УДК 004.056.55 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.172

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Чалий Д.В.
Науковий керівник – ст. вик. кандидат технічних наук Калюжний М.М.
кафедри інформаційно-Мережної інженерії
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
email: dmytro.chalyi@nure.ua

Cryptographic methods of information security are one of the key elements of modern information security; they themselves help to protect special information from malicious actors. These methods include a variety of encryption methods: symmetric and asymmetric encryption, hash functions, digital signatures, authentication and key exchange protocols, as well as cryptographic mechanisms such as factor authentication and quantum cryptography. Yu. The combination of all these methods makes it possible to create complex data protection systems that ensure a reliable level of security in the current digital environment.

Криптографічні методи захисту інформації є одним з ключових елементом сучасної інформаційної безпеки. Ці методи включають різні способи шифрування: симетричне та асиметричне шифрування, хеш-функції, цифрові підписи, протоколи аутентифікації та обмін ключами, а також криптографічні механізми факторної аутентифікації та квантову криптографію. Поєднання всіх цих методів дозволяє створити комплексні системи захисту даних, що забезпечують надійний рівень безпеки в сучасному цифровому середовищі.

Класифікація методів криптографічного захисту даних:

- Симетричне шифрування;
- Асиметричне шифрування;
- Хеш-функції;
- Цифровий підпис;
- Протоколи аутентифікації та обміну ключами;
- Контейнери даних та цифрові підписи;
- Криптографія мультифакторної аутентифікації;
- Квантова криптографія.

Симетричне шифрування - це метод в якому використовується один і той самий ключ як для шифрування, так і для розшифрування повідомлень. Головна мета цього методу запобігання отримання ключа, так як без нього розшифрувати дані не можливо. Приклади алгоритмів симетричного шифрування: AES, IDEA, Blowfish, Twofish, DES. Цей метод використовується в захисті даних в інтернеті, мобільних додатках, зберігання даних на сервері та в інших сверах.

Асиметричне шифрування – це метод в якому використовуються відкритий ключ, він використовує пари ключів: приватний і публічний. Публічний ключ використовується для шифрування повідомлень, а приватний ключ використовується для розшифрування. Цей метод використовується в багатьох сверах. В протоколах передачі даних, як TLS/SSL, та для шифрування трафіку,

цифрових підписах, SSH для безпечного з’єднання з віддаленим сервером, PGP/GPG для захисту електронної пошти та файлів, та в авторизації і аутентифікація.

Хеш-функції - це криптографічні алгоритми, які приймають вхідні обсях даних будь-якої довжини і перетворюють їх у фіксований вихідний хеш-код фіксованої довжини. Основна ціль хеш-функцій полягає в тому, що вони повинні бути односторонніми для того щоб неможливо було віднтворити вихідних даних з хеш-коду, стійкими до колізій (різних вхідних даних, що дають один і той самий хеш) та незмінні (той самий вхід завжди дає один і той самий вихід). Хеш-функції часто використовуються для перевірки цілісності даних. Це означає, що вони дозволяють перевірити, чи були дані змінені або пошкоджені під час передачі чи зберігання. Також хеш-функції використовуються для створення унікальних ідентифікаторів для об'єктів, файлів, повідомлень. Це може бути використано для швидкого пошуку чи ідентифікації об'єктів. Хеш-функції використовуються також для збереження паролів у вигляді хеш-кодів. Взамін зберігання самого пароля, система зберігає його хеш-код, що забезпечує більшу безпеку, оскільки паролі не зберігаються у відкритому вигляді. Також один з випадків використання хеш функцій для створення цифрових підписів, які дозволяють перевірити автентичність повідомлення та ідентифікацію відправника. Використовуються хеш-функції:

- Хеш-функції використовуються в криптографічних протоколах та системах для забезпечення безпеки даних;
- Хеш-функції використовуються для швидкого пошуку та індексації даних у базах даних;
- Хеш-функції використовуються для перевірки цілісності файлів та даних, що передаються через мережу;
- Хеш-функції використовуватися для створення унікальних ідентифікаторів для доступу до ресурсів чи послуг;
- Хеш-функції використовуються для збереження та обробки паролів користувачів в різних системах та сервісах.

Квантова криптографія базується на принципах квантової механіки для забезпечення безпеки комунікаційних каналів. Основною ідеєю квантової криптографії є використання фізичних властивостей квантових систем для забезпечення безпеки передачі даних. Вона дає надійну захист від криптоаналізу квантовими комп'ютерами, які можуть швидко розв'язувати складні математичні проблеми, що застосовуються у сучасних криптографічних алгоритмах.

Список використаних джерел:

1. Dong L., Chen K. Cryptographic Protocol. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. URL: https://doi.org/10.1007/978-3-642-24073-7;
2. Otruba K. CEC1702 Cryptographic Embedded Controller - Data Sheet. Microchip Technology Incorporated, 2016.
3. Petrov A. a. Computer security. Cryptographic methods of protection. Book on Demand Ltd., 2018. 450 p.