компонентів та адаптуючи їх використання. Чим більше компонентів багатократного використання, з яких складений процес прийняття рішень, тим легше процес інтеграції. Адаптація означає концепцію процесу прийняття рішень, згідно якої побудовано розв'язання проблеми, знижуючись або змінюючи деяку частину(и) існуючого, або розширюючи існуюче деякою новою частиною(ами). Адаптація базується на прецедентах. Прецедент будемо розглядати як використання попереднього досвіду, що базується на описі проблеми чи ситуації разом із докладним зазначенням дій, що роблять у цій ситуації чи розв'язання цієї проблеми та отриманим результатом. Прецедент базується на багаторівневому представленні: прикладному, прикладно-формальному, формальному та реалізаційному. На кожному рівні прецедент повинен включати наступні складові елементи: онтологічний опис ситуації; онтологічне представлення процесу, який було реалізовано в цій ситуації; отриманий результат (позитивний чи негативний).

Кожна стратегія розглядається з трьох точок зору: як раціональний процес аналізу факторів зовнішнього оточення та внутрішніх можливостей системи управління, та формування цілей та визначення результатів реалізації прийняття рішень, обумовлених інтересами та очікуваннями зацікавлених сторін процесу прийняття рішень, як процес вибору та ухвалення рішень, що базується на знаннях та контексті з урахуванням результатів аналізу, як процес реалізації рішень у вигляді реальних дій з проведенням аналізом наслідків їх виконання та формування можливих систем управління змінами.

Онтологічне представлення розглянутих стратегій використовується при виконанні науково-дослідної роботи «Розробити онтологокеровані методи підтримки створення та функціонування системи управління безпечністю продуктів харчування на основі процедур системної оптимізації». Це дозволяє реалізувати поведінковий аспект прийняття рішень (описує ситуації прийняття рішень та порядок, в якому розглядаються задачі та в якому виконуються відповідні дії), організаційний аспект (описує структуру середовища прийняття рішень, ресурси та засоби та визначає організаційну структуру, в якій розв'язання задачі виконується або буде виконуватися і відносини між елементами структури), інформаційний аспект (описує інформацію, яка використовується при прийнятті рішень, як вона представляється і як вона може застосовуватися).

Список використаної літератури

[1] Ю.П. Чаплінський та О.В.Субботіна, "Онтологія та контекст при розв'язанні прикладних задач прийняття рішень", *Штучний інтелект,* № 2, с. 147—155, 2016.

[2] Ю.П. Чаплінський, "Контекстно-онтологічна системна оптимізація проблемно-орієнтованої підтримки прийняття рішень", у *Нові інформаційні технології, моделювання та автоматизація.* С. В. Котлик Ред. Одеса : Екологія, 2022, с. 6 – 44.

УДК 004.056.55

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ШИФРУВАННЯ AES ТА RSA ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Янко А.С., Прокудін А.Ю., Крук О.О. (al9_yanko@ukr.net, auprokudin@gmail.com, kruk.aleksandr1989@icloud.com)
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

У тезі запропоновано до розгляду алгоритмів шифрування даних, які використовуються для забезпечення безпеки інформації в умовах цифрового середовища. Розглянуто основні принципи симетричного та асиметричного шифрування на прикладах AES та RSA. Після аналізу алгоритмів шифрування було здійснено порівняльний аналіз переваг та недоліків алгоритмів шифрування з урахуванням потенційних загроз та вимог до захисту даних.

Кібербезпека стала критично важливою для захисту даних в організаціях, оскільки кіберзагрози і витоки даних стають дедалі частішими та складнішими. Одним із ключових елементів кібербезпеки є шифрування даних, яке забезпечує конфіденційність інформації та її захист від несанкціонованого доступу. Незважаючи на це, дослідження Thales Group у 2023 році

показало, що лише 20% респондентів повідомили про шифрування більше 60% своїх хмарних даних, і в середньому лише 45% чутливих даних було зашифровано. Це вказує на значні прогалини в захисті даних, які потребують вирішення [1].

Шифрування є методом перетворення даних у нечитабельний формат, який може бути повернений у початковий стан тільки за допомогою ключа. Залежно від типу шифрування, застосовуються симетричні або асиметричні криптографічні ключі.

Симетричні системи ключів. У таких системах один і той самий ключ використовується для шифрування та дешифрування даних. Основною проблемою є безпечна передача цього ключа, що обмежує їх застосування в комерційних цілях. А**симетричні системи ключів**, які використовують пару ключів, приватний і публічний. Публічний ключ доступний широкому загалу для шифрування даних, тоді як приватний залишається секретним для дешифрування. Такий підхід забезпечує вищий рівень безпеки.

Поширені алгоритми шифрування:

1. Triple DES застосовує алгоритм DES із трьома різними ключами, забезпечуючи надійність [2]. Проте він поступово замінюється більш ефективним методом шифрування AES.

2. AES (Advanced Encryption Standard) – це стандартний алгоритм шифрування, що використовується урядом США, забезпечує шифрування на 128, 192 або 256 біт, що робить його практично недоступним для взлому [3].

3. RSA – використовується для шифрування даних в інтернеті за допомогою публічного та приватного ключів. RSA вважається надійним, але потребує значних обчислювальних ресурсів [4].

4. Blowfish та Twofish Швидкі та гнучкі алгоритми симетричного шифрування, доступні в загальному доступі, підходять для широкого спектру програм [5].

Основу сучасного шифрування становлять складні математичні алгоритми, зокрема AES(Advanced Encryption Standard) – це симетричним алгоритмом блочного шифрування, що оперує блоками даних фіксованого розміру 128 біт. Основні математичні операції включають: SubBytes – кожен байт даних проходить через нелінійну таблицю підстановок (S–Box), яка замінює вхідний байт на інший згідно з фіксованою таблицею. ShiftRows – байти кожного рядка зміщуються на певну кількість позицій вліво (0–ий рядок залишається на місці, 1–й зміщується на одну позицію, 2–й на дві, і т.д.). MixColumns – кожен стовпець матриці даних множиться на фіксовану матрицю в полях Галуа $GF(2^8)$, що здійснюється за формулою (1) для одного байта a_i у стовпці:

$$a_i' = (a_i \cdot c_0) \otimes (a_{i+1} \cdot c_1) \otimes (a_{i+2} \cdot c_2) \otimes (a_{i+3} \cdot c_3), \quad (1)$$

де c_i – елементи фіксованої матриці. Та AddRoundKey: побітовий XOR між блоком даних і раундовим ключем. Нижче наведені формули(2), які є загальними виразами для процесів шифрування та дешифрування AES:

$$C = E(K, P), \quad (2)$$

де C – зашифрований текст, P – відкритий текст, а E – функція шифрування з використанням ключа K. Дешифрування здійснюється за формулою(3):

$$P = D(K, C), \quad (3)$$

де D – функція дешифрування.

На кожному з раундів, що їх може бути 10, 12 або 14 (залежно від розміру ключа), використовуються наведені операції. Таким чином, AES є досить складним для зламу, оскільки алгоритм поєднує лінійні й нелінійні перетворення.

Алгоритм RSA (Rivast, Shamir та Adelman) є асиметричним криптографічним методом, який використовує пару ключів: публічний і приватний. Він базується на складності факторизації великих чисел, наприклад числа p та q, які перемножуються для отримання $n = p \cdot q.$ Обчислюється значення функції Ейлера $\varphi(n) = (p-1)(q-1).$ Відкритий ключ складається з n і експоненти e, Вибирається відкрита експонента e, така що $1 < e < \varphi(n)$ e є взаємно простим із $\varphi(n)$ (тобто $\gcd(e, \varphi(n)) = 1).$ Далі обчислюється приватна експонента d, яка є оберненою до e по модулю $\varphi(n),$ $d \cdot e \equiv 1 \bmod \varphi(n)$ Саме шифрування виконується за формулою (4):

$$c = m^e \bmod n, \quad (4)$$

де m – повідомлення, c – зашифроване повідомлення. Дешифрування здійснюється за формулою(5):

$$m = c^d \bmod n, \tag{5}$$

де d – приватний ключ.

Щоб було наглядно наведемо приклад шифрування типу RSA.

Нехай $p = 61,\ q = 53$ тоді виконаємо наступні операції $n = 61 \cdot 53 = 3233,$ далі $\varphi_n = (61-1)(53-1) = 3120$ оберемо число $e = 17,$ яке є взаємно простим з 3120. Далі обчислюємо $d \cdot 17 \equiv 1 \bmod 3120 = 2753.$ Наступним кроком виконуємо шифрування повідомлення $m = 65,$ $c = 65^{17} \bmod 3233 = 2790.$ Тобто зашифроване повідомлення c вийшло 2790.

Для перевірки правильності результату шифрування повідомлення за допомогою RSAБ, виконаємо дешифрування за формулою (5) $m = 2790^{2753} \bmod 3233 = 65$. Результат перевірки демонструє, що алгоритм був виконаний вірно.

Алгоритми AES та RSA мають різні механізми шифрування і застосовуються для різних завдань у криптографії. Нижче наведено порівняння ключових аспектів цих алгоритмів (див. табл. 1).

Таблиця 1 – Порівняльна таблиця алгоритмів AES та RSA

Критерій	AES	RSA
Тип алгоритму	Симетричний, один ключ для шифрування і дешифрування	Асиметричний, пару ключів (публічний і приватний)
Механізм шифрування	Оперує блоками фіксованого розміру (128 біт)	Шифрування на основі експоненціювання та факторизації чисел
Швидкість	Швидке шифрування і дешифрування; підходить для обробки великих обсягів даних	Повільне шифрування і дешифрування; обмежене використання для малих обсягів даних
Розмір ключа	128, 192 або 256 біт	Публічні ключі можуть мати розміри від 1024 до 4096 біт і більше
Стійкість до атак	Вважається безпечним, якщо використовуються ключі довжиною 128 біт або більше	Безпека базується на складності факторизації великих чисел.
Застосування	Шифрування великих обсягів даних, захист файлів та мережевого трафіку	Безпечний обмін ключами, цифрові підписи, захист даних при передаванні
Ресурсоємність	Менш вимогливий до ресурсів обчислень	Висока обчислювальна складність, особливо для великих ключів

Отже, AES та RSA мають різні переваги й недоліки, які роблять їх придатними для різних завдань. AES є кращим для шифрування великих обсягів даних завдяки високій швидкості та низьким обчислювальним вимогам. RSA, хоча й більш обчислювально складний, забезпечує безпечний обмін ключами та використовується для цифрових підписів. Комбіноване використання обох алгоритмів є більш ефективним та практичним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. “Thales Group – міжнародна промислова група, що випускає інформаційні системи для авіакосмічного, військового і морського застосування,” *Novazii company*, 14.09.2024. [Online]. Available: https://novations.ua/thales-group/ [Accessed: October 18, 2024].

2. S. Subaselvi, C. Mytheesh, R. Sanjay, G. Parithi malavan and S. D. Ragunath, "VLSI Implementation of Triple-DES Block Cipher," *2023 7th International Conference on Computing*

Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1162–1166, doi: 10.1109/ICCMC56507.2023.10083953.

3. T. V. Jaswanth and S. J. J. Thangaraj, "Minimized Computational Time in Cloud Using Advanced Encryption Standard Algorithm Over File Changed with Security," *2024 Second International Conference on Advances in Information Technology (ICAIT)*, Chikkamagaluru, Karnataka, India, 2024, pp. 1–6, doi: 10.1109/ICAIT61638.2024.10690288.

4. Z. Chen, C. Liu, F. Li and S. C. -I. Chen, "Security Analysis of Another Vulnerability to RSA Algorithm," *2023 13th International Conference on Information Technology in Medicine and Education (ITME)*, Wuyishan, China, 2023, pp. 434–438, doi: 10.1109/ITME60234.2023.00092.

5. H. K. Hoomed, S. A. Makki and Q. M. Ardeoy, "Modified Blowfish Algorithm for Internet of Things Devices using new 4-Dimensional Chaotic System," *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019, pp. 1004–1010, doi: 10.1109/ICCS45141.2019.9065652.