УДК 004.056.55

Я. О. Оболонська
В. В. Лукічов

СИМЕТРИЧНЕ ШИФРУВАННЯ У СТЕГАНОГРАФІЇ

Вінницький національний технічний університет

Анотація

Досліджено особливості використання симетричного шифрування у стеганографії як одного з сучасних підходів до забезпечення інформаційної безпеки. Проаналізовано принципи роботи основних симетричних алгоритмів, зокрема AES-256, ChaCha20 та механізму автентифікації Poly1305 у складі ChaCha20-Poly1305. Описано їхні ключові характеристики, переваги та особливості застосування. Розглянуто роль симетричного шифрування у підвищенні рівня захисту прихованих даних у стеганографічних системах. Поєднання криптографічних та стеганографічних методів дозволяє значно підвищити конфіденційність, цілісність та автентичність інформації.

Ключові слова: симетричне шифрування, криптографія, стеганографія, захист інформації, AES-256, ChaCha20, Poly1305, автентифіковане шифрування, конфіденційність даних, цілісність даних, криптографічні алгоритми, потокове шифрування, блочне шифрування, інформаційна безпека.

Abstract

The features of the use of symmetric encryption in steganography as one of the modern approaches to ensuring information security are studied. The principles of operation of the main symmetric algorithms, in particular AES-256, ChaCha20 and the Poly1305 authentication mechanism as part of ChaCha20-Poly1305, are analyzed. Their key characteristics, advantages and application features are described. The role of symmetric encryption in increasing the level of protection of hidden data in steganographic systems is considered. The combination of cryptographic and steganographic methods allows to significantly increase the confidentiality, integrity and authenticity of information.

Keywords: symmetric encryption, cryptography, steganography, information protection, AES-256, ChaCha20, Poly1305, authenticated encryption, data confidentiality, data integrity, cryptographic algorithms, stream encryption, block encryption, information security.

Вступ

У сучасному інформаційному середовищі питання захисту даних набуває особливої важливості через зростання кіберзагроз і обсягів переданої інформації. Ефективними підходами до забезпечення безпеки є криптографія та стеганографія, які дозволяють як захистити зміст повідомлення, так і приховати сам факт його передачі. Симетричне шифрування забезпечує швидке перетворення даних із використанням спільного секретного ключа. Його поєднання зі стеганографією підвищує рівень захисту, оскільки зашифровані дані додатково маскуються в інформаційному контейнері.

Результати дослідження

Симетричне шифрування – це спосіб захисту інформації, при якому один і той самий ключ використовується як для шифрування, так і для розшифрування даних. До початку обміну даними сторони мають уже мати в розпорядженні або згенерувати спільний секретний ключ і гарантувати його абсолютну конфіденційність. Сам процес шифрування полягає у перетворенні відкритих даних (тексту, зображення, аудіо чи файлів) за допомогою математичних операцій у зашифрований вигляд, який не має зрозумілого змісту без ключа [1]. Таке перетворення базується на принципах підстановки та перестановки, що багаторазово повторюються для ускладнення структури даних. Важливою властивістю є те, що навіть незначна зміна ключа або вхідних даних призводить до повністю іншого результату шифрування. У стеганографії це забезпечує додатковий рівень захисту навіть якщо приховане повідомлення буде виявлено, його зміст залишатиметься недоступним без відповідного ключа.

Серед великої кількості алгоритмів симетричного шифрування існує багато різних підходів до захисту інформації, однак найбільш поширеними та ефективними на сьогодні є AES-256, ChaCha20 та комбінація ChaCha20-Poly1305. Алгоритми широко застосовуються у сучасних інформаційних системах завдяки високому рівню безпеки, швидкодії та стійкості до криптоаналізу. AES-256 є стандартом для захисту конфіденційних даних і використовується у багатьох програмних і апаратних рішеннях. ChaCha20 відзначається високою продуктивністю та ефективністю на різних типах пристроїв. Поєднання ChaCha20-Poly1305 забезпечує не лише

шифрування, а й перевірку цілісності даних, що робить його одним із найнадійніших варіантів для захисту інформації у сучасних умовах.

Алгоритм AES-256 є одним із найнадійніших представників симетричного шифрування і широко використовується у сучасних інформаційних системах. Він працює за блочним принципом, розбиваючи дані на блоки фіксованого розміру, які обробляються послідовно. Кожен блок проходить серію раундів, у межах яких виконуються складні перетворення заміна байтів за спеціальними таблицями (S-box), циклічні зсуви рядків, перемішування стовпців та додавання раундового ключа. Кожен раунд використовує частину основного ключа, що генерується за допомогою процедури розширення ключа. Багаторівнева обробка забезпечує сильний ефект розсіювання та плутанини, коли залежність між вхідними і вихідними даними стає максимально складною. Ключ довжиною 256 біт створює надзвичайно велику кількість можливих комбінацій, що робить перебір ключа практично неможливим навіть із використанням сучасних обчислювальних ресурсів. Завдяки поєднанню надійності, швидкодії та стандартизації AES-256 активно застосовується у фінансових системах, мережевих протоколах, захищених сховищах даних [2].

Алгоритм ChaCha20 належить до сучасних потокових шифрів і має зовсім інший принцип роботи, ніж блочні алгоритми, такі як AES. Замість поділу даних на блоки він генерує так званий ключовий потік довгу послідовність псевдовипадкових чисел, яка виглядає як випадковий набір байтів. Для генерації цього потоку використовується секретний ключ, унікальне значення nonce (одноразовий параметр) та лічильник блоку. Всі ці значення разом формують початковий стан алгоритму у вигляді матриці чисел. Далі над цим станом виконуються багаторазові раунди спеціальних операцій. Кожен такий раунд включає додавання чисел, операцію XOR та циклічні зсуви бітів. Операції багаторазово перемішують дані таким чином, що отриманий результат стає максимально непередбачуваним. Після завершення всіх раундів формується блок ключового потоку, який потім поєднується з відкритими даними за допомогою операції XOR. Суть цієї операції дуже проста кожен біт повідомлення комбінується з відповідним бітом ключового потоку. У результаті отримується зашифрований текст. Для розшифрування виконується та сама операція XOR із тим самим ключовим потоком, що дозволяє відновити початкові дані. Особливістю ChaCha20 є те, що він дуже швидкий, не потребує складного обладнання і добре працює навіть на звичайних процесорах. Завдяки використанню nonce забезпечується унікальність шифрування навіть для однакових повідомлень, що запобігає повторному використанню однакових ключових потоків [3].

Алгоритм Poly1305 використовується не для шифрування, а для забезпечення цілісності та автентичності даних. Його основне завдання створити короткий перевірочний код (тег автентифікації), який залежить від вмісту повідомлення та секретного ключа. Принцип роботи Poly1305 базується на математичних обчисленнях над великими числами повідомлення розбивається на невеликі частини, які послідовно обробляються за допомогою множення і додавання за модулем великого простого числа. У результаті формується унікальний тег. Навіть найменша зміна у вхідних даних призведе до зовсім іншого тегу, що дозволяє легко виявити підробку або пошкодження інформації. У поєднанні ChaCha20-Poly1305 ці два алгоритми працюють разом як єдина система захисту. Спочатку повідомлення шифрується за допомогою ChaCha20, після чого до зашифрованих даних застосовується Poly1305 для обчислення тегу автентичності. При отриманні даних виконується зворотний процес спочатку перевіряється тег, і лише якщо він правильний, дані розшифровуються. Дозволяє уникнути обробки підроблених або змінених повідомлень. Подібний підхід прийнято називати автентифікованим шифруванням він забезпечує одразу три ключові властивості безпеки конфіденційність дані приховані, цілісність дані не змінені та автентичність джерело даних підтверджене. У стеганографії це особливо корисно, адже навіть якщо приховане повідомлення буде витягнуте, будь-яке втручання або спроба зміни інформації буде одразу виявлена [3].

Висновки

Симетричне шифрування залишається базовим інструментом захисту інформації завдяки своїй високій швидкодії та стійкості, де критичною умовою безпеки є наявність попередньо згенерованого спільного ключа та його сувора конфіденційність. Сучасні стандарти, такі як

блочний алгоритм AES-256 та потоковий шифр ChaCha20, демонструють високу ефективність у різних сценаріях застосування. Окремої уваги заслуговує підхід автентифікованого шифрування, реалізована у поєднанні ChaCha20-Poly1305, яка гарантує одночасно конфіденційність, цілісність та автентичність даних, дозволяючи миттєво виявити будь-яке втручання або підробку. У контексті стеганографії використання таких алгоритмів створює необхідний додатковий захист, адже навіть у разі виявлення прихованого каналу зв'язку, зміст повідомлення залишатиметься недоступним для сторонніх осіб, що робить ці криптографічні рішення невід'ємною частиною сучасних систем захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Римчук, І., Костючко, С., Поліщук, М., Гринюк, С., & Конкевич, Л. (2024). БЕЗПЕКА КОМУНІКАЦІЙНИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ ВІЗУАЛЬНОЇ КРИПТОГРАФІЇ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2(26), 258–267. https://doi.org/10.28925/2663-4023.2024.26.677
2. National Institute of Standards and Technology. Advanced Encryption Standard (AES). *Federal Information Processing Standards (FIPS) Publication 197*. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.
3. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 7539. *Internet Engineering Task Force (IETF)*, 2015. 46 p. URL: https://datatracker.ietf.org/doc/html/rfc7539

Оболонська Яна Олександрівна – студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com

Науковий керівник: ***Лукічов Віталій Володимирович*** – доцент, кафедри захисту інформації, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua

Obolonska Yana Oleksandrivna - student of group 1BS-22b, faculty of information technologies and computer engineering, citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com

Research supervisor: ***Lukichov Vitaliy Volodymyrovych*** – associate professor, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lukichov.vitalyi@vntu.edu.ua