https://www.sworldjournal.com/index.php/swj/article/view/swj25-00-023
DOI: 10.30888/2663-5712.2024-25-00-023

УДК 004.056.5

ACTUAL ENCRYPTION ALGORITHMS: DETAILED ANALYSIS AND DEVELOPMENT PERSPECTIVES

СУЧАСНІ АЛГОРИТМИ ШИФРУВАННЯ: ДЕТАЛЬНИЙ АНАЛІЗ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

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. *Стаття присвячена аналізу сучасних алгоритмів шифрування, зокрема симетричних (DES, 3DES, AES) та асиметричних (RSA, DSA, DH). Автор розглядає основні характеристики кожного алгоритму, їх переваги та недоліки, особливості їх використання. Особливу увагу приділено впливу довжини ключа на стійкість алгоритму до атак, а також швидкості обробки даних. Тут розглядаються перспективи розвитку гібридних алгоритмів шифрування. Автор пропонує ідею подвійного шифрування, що може підвищити стійкість системи та зробити атаку ще складнішою. Стаття містить практичні рекомендації щодо вибору алгоритмів шифрування для різних об'ємів даних та наборів критеріїв. Автор пропонує власний метод перебору алгоритмів шифрування з різними довжинами ключів (AES, RSA, DES, 3DES, Camellia) та демонструє його реалізацію на прикладі ПЗ.*

Ключові слова: *DES, 3DES, AES, RSA, DH, гібридні алгоритми шифрування, подвійне шифрування, комбінація критеріїв для вибору алгоритмів.*

Вступ.

У сучасному світі, де дані є найціннішим активом [1], захист інформації стає важливою проблемою [2-3]. Шифрування даних є одним з найефективніших способів забезпечення конфіденційності і цілісності інформації [4-7]. Ця стаття присвячена аналізу сучасних алгоритмів шифрування, включаючи симетричні та асиметричні методи, а також перспективи розвитку гібридних алгоритмів та подвійного шифрування. Ми розглянемо ключові характеристики кожного алгоритму, їх переваги та недоліки, а також можливі напрямки для подальшого вдосконалення та оптимізації. Крім того, ми обговоримо практику комбінації критеріїв для вибору алгоритмів шифрування.

Аналіз сучасних алгоритмів шифрування.

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).

1. *DES* (Data Encryption Standard), був розроблений компанією IBM та затверджений NIST у 1977 році як офіційний стандарт шифрування. DES є блоковим алгоритмом, який використовує блоки розміром 64 біти і ключ довжиною 56 біт. Процес шифрування в DES складається з 16 циклів (раундів) обробки, кожен з яких включає в себе перестановку та заміну бітів. DES працює

за схемою Фейстеля, що означає, що блоки даних поділяються на дві частини, і одна частина проходить через різні операції, які залежать від ключа, а потім об'єднується з іншою частиною. Основним недоліком DES є його коротка довжина ключа, що робить його вразливим до атаки повного перебору, яка стала практично здійсненною з розвитком обчислювальних потужностей.

2. *3DES (Triple DES)*. У відповідь на загрози, пов'язані з коротким ключем DES, був розроблений алгоритм 3DES, або потрійний DES. 3DES використовує три послідовних застосування алгоритму DES для підвищення рівня безпеки. Існують три основні варіанти реалізації 3DES:

- К1 = К2 = К3: еквівалентний звичайному DES.
- К1 = К3 ≠ К2: більш безпечний варіант, часто використовується.
- К1 ≠ К2 ≠ К3: найвищий рівень безпеки.

Процес шифрування в 3DES включає три етапи: шифрування з першим ключем, дешифрування з другим ключем, і знову шифрування з третім ключем. Цей метод значно підвищує стійкість до атак, однак також значно збільшує час обробки даних через триразове застосування DES.

3. *AES* (Advanced Encryption Standard) був затверджений NIST у 2001 році як заміна DES та 3DES. AES є блоковим шифром, який працює з блоками розміром 128 біт та підтримує ключі довжиною 128, 192, або 256 біт. На відміну від DES, AES не використовує схему Фейстеля, а базується на замінах і перестановках, які виконуються в кількох раундах (10, 12 або 14 залежно від довжини ключа). Кожен раунд включає кілька етапів: SubBytes (заміна байтів), ShiftRows (переміщення рядків), MixColumns (змішування стовпців) та AddRoundKey (додавання ключа раунду). AES вважається високоефективним та безпечним алгоритмом, здатним забезпечувати захист даних на найвищому рівні. Його структура дозволяє ефективно реалізовувати алгоритм як у програмному, так і апаратному забезпеченні, що робить його популярним вибором для різноманітних додатків, від захисту даних у хмарних сервісах до забезпечення безпеки у вбудованих системах.

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

1. *RSA* є одним з найбільш відомих та широко використовуваних асиметричних алгоритмів шифрування; базується на математичній складності факторизації великих простих чисел. Основні етапи роботи RSA: генерація ключів, шифрування та дешифрування. Основною перевагою RSA є його стійкість до криптоаналітичних атак завдяки складності факторизації великих чисел. Водночас, ефективність алгоритму може бути знижена через значну обчислювальну вартість операцій з великими числами.

2. *DSA* або алгоритм цифрового підпису, стандарт для цифрових підписів – базується на математичних властивостях дискретних логарифмів у скінченних полях і використовується для створення та перевірки цифрових підписів. Кроки роботи: 1.Генерація ключів; 2. Створення підпису; 3.Перевірка підпису.

3. *DH* є одним з перших практичних алгоритмів обміну ключами, що дозволяє двом сторонам безпечно обмінятися криптографічними ключами через незахищений канал. Кроки роботи: 1. Вибір параметрів; 2. Генерація ключів; 3. Обмін ключами. DH забезпечує надійний механізм безпечного обміну ключами, але не забезпечує автентифікацію, тому його використовують у поєднанні з іншими протоколами для підвищення безпеки.

Перспектива розвитку гібридних алгоритмів та ідея підвищення стійкості алгоритму за рахунок подвійного шифрування.

Гібридні алгоритми шифрування поєднують переваги симетричних та асиметричних методів з метою забезпечення високої безпеки та ефективності. Зазвичай вони використовують симетричні методи для ефективного шифрування великих об'ємів даних та асиметричні для безпечного обміну ключами. Під час комунікації сторони можуть використовувати асиметричне шифрування для обміну симетричним ключем, який потім використовується для шифрування самого повідомлення.

Деякі перспективні аспекти гібридних алгоритмів включають розробку нових методів комбінування симетричного та асиметричного шифрування для оптимізації ефективності та безпеки. Також, розвиток квантових алгоритмів може вимагати перегляду та апгрейду гібридних систем для збереження стійкості шифрування. Ідея подвійного шифрування полягає в тому, щоб застосовувати два різні алгоритми шифрування один за одним. Такий підхід може підвищити стійкість системи та зробити атаку ще складнішою.

Важливо враховувати, що подвійне шифрування може призводити до збільшення обчислювальних витрат і тривалості процесів, тому вибір алгоритмів та їх комбінація повинні бути обрані з урахуванням вимог конкретної задачі та потреб.

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: алгоритм має бути стійким до атак, щоб захистити інформацію від несанкціонованого доступу;
- Швидкість: алгоритм має бути ефективним з точки зору обчислювальних витрат, щоб забезпечити прийнятну продуктивність;
- Довжина ключа: довжина ключа визначає рівень стійкості алгоритму до атак. Довші ключі, як правило, забезпечують вищий рівень безпеки, але можуть призвести до зниження швидкості;

Вибір алгоритмів для малого та великого об’єму даних для набору критеріїв показано на рис. 1-2.

За авторським методом *Algorithms()* (рис. 3) відбувається перебір засобами конструкції *switch* за значенням аргументу *name*. Власне, як було згадано раніше, в цьому ПЗ автор реалізував 5 алгоритмів із різними довжинами ключів: AES, RSA, DES, 3DES, Camellia.

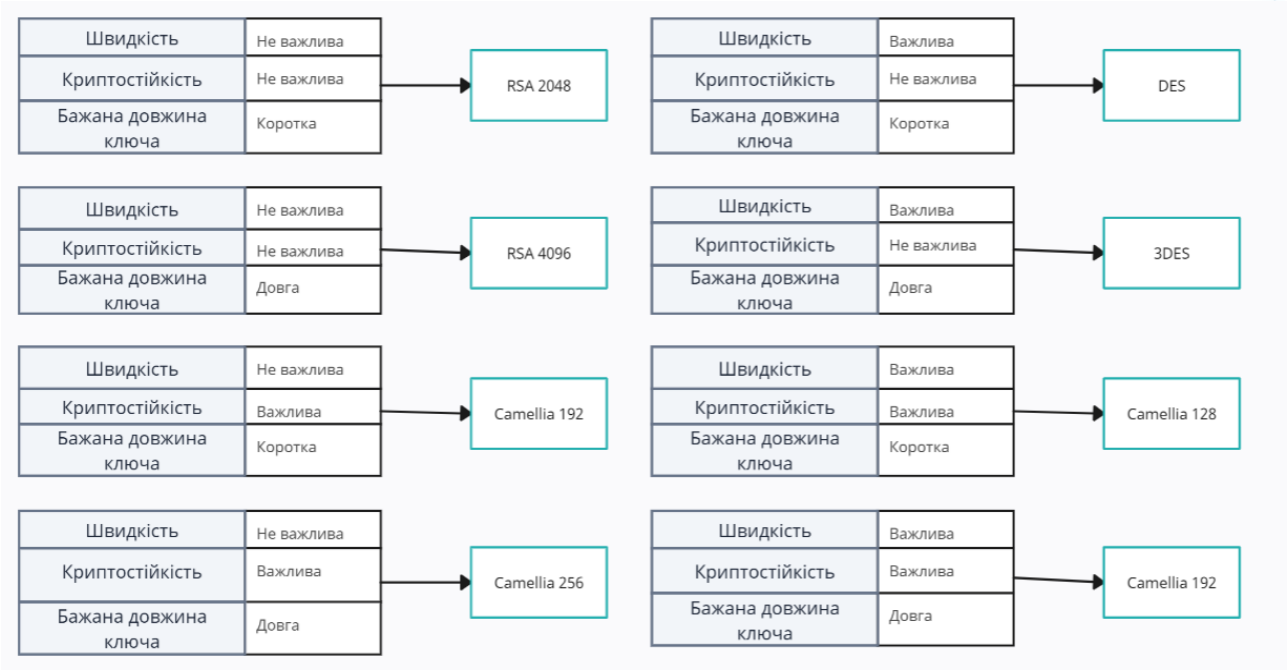

Рисунок 1 – Вибір алгоритмів для малого об'єму даних

Авторська розробка

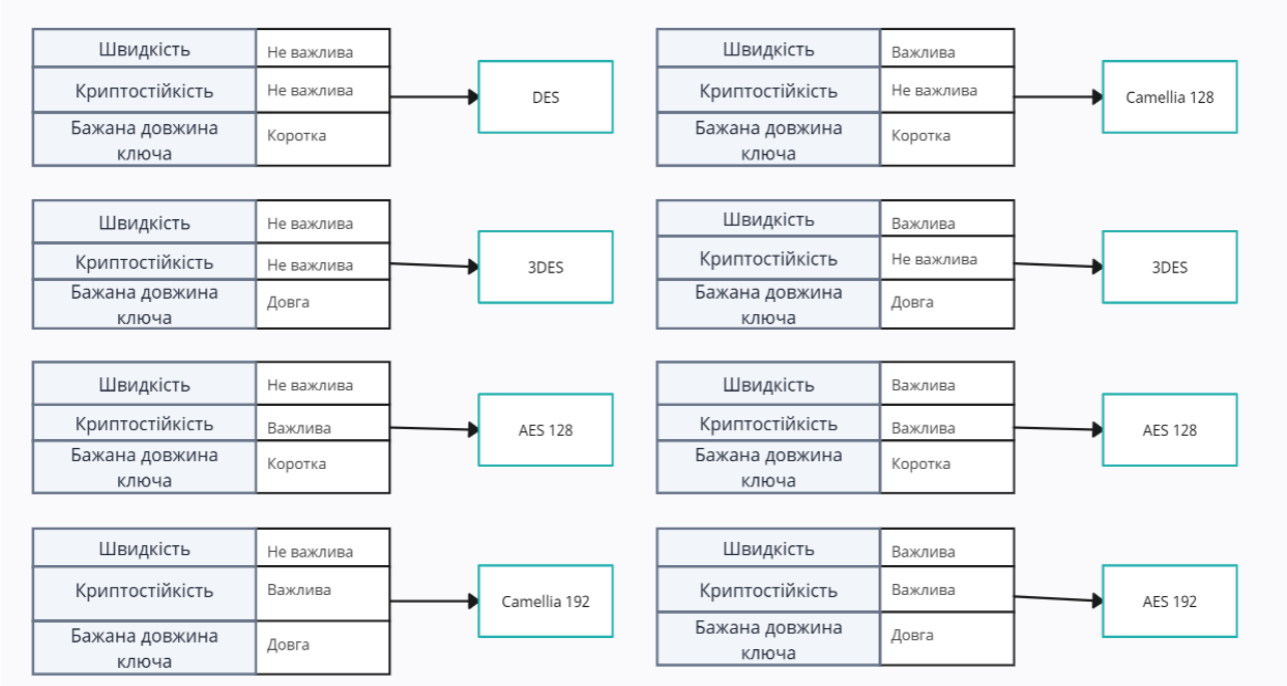

Рисунок 2 – Вибір алгоритмів для великого об'єму даних

Авторська розробка

Кількість критеріїв невелика, автор вибрав 5 алгоритмів (DES, 3DES, Camellia, RSA, AES); обрані критерії та відповідні алгоритми показано в таблиці 1, а один із варіантів вибору критеріїв та автоматизованого процесу вибору алгоритму, який реалізував автор у запропонованому ПЗ наведено на рис. 4.

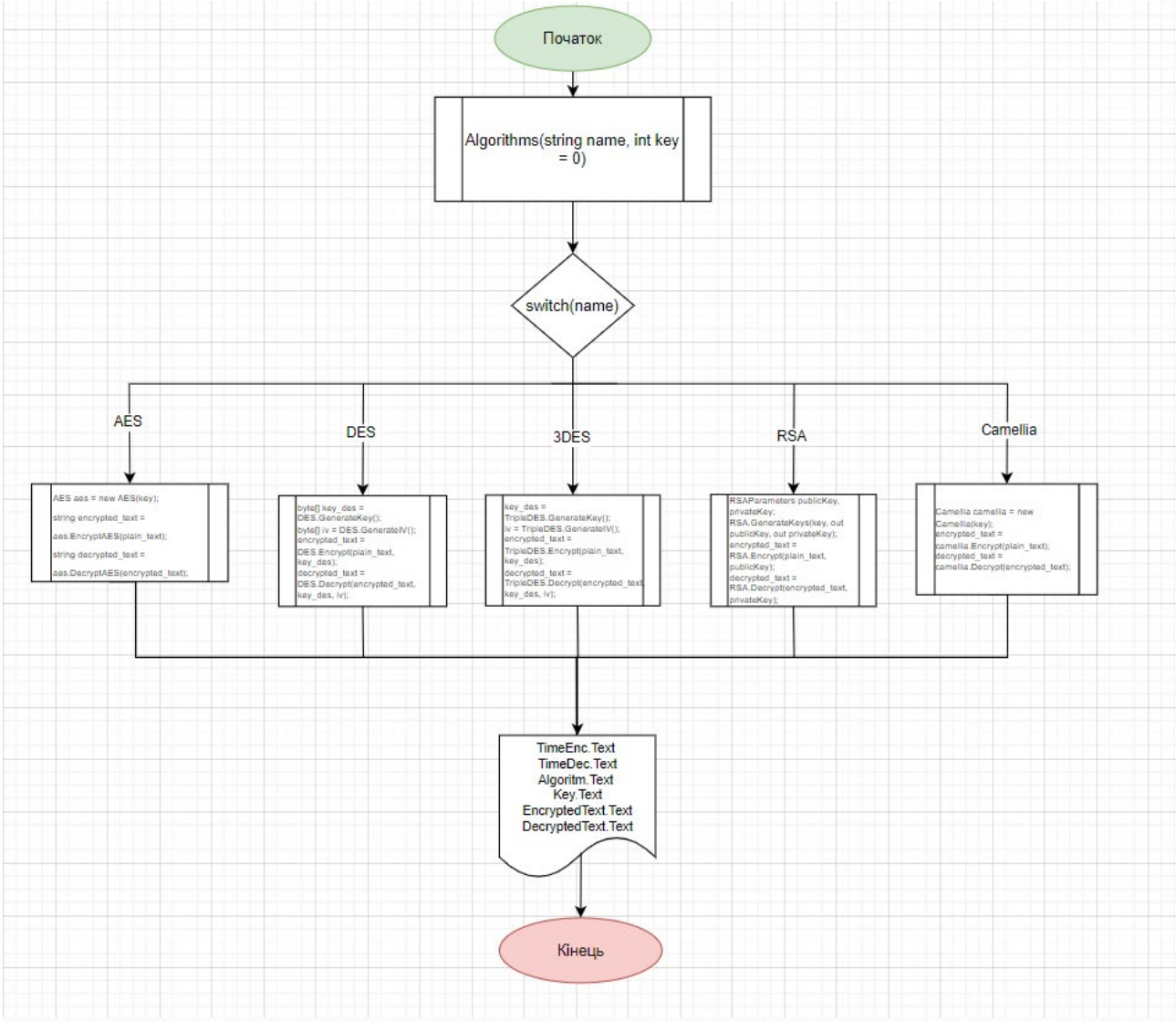

Рисунок 3 – Функціональна схема роботи методу Algorithms()

Авторська розробка

Таблиця 1 – Критерії та алгоритми

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

Авторська розробка

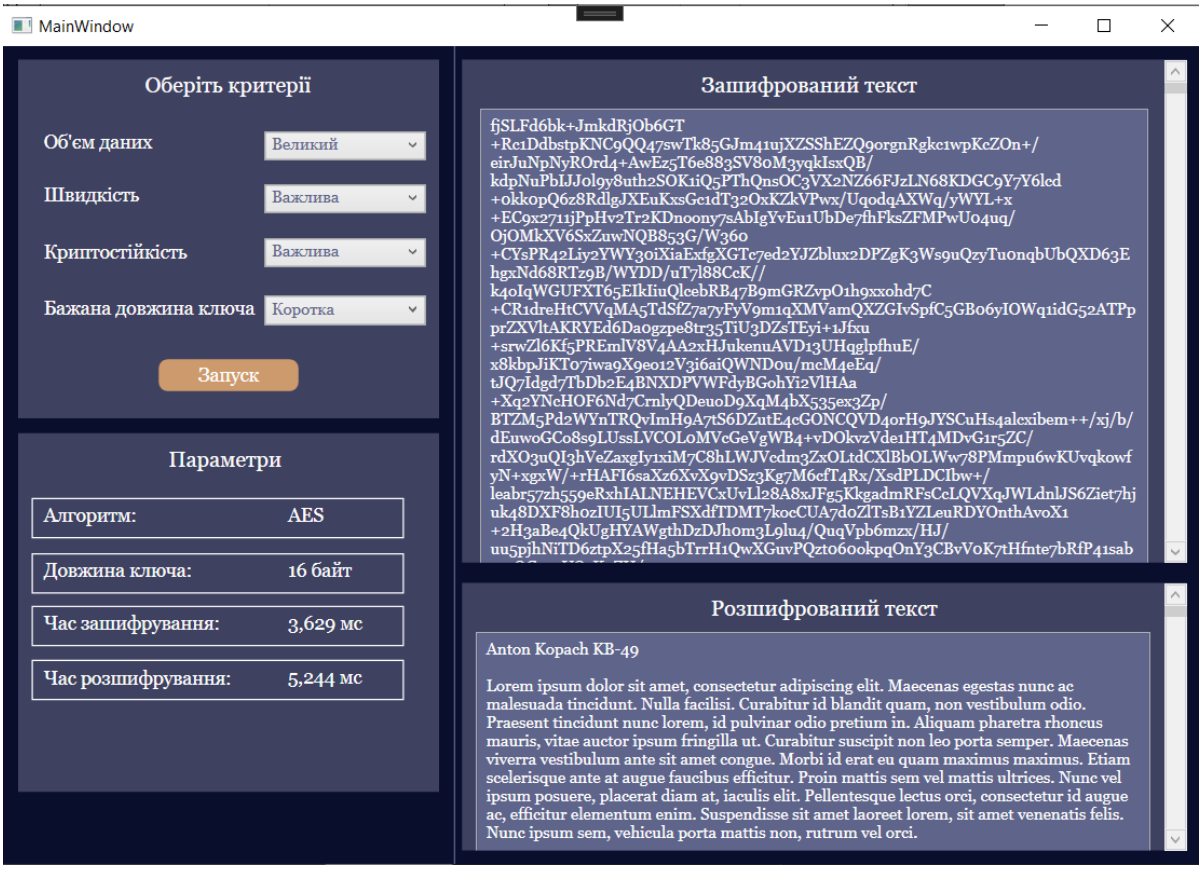

Рисунок 4 – Кейс виклику алгоритму AES для великого об'єму даних
Авторська розробка

Висновки.

В даній роботі виконаний аналіз сучасних алгоритмів шифрування виявив різноманітність методів та підходів, які використовуються для забезпечення безпеки даних. Симетричні алгоритми, такі як DES, 3DES та AES, забезпечують ефективне шифрування за рахунок використання одного ключа для шифрування та дешифрування даних. Однак, вони можуть бути вразливими до атак повного перебору через обмежену довжину ключа. Асиметричні алгоритми, такі як RSA, DSA та DH, забезпечують високий рівень безпеки за рахунок використання двох ключів: відкритого для шифрування та закритого для дешифрування. Ці алгоритми використовують складні математичні проблеми, такі як факторизація великих простих чисел або дискретні логарифми, щоб ускладнити криптоаналітичні атаки.

Гібридні алгоритми шифрування поєднують переваги симетричних та асиметричних методів, щоб забезпечити високий рівень безпеки та ефективності. Вони використовують симетричні методи для шифрування великих об'ємів даних та асиметричні методи для безпечного обміну ключами.

Однак, незалежно від вибраного алгоритму, важливо враховувати декілька ключових критеріїв, таких як криптостійкість, швидкість та довжина ключа. Крім того, важливо розглядати можливість подвійного шифрування та використання гібридних алгоритмів для підвищення стійкості системи. В цілому, сучасні алгоритми шифрування надають потужні інструменти для захисту даних, але вони також вимагають постійного оновлення та вдосконалення, щоб

витримати крок із швидким розвитком технологій та зростаючими загрозами кібербезпеки.

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).

Abstract. *The article is dedicated to the analysis of modern encryption algorithms, particularly symmetric (DES, 3DES, AES) and asymmetric (RSA, DSA, DH). The author examines the main characteristics of each algorithm, their advantages and disadvantages, and their specific uses. Special attention is paid to the impact of key length on the algorithm's resistance to attacks and the speed of data processing. The prospects for the development of hybrid encryption algorithms are also considered. The author proposes the idea of double encryption, which can enhance system robustness and make attacks more difficult. The article contains practical recommendations for selecting encryption algorithms for different volumes of data and sets of criteria. The author proposes their own method for selecting encryption algorithms with various key lengths (AES, RSA, DES, 3DES, Camellia) and demonstrates its implementation using software.*

Keywords: *DES, 3DES, AES, RSA, DH, hybrid encryption algorithms, double encryption, combination of criteria for selecting algorithms.*

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

Стаття надіслана: 18.05.2024 р.