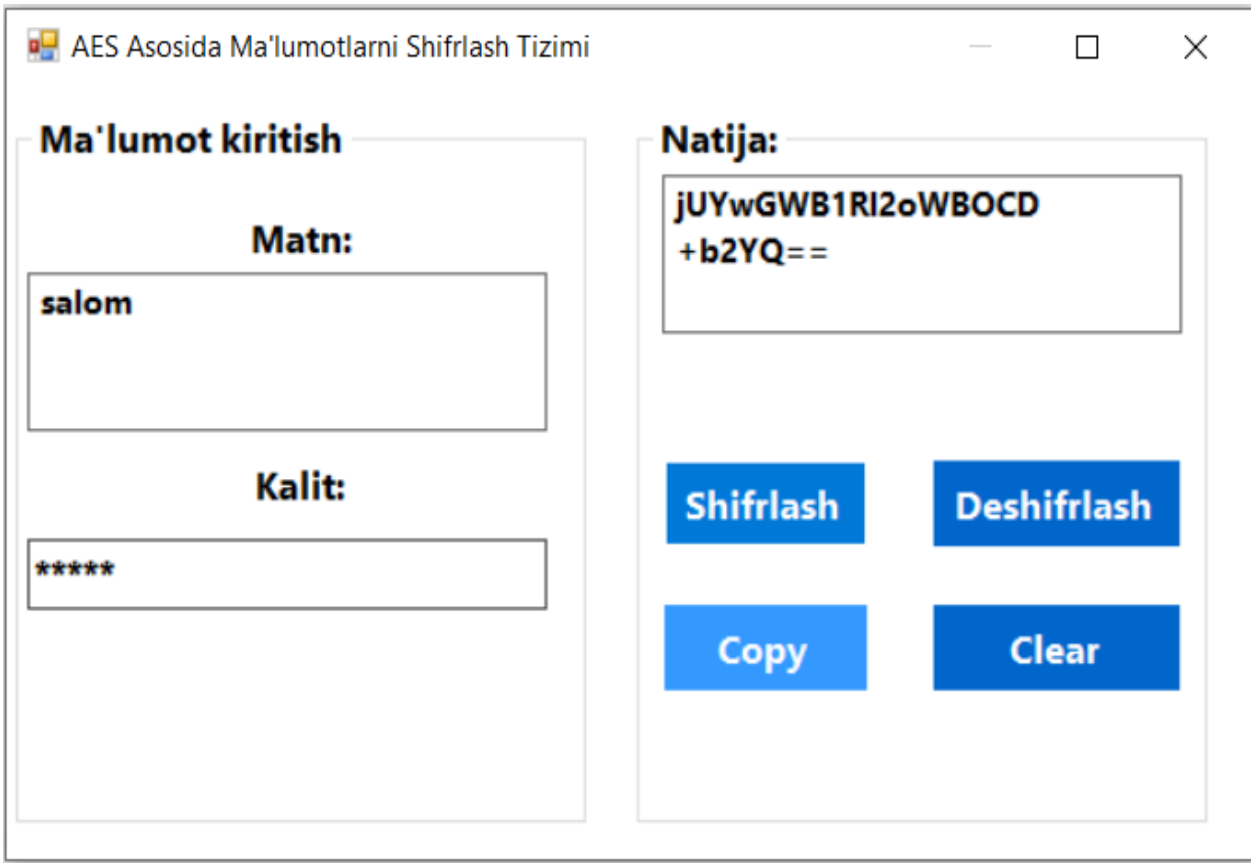
Shunday qilib, ishlab chiqilgan dasturiy tizim AES algoritmi asosida ma’lumotlarni ishonchli shifrlash va deshifrlashni amalga oshiradi hamda axborot xavfsizligini ta’minlashda samarali vosita sifatida xizmat qiladi.

AES algoritmi asosida ma’lumotlarni shifrlash tizimining modeli.

Quyida AES algoritmi asosida ma’lumotlarni shifrlash va deshifrlash tizimining dasturiy modeli keltiriladi. Ushbu model foydalanuvchi kiritgan matnli ma’lumotlarni maxfiy kalit yordamida shifrlash va qayta tiklash imkonini beradi.

Algoritm bosqichlari quyidagilardan iborat:

1. Kirish ma’lumotini (matnni) qabul qilish;
2. Maxfiy kalitni kiritish;
3. Ma’lumotlarni baytlar ketma-ketligiga o‘tkazish;
4. AES algoritmi yordamida shifrlash jarayonini amalga oshirish;
5. Natijani Base64 formatida chiqarish;
6. Zarur holatda shifrlangan ma’lumotni qayta deshifrlash.



1-rasm. AES algoritmi asosida ma’lumotlarni shifrlash va deshifrlash dastur interfeysi.

1-jadval

Kiruvchi matn	Shifrlangan natija	Kalit
salom	jUYwGWB1RI2oWBOCD+b2YQ==	12345
hello	Pcg1Sb4c/M8pOLEJRQtqSg==	12345
test	8GeFSf07qUVhmR4bn0W9+g==	12345

Xulosa o‘rnida shuni ta’kidlash joizki, maqola C# dasturlash muhiti yordamida AES algoritmi asosida ma‘lumotlarni shifrlash va deshifrlash tizimi muvaffaqiyatli ishlab chiqildi. Amalga oshirilgan tadqiqot natijalari shuni ko‘rsatadiki, AES algoritmi zamonaviy axborot xavfsizligi sohasida eng ishonchli va samarali kriptografik standartlardan biri bo‘lib qolmoqda.

Ishlab chiqilgan dasturiy tizim Windows Forms texnologiyasi asosida qulay foydalanuvchi interfeysi bilan ta‘minlangan. Dastur yordamida foydalanuvchi matnli ma‘lumotlarni maxfiy kalit asosida shifrlash va deshifrlash imkoniyatiga ega bo‘ldi. .NET platformasining

System.Security.Cryptography kutubxonasidan foydalanish dasturning ishonchliligi va samaradorligini oshirdi. AES algoritmining SubBytes, ShiftRows, MixColumns va AddRoundKey kabi asosiy bosqichlari o‘rganildi va ularning kriptografik mustahkamlikni ta‘minlashdagi roli tahlil qilindi. 128 bitli blok uzunligi va turli kalit uzunliklarida (128, 192, 256 bit) ishlash qobiliyati AES algoritmini turli sohalarda qo‘llashga imkon beradi.

Sinovlar natijalari ko‘rsatdiki, tizim turli xil matnli ma‘lumotlarni (“salom”, “hello”, “test” va boshqalar) kalit yordamida to‘g‘ri shifrlaydi va deshifrlaydi. Noto‘g‘ri kalit kiritilganda dastur foydalanuvchini xatolik haqida ogohlantiradi, bu esa tizimning xavfsizlik darajasini yanada oshiradi.Kelajakda ushbu tizimni fayl shifrlash, tarmoq orqali xavfsiz ma‘lumot uzatish va ma‘lumotlar bazalarini himoyalash kabi yanada keng ko‘lamli sohalarda qo‘llash rejalar qilinmoqda. Bundan tashqari, assimetrik algoritmlar (RSA, ECC) bilan integratsiyalash orqali gibrid kriptografik tizim yaratish ham istiqbolli yo‘nalish hisoblanadi. Mazkur maqolada axborot xavfsizligini ta‘minlashda dasturiy yechimlarning amaliy ahamiyatini yaqqol namoyon etadi.

Adabiyotlar ro‘yxati:

1. Onur Aci, cmez1, Werner Schindler, and Çetin K. Ko c. Cache based remote timing attack on the aes. 2007.

2. C Ashokkumar, Bholanath Roy, M Bhargav Sri Venkatesh, and Bernard L. Menezes. s-box implementation of aes is not side channel resistant. 2018.

3. Navid Ghaedi Bardeh and Sondre Rønjom. Practical attacks on reduced-round aes. 2019.

4. Eli Biham, Alex Biryukov, Orr Dunkelman, and Eran Richardson. Cryptanalysis of skipjack-4xor. pages 5–6, jun 1998.

5. Eli Biham and Nathan Keller. Cryptanalysis of reduced variants of rijndael. 2000.

6. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

7. Simmons G. J. Authentication theory/coding theory, in Advances in Cryptology, Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Lecture Notes in Computer Science, No. 196. New York, NY: Springer, 1985, pp. 411–431.

8. Бабаш А.В., Шанкин Г.П. Криптография. –Москва: Лори Гелиос АРВ, 2002. –512 с.

9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003. – 816 с.

10. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. – 448 с.