УДК 004.056.53

Я. І. Насталенко

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ РЕЖИМІВ БЛОКОВОГО ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація. *В доповіді проведено аналіз режимів блокового шифрування та наведено порівняльну характеристику їх особливостей. Розглянуто відомі та найбільш поширені режими, визначено їх вразливості та недоліки. Зазначено вагомий недолік для сучасних систем та великих об'ємів інформації.*

Ключові слова: *шифрування, режим блокового шифрування, конфіденційність, цілісність, гнучкість.*

Abstract*: The report analyzes the modes of block encryption and provides a comparative description of their features. The well-known and most common modes are considered, their vulnerabilities and shortcomings are identified. A significant drawback for modern systems and large amounts of information is noted.*

Keywords*: encryption, block encryption mode, confidentiality, integrity, flexibility.*

Вступ

Обробка великих обсягів інформації вже значний час викликає дискусії та питання економії ресурсів. Абсолютна більшість даних у інформаційних системах потребує конфіденційності, саме тому використовується шифрування для її забезпечення. Оскільки обсяги даних, як правило, є доволі масивними і перевищують стандартні розміри блоку для шифрування, використовуються режими блокового шифрування, які дозволяють шифрувати дані частинами. Проте за сучасними тенденціями дані все частіше змінюються і потребують повторної обробки, що за використання певних режимів блокового шифрування забирає забагато ресурсів, зокрема такого цінного, як час.

Саме тому метою роботи є покращення захищеності шляхом дослідження показників ефективності режимів блокового шифрування у розрізі їх застосування під час шифрування для даних, що постійно змінюються.

Результати дослідження

Шифрування може бути симетричним та асиметричним, різниця у особливостях ключів: для симетричного використовується один приватний ключ для шифрування та розшифрування, а для асиметричного використовується два різних – публічний та приватний відповідно для обох процесів [1]. Для симетричного використовуються блочні шифри, які у свою чергу використовуються у режимах шифрування, які розглядаються.

Загалом є шість видів блокового шифрування:

- електронна книга кодів (ECB, Electronic Codebook) [2];
- ланцюгування шифроблоків (CBC, Cipher Block Chaining) [3];
- ланцюгування шифроблоків із поширенням (PCBC, Propagating Cipher Block Chaining) [4];
- зворотній зв'язок по шифротексту (CFB, Cipher Feedback) [2];
- зворотній зв'язок по виходу (OFB, Output Feedback) [5];
- лічильник (CTR, Counter Mode) [6].

Режим ECB є найпростішим способом шифрування. У цьому режимі повідомлення розбивається на блоки, кожен з яких шифрується окремо, що створює серйозний недолік — однакові блоки тексту перетворюються на ідентичні блоки шифротексту, що утворює видимий шаблон. Через це ECB не рекомендують для використання у криптографічних протоколах [1].

CBC працює шляхом XOR між відкритим текстом і попереднім зашифрованим блоком, завдяки чому кожен наступний блок залежить від попередніх, на відміну від режиму електронної книги кодів. Але для розшифрування одного блоку потрібно опрацювати всі попередні. Це один із найпоширеніших режимів у сучасних протоколах, але його недолік у послідовності виконання, що сповільнює обробку,

оскільки не дозволяє реалізувати повною мірою паралелізацію, а також вимагає повторного проходження даними у випадку зміни якоїсь частини [7].

Ланцюгування шифроблоків із поширенням є модифікацією CBC і створює додаткову залежність між блоками, оскільки додає XOR із попереднім відкритим текстом. Це ускладнює маніпуляції з наступними блоками при незначних змінах у тексті. Проте через чутливість до помилок і нижчий рівень безпеки PCBC не настільки поширений і був вилучений із протоколу Kerberos 4 [8].

CFB базується на механізмі зворотного зв'язку за шифротекстом, де шифрування починається із вектора ініціалізації, який поєднується шляхом застосування операції XOR з блоком відкритого тексту. Цей режим зручний для потокового шифрування і маскує ідентичні блоки, роблячи їх різними у шифротексті. Однак, CFB також чутливий до помилок: збій в одному блоці може вплинути на наступні.

Режим OFB, як і CFB, перетворює блочний шифр у потоковий, але тут замість шифротексту для зворотного зв'язку використовується результат попереднього шифрування. Це дозволяє уникнути ланцюгових помилок, оскільки помилка в одному блоці не впливає на інші. OFB забезпечує високу швидкість і дозволяє паралельну обробку даних, але повторне використання вектора ініціалізації може спричинити вразливість до криптографічного аналізу.

Режим CTR також перетворює блочний шифр у потоковий, використовуючи лічильник як основу. Завдяки високій продуктивності і простоті реалізації, CTR часто застосовується для потокового шифрування. Він не поширює помилки: навіть якщо шифротекст пошкоджений, це не вплине на наступні блоки. Водночас кожне шифрування повинно використовувати унікальний лічильник, і бажано застосовувати автентифікацію, щоб запобігти спотворенню шифротексту.

Для зручності варто винести характеристики всіх режимів у таблицю.

Таблиця 1 – Порівняльна характеристика режимів блокового шифрування

Режим	Характеристика	Швидкість	Повторна обробка при внесенні змін у дані	Переваги	Вразливості
ECB	Окреме шифрування блоків	Висока	-	Простий	Легко виявити шаблони
CBC	XOR з попереднім шифроблоком	Помірна	+	Приховує шаблони	Послідовний, поширення помилок
PCBC	Додатковий XOR з попереднім текстом	Низька	+	Зв'язок між блоками	Чутливий до помилок
CFB	Зворотній зв'язок за шифротекстом	Помірна	+/- (вплив на наступні блоки)	Потоковий, маскує блоки	Поширення помилок
OFB	Зворотній зв'язок по виходу	Висока	-	Потоковий, стійкий до помилок	Вразливий до повтору IV, відсутність автентифікації
CTR	Лічильник для кожного блоку	Висока	-	Швидкий, підтримує паралельність	Чутливий до атак без автентифікації

Загальною вразливістю всіх розглянутих режимів блокового шифрування є їх мала ефективність при потребі повторної обробки даних, особливо великих обсягів, що спричиняє також низький рівень гнучкості. Також можна помітити, що кожен наступний режим вирішує проблеми та вразливості попередніх, породжуючи нові. Тобто режими ECB, CTR та OFB теоретично можуть підійти для ефективної обробки даних, що часто змінюються, оскільки не потребують повторної обробки при внесенні змін. Проте, ECB має занадто вагому вразливість – йому характерна поява шаблонів, що дуже легко виявляються, в свою чергу OFB вирішує цю проблему за рахунок зворотного зв'язку між блоками, але також має вразливість – він не підтримує автентифікацію, тобто якщо блок підмінили, це не буде вчасно помічено. Також він є вразливим до атак на повторення вектору ініціалізації. Режим лічильника вирішує цю проблему, але також є доволі вразливим та потребує використання додаткових

ресурсів: потрібно завжди використовувати унікальні лічильники та додаткову автентифікацію. Тобто ці режими також не підходять для обробки даних, що піддаються частим змінам.

Висновки

Отже, було розглянуто проблему актуальності та ефективності відомих режимів блокового шифрування при обробці даних великих об’ємів, що потребують одночасного забезпечення високого рівня цілісності, конфіденційності та автентичності. Проведений аналіз показав їх наявні вразливості та основну закономірність: кожний наступний режим вирішує наявну проблему попереднього та породжує нові вразливості та недоліки, що каже про підвищення необхідності повної оцінки ризиків перед впровадженням обраного режиму блокового шифрування. Таким чином, стає зрозумілим факт, що існуючі режими блокового шифрування потребують покращення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vanstone S. A., Menezes A. J., Oorschot P. C. v. Handbook of Applied Cryptography. Taylor & Francis Group, 2018. 810 p.
2. NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation. Methods and Techniques. Official edition. 2001.
3. Ehrsam W., Meyer C., Smith J., Tuchman W., "Message verification and transmission error detection by block chaining", US Patent 4074066, 1976.
4. Kaufman C., Perlman R., Speciner M. Network Security: Private Communications in a Public World. Pearson Education, Limited, 2021. 752 p.
5. Sridevi. Construction of Stream Ciphers from Block Ciphers and their Security. International Journal of Computer Science and Mobile Computing. 2014. Vol. 3. P. 703–714. URL: https://ijcsmc.com/docs/papers/September2014/V3I9201499a18.pdf (accessed: 01.11.2024).
6. R. Tirtea and G. Deconinck, "Specifications overview for counter mode of operation. Security aspects in case of faults," Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, Dubrovnik, Croatia, 2004, 769-773 p.
7. Understanding cryptography: A textbook for students and practitioners / ed. by P. Jan. Heidelberg : Springer, 2010. 372 p.
8. Kohl, J. (1990). "The Use of Encryption in Kerberos for Network Authentication". Proceedings, Crypto '89. Berlin: Springer.

Насталенко Яна Іванівна – студентка групи 1БС-23м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sof8013@gmail.com.

Науковий керівник: ***Баришев Юрій Володимирович*** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Yana Nastalenko ─ Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : sof8013@gmail.com.

Scientific supervisor: ***Yurii Baryshev***— PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, yuriy.baryshev@vntu.edu.ua