https://www.proconference.org/index.php/usc/article/view/usc24-00-011
DOI: 10.30888/2709-2267.2024-20-00-011

УДК 004.056.5

ANALYSIS OF MODERN ENCRYPTION ALGORITHMS AND THEIR IMPACT ON THE SECURITY AND EFFECTIVENESS OF INFORMATION PROTECTION

АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ ШИФРУВАННЯ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ І ЕФЕКТИВНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Kopach A. I. / Копач А. І.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *У роботі досліджується сучасні алгоритми шифрування та їх вплив на безпеку та ефективність. Розглянуто симетричні алгоритми, зокрема DES, 3DES і AES, виявлено їх переваги та недоліки. Також описані асиметричні алгоритми, такі як RSA, DSA і DH, що забезпечують надійний захист інформації. Подальше обговорення стосується перспектив розвитку гібридних алгоритмів та ідеї подвійного шифрування для підвищення стійкості. В статті надані практичні поради щодо вибору алгоритмів шифрування в залежності від обсягу даних та критеріїв безпеки.*

Ключові слова: *алгоритми шифрування, безпека, DES, 3DES, AES, RSA, DSA, DH, гібридні алгоритми, подвійне шифрування, вибір, критеріїв.*

Abstract. *Modern encryption algorithms and their impact on information security and efficiency are thoroughly examined in the article. The study covers both symmetric (DES, 3DES, AES) and asymmetric (RSA, DSA, DH) algorithms, focusing on their characteristics, advantages, and disadvantages. Perspectives on the development of hybrid algorithms and ideas of double encryption to enhance security are proposed. Practical advice on algorithm selection and a proprietary method for choosing encryption algorithms are also discussed.*

Key words: *encryption algorithms, security, DES, 3DES, AES, RSA, DSA, DH, hybrid algorithms, double encryption, selection, criteria.*

Вступ.

У сучасному світі, де дані стають найціннішим ресурсом, захист інформації від несанкціонованого доступу стає критично важливим. Криптографія, наука про шифрування даних, відіграє ключову роль у забезпеченні конфіденційності, цілісності та автентичності інформації [1-3]. Ця стаття присвячена аналізу основних алгоритмів шифрування, що використовуються в сучасній криптографії, зокрема симетричних (DES, 3DES, AES) та асиметричних (RSA, DSA, DH) алгоритмів [4-7]. Ми розглянемо їх основні характеристики, переваги та недоліки, а також дослідимо перспективи

розвитку гібридних алгоритмів та подвійного шифрування. Крім того, ми обговоримо критерії вибору алгоритмів шифрування та представимо авторську розробку, спрямовану на автоматизацію цього процесу.

Симетричні алгоритми шифрування є ключовою складовою сучасної криптографії, забезпечуючи конфіденційність даних за рахунок використання одного секретного ключа для шифрування та дешифрування даних. Найбільш відомими симетричними алгоритмами є DES (Data Encryption Standard), 3DES (Triple DES), та AES (Advanced Encryption Standard).

DES (Data Encryption Standard) був розроблений компанією IBM та затверджений NIST у 1977 році як офіційний стандарт шифрування. Основним недоліком DES є його коротка довжина ключа, що робить його вразливим до атаки повного перебору.

3DES (Triple DES) був розроблений у відповідь на загрози, пов'язані з коротким ключем DES. 3DES використовує три послідовних застосування алгоритму DES для підвищення рівня безпеки.

AES (Advanced Encryption Standard) був затверджений NIST у 2001 році як заміна DES та 3DES. AES вважається високоефективним та безпечним алгоритмом, здатним забезпечувати захист даних на найвищому рівні.

Асиметричні алгоритми шифрування забезпечують надійний захист інформації шляхом використання двох ключів: відкритого для шифрування та закритого для дешифрування. Серед найважливіших і найпоширеніших асиметричних алгоритмів можна виділити RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) та DH (Diffie-Hellman).

RSA є одним з найбільш відомих та широко використовуваних асиметричних алгоритмів шифрування; базується на математичній складності факторизації великих простих чисел.

DSA або алгоритм цифрового підпису, стандарт для цифрових підписів і базується на математичних властивостях дискретних логарифмів у скінченних полях і використовується переважно для створення та перевірки цифрових підписів.

DH є одним з перших практичних алгоритмів обміну ключами, що дозволяє двом сторонам безпечно обмінятися криптографічними ключами через незахищений канал.

Перспектива розвитку гібридних алгоритмів та ідея підвищення стійкості алгоритму за рахунок подвійного шифрування. Гібридні алгоритми шифрування поєднують в собі переваги симетричних та асиметричних методів з метою забезпечення високої безпеки та ефективності.

Практика комбінації критеріїв для вибору алгоритмів. Вибір криптографічного алгоритму є важливим завданням, яке потребує ретельного аналізу та врахування декількох факторів. До числа ключових критеріїв, які слід брати до уваги, належать: криптостійкість, швидкість, довжина ключа.

Обґрунтування вибору критеріїв

1. Об’єм тексту. Об'єм тексту визначає можливості системи щодо обробки різних обсягів даних. Деякі алгоритми можуть бути більш ефективними при обробці великих обсягів даних, коли інші можуть забезпечувати кращу продуктивність при роботі з невеликими обсягами. Таким чином, важливо враховувати специфіку застосування та потреби користувачів при виборі алгоритму шифрування.

2. Швидкість. Швидкість шифрування і розшифрування є критичними для багатьох застосувань. Наприклад, у великих мережевих систем чи систем передачі даних, швидкість може бути визначальним фактором у виборі алгоритму. Деякі застосування можуть вимагати швидкого оброблення великого обсягу даних в реальному часі. У таких випадках важливо обирати алгоритми, які забезпечують не лише високий рівень безпеки, але й ефективність в операціях шифрування та розшифрування.

3. Криптостійкість. Криптостійкість є фундаментальним критерієм при виборі алгоритмів шифрування. Основна мета шифрування полягає в тому, щоб забезпечити конфіденційність, цілісність та доступність даних. Обрані алгоритми мають бути відповідними для використання в реальних умовах і повинні витримувати широкий спектр атак, включаючи криптоаналіз, перебір

ключів та атаки на структуру алгоритму. Для цього важливо враховувати рівень безпеки, що надається алгоритмом і як він відповідає сучасним вимогам до криптографічної стійкості.

4. Довжина ключа. Довжина ключа є таким параметром, що визначає криптографічну стійкість алгоритму. Зазвичай, чим довший ключ, тим складніше зламати шифр методами перебору. Однак, разом з цим збільшується обчислювальна складність операцій шифрування та розшифрування. Тому вибір довжини ключа повинен бути збалансованим, враховуючи потреби в безпеці та ефективності використання ресурсів.

Обґрунтування вибору параметрів.

В перелік загальних параметрів, які б допомогли середньостатистичному користувачу обрати собі потрібний алгоритм такий: довжина ключа і власне час, який був витрачений на шифрування і дешифрування даних.

1. Довжина ключа. Виведення довжини ключа дозволяє користувачам зрозуміти рівень криптографічної стійкості, який використовується для захисту їхніх даних. Більша довжина ключа зазвичай означає більшу безпеку, але також може впливати на продуктивність системи. Таким чином, надання інформації про довжину ключа дозволяє користувачам бути впевненими у рівні захисту їхніх даних.

2. Час шифрування і дешифрування. Швидкість шифрування і розшифрування є критичними параметрами, особливо для застосувань, де час відгуку системи має значення. Виведення цих параметрів дозволяє користувачам оцінити продуктивність системи та при необхідності зробити вибір між криптографічною стійкістю та швидкістю операцій. Така інформація допомагає користувачам забезпечити оптимальний баланс між безпекою та ефективністю при використанні програми.

Автор вибрав 5 алгоритмів (DES, 3DES, Camellia, RSA, AES); обрані критерії та відповідні алгоритми показано в табл. 1, а один із варіантів вибору критеріїв та автоматизованого процесу вибору алгоритму, який реалізував автор у запропонованому ПЗ наведено на рис. 1.

Таблиця 1 – Критерії та алгоритми

Алгоритм	Довжина ключа, **біт**	Криптостійкість (0-100)	Час зашифр. Мб/с	Час розшифр. Мб/с
DES	64	20	60	55
3DES	192	50	25	20
Camellia	128, 192, 256	92	500-1500	500-1500
RSA	2048	90	0.1-0.5	1-10
RSA	4096	95	0.01-0.5	0.1-5
AES	128, 192, 256	95	500-1500	500-1500

Авторська розробка

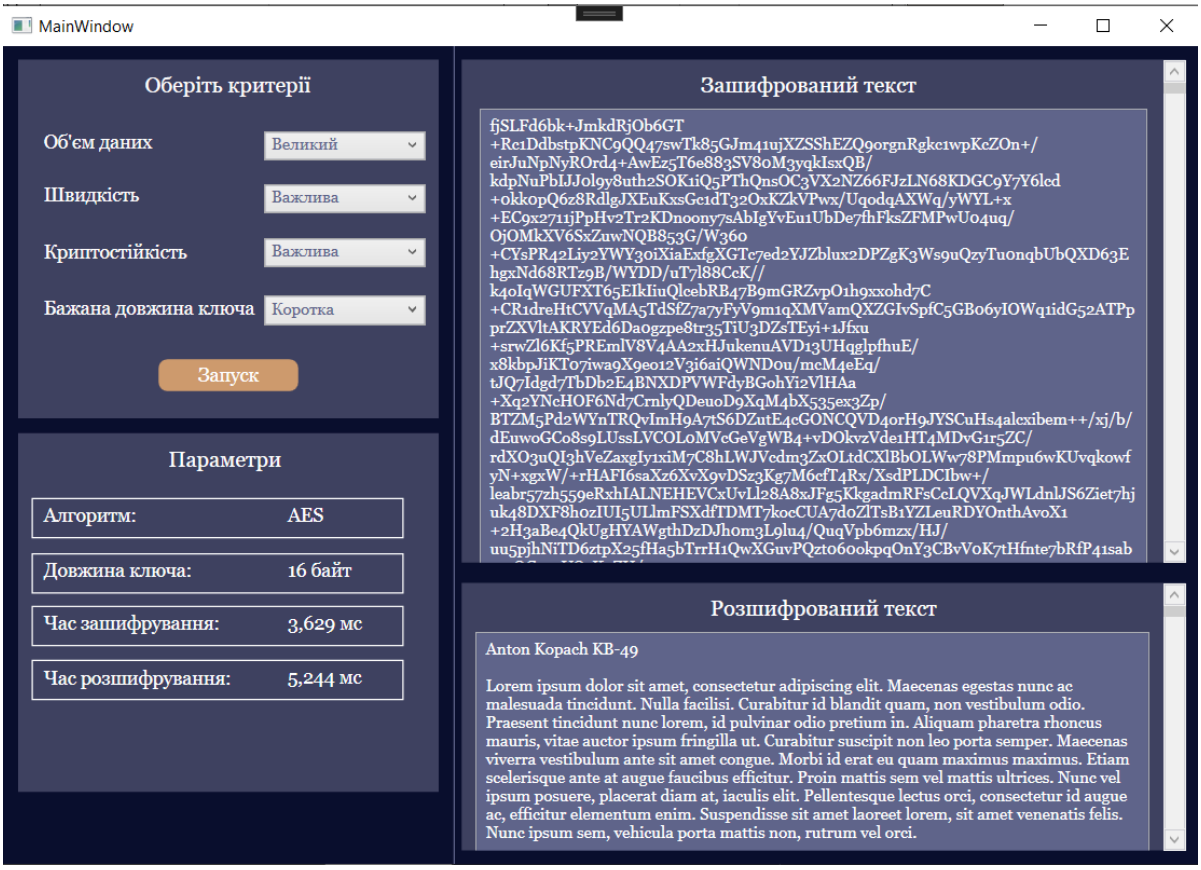

Рисунок 1 – Кейс виклику алгоритму AES для великого об'єму даних

Авторська розробка

Висновки.

В даній роботі запропоновано ідея підвищення стійкості алгоритму за рахунок подвійного шифрування. Гібридні алгоритми шифрування, які

поєднують в собі переваги симетричних та асиметричних методів, можуть забезпечити високий рівень безпеки та ефективності. В цілому, розуміння основних принципів роботи різних алгоритмів шифрування та вміння правильно вибрати найбільш підходящий алгоритм для конкретного застосування є ключовими для забезпечення надійного захисту даних.

Література:

1. "Cryptography and Network Security: Principles and Practice", William Stallings (2016).

2. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th Edition).

3. "Cryptography Engineering: Design Principles and Practical Applications", Niels Ferguson, Bruce Schneier і Tadayoshi Kohno (2010).

4. "Serious Cryptography: A Practical Introduction to Modern Encryption", Jean-Philippe Aumasson (2017).

5. "Understanding Cryptography: A Textbook for Students and Practitioners", Christof Paar і Jan Pelzl (2010).

6. "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Bruce Schneier (2015).

7. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd Edition).

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 18.05.2024 р.