МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XI Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

18 грудня 2025 року

Полтава 2025

УДК 621.745
***А.Ю. Батраченко**, магістрант,*
***Г.В. Головко**, к.т.н., доцент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ПОРІВНЯННЯ СУЧАСНИХ КРИПТОГРАФІЧНИХ ШИФРІВ ІЗ ШИФРОМ AES

Проблема збереження та безпеки даних виникла значно раніше, ніж були створені перші комп'ютери. Проте розвиток інформаційних технологій суттєво змінив підходи до організації захисту. Саме тому конфіденційність інформації — її збереження від сторонніх очей — була головним пріоритетом перших систем захисту. Найефективнішим способом убезпечити дані від перехоплення чи розголошення традиційно вважалося їхнє повне шифрування. Сьогодні ж ключовим викликом у цій сфері є захист інформації, що передається та зберігається у комп'ютерних мережах.

Активне впровадження комп'ютерів у всі сфери життя, зростання їхніх можливостей та широке використання мереж різного рівня зробили ризик витоку конфіденційних даних постійним фактором будь-якої діяльності. Теоретично ідеально захищений комп'ютер — це пристрій, що зберігається у заблокованому сейфі, не під'єднаний до жодної мережі та навіть вимкнений. Така машина практично недосяжна для зловмисників, але водночас абсолютно непридатна для використання. Цей приклад наочно демонструє, що абсолютний захист неможливий через необхідність доступу до даних, а також через складність самих систем безпеки.

Серед численних методів шифрування, що застосовуються сьогодні для захисту інформації, особливе місце займає алгоритм AES (Advanced Encryption Standard). Вже понад два десятиліття залишається одним із найнадійніших засобів захисту даних у світі. Його популярність пояснюється поєднанням високого рівня безпеки, ефективності та універсальності застосування.

Однією з головних переваг AES є використання симетричного ключа — одного й того самого для шифрування та розшифрування, що забезпечує високу швидкість обробки даних навіть на пристроях із невеликою обчислювальною потужністю. Алгоритм підтримує кілька довжин ключа — 128, 192 та 256 біт — що дозволяє обирати оптимальний рівень захисту залежно від вимог системи.

Крім того, AES відзначається високою стійкістю до сучасних методів криптоаналізу. Його структура побудована на багатоетапних перетвореннях даних, включно з підстановками, перестановками та змішуваннями, що робить відновлення вихідного повідомлення без знання ключа практично неможливим. Саме завдяки такій архітектурі AES широко використовується

в найрізноманітніших сферах — від захисту банківських транзакцій і персональних даних до шифрування урядової та військової інформації.

Алгоритм реалізується на апаратному та програмному рівнях, легко інтегрується в сучасні протоколи безпеки та здатний працювати з великими обсягами даних у реальному часі. Поєднання продуктивності, гнучкості та надійності зробило AES фактичним стандартом де-факто у сфері захисту інформації.

Щоб повною мірою оцінити переваги AES, варто порівняти його з іншими відомими алгоритмами шифрування, які застосовуються у сфері захисту інформації. Серед них найбільш поширеними є DES, 3DES та RSA, кожен із яких має власні особливості та обмеження.

DES (Data Encryption Standard) — один із перших загальноприйнятих стандартів шифрування, який активно використовувався з 1970-х років. Проте на сучасному етапі він вважається застарілим через надто короткий ключ довжиною 56 біт. Такий розмір ключа робить DES вразливим до атак перебором, які сьогодні можуть бути здійснені навіть із використанням відносно доступних обчислювальних ресурсів.

3DES (Triple DES) був створений як тимчасове рішення для підвищення безпеки оригінального DES шляхом триразового застосування шифрування з різними ключами. Хоча це значно підвищило криптостійкість, 3DES має суттєвий недолік — низьку продуктивність.

Інший підхід до шифрування представляє RSA — алгоритм з відкритим ключем, який базується на складності факторизації великих чисел. RSA широко використовується для захисту обміну ключами та цифрових підписів, однак він не призначений для шифрування великих обсягів даних через значно нижчу швидкість у порівнянні з симетричними алгоритмами.

На відміну від згаданих алгоритмів, AES поєднує високу криптографічну стійкість, ефективність і гнучкість. Він здатен шифрувати великі обсяги даних значно швидше, ніж 3DES або RSA, і при цьому забезпечує набагато вищий рівень безпеки, ніж застарілий DES. Крім того, завдяки підтримці ключів різної довжини AES може масштабуватися залежно від рівня загроз і вимог до продуктивності, що робить його оптимальним вибором як для персональних пристроїв, так і для корпоративних або державних систем.

ЛІТЕРАТУРА:

1. Alanazi, H. et al. New Comparative Study Between DES, 3DES and AES Within Nine Factors. arXiv, 2010.

2. Shevchuk, Y. Analytical Approach to Evaluating the Effectiveness of Cryptographic Methods in Modern Information Security Systems. Futurity Proceedings, 2023.

3. Golovko G., Rudenko O., Batrachenko. A., Ryzymenko R, Organization of information protection at the "Drive Petrol" enterprise using a cryptographic algorithm AES.

COMPARISON OF MODERN CRYPTOGRAPHIC CIPHERS WITH THE AES CIPHER

***A. Batrachenko**, undergraduate,*
***G. Golovko**, Ph.D., Associate professor*
National University «Yuri Kondratyuk Poltava Polytechnic»