Секція 1

АНАЛІЗ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ

Лісних О. І.
Національний аерокосмічний університет ім. М. Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Морозова О. І.

Актуальність. Сьогодні криптографія має велике значення для більшості сучасних технологій, наприклад, електронної комерції або цифрового документообігу. Дані, які передаються з однієї системи в іншу через загальнодоступну мережу, повинні бути захищеними за допомогою методів шифрування, а саме алгоритмів цифрового підпису. Довести те, що певний документ не був змінений або підроблений, має значну роль, бо весь світ пов'язаний з документообігом. Отже, можна зробити висновок, що важливо використовувати алгоритм, який дає гарантію цілісності даних та аутентифікації власника [1-2].

Мета роботи полягає в аналізі основних чотирьох алгоритмів цифрового підпису та визначити, який саме з алгоритмів має наразі переваги в порівнянні з іншими.

Основні положення. Розглянемо основні чотири алгоритми цифрового підпису [3-5]. Ця вибірка алгоритмів має змогу описати картину сучасного документообігу на дуже високому рівні. Серед них представлено алгоритми, які набирають суттєвих оборотів серед розробників та використовуються в сервісах. В цих алгоритмах необхідно звернути основну увагу на генерацію ключів, генерацію та перевірку підпису, а також розглянути математичне обґрунтування кожного алгоритму, щоб дізнатися про їх крипостійкість, що є одним з потрібних параметрів для повного порівняння.

Rivest, Shamir и Adleman (RSA) – криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності завдання факторизації великих цілих чисел, що означає, що чим більша послідовність чисел у вас є, тим більше ви захищені. Алгоритм RSA був розроблений в Массачусетському технологічному інституті (MIT) у 1977 році Роном Рівестом, Аді Шаміром і Леонардом Адельманом.

ElGamal – криптосистема, яку засновано на складності обчислення дискретних логарифмів у скінченному полі. Криптосистема включає у себе алгоритм шифрування та алгоритм цифрового підпису. Схема підпису ElGamal дозволяє верифікатору підтвердити автентичність повідомлення, надісланого підписувачем через незахищений канал. Цей алгоритм описав Тахер Ель-Гамал у 1984 році.

Digital Signature Algorithm (DSA) – криптографічний алгоритм, який засновано на складності обчислення дискретних логарифмів у скінченному полі. Алгоритм запропоновано у 1991 та він створений лише для електронного підпису.

В тому ж році було запропоновано алгоритм Elliptic Curve Digital Signature Algorithm (ECDSA) – це криптографічно захищена схема цифрового підпису, заснована на криптографії еліптичної кривої (ECC). Алгоритм підписання/перевірки ECDSA базується на математичний опис циклічних груп еліптичних кривих над кінцевими полями та на складність проблеми дискретного логарифмування еліптичної кривої (ECDLP).

Висновки. Робота присвячена порівняльному аналізу алгоритмів цифрового підпису. Було проведено аналіз кожного з чотирьох алгоритмів, які використовують метод відкритого ключа, та було досліджено недоліки та переваги кожного з запропонованих алгоритмів Виявлено, що алгоритм RSA має переваги у порівнянні з іншими алгоритмами, а саме надає гарантії цілісності даних та аутентифікацію власника, має невеликий розмір пари ключів, досить непогану швидкодійність та велику криптостійкість.

Список літератури

1. Information Security Stack Exchange. *Stackexchange*. URL – https://security.stackexchange.com (дата звернення: 23.10.2022);

2. Digital signatures. *Cryptobook*. URL – https://cryptobook.nakov.com/digital-signatures/ (дата звернення: 27.10.2022);

3. What Are the Differences Between RSA, DSA, and ECC Encryption Algorithms? *Sectio*. URL – https://sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption (дата звернення: 25.10.2022);

4. Comparing SSH Keys – RSA, DSA, ECDSA, or EdDSA? *Goteleport*. URL – https://goteleport.com/blog/comparing-ssh-keys/ (дата звернення: 29.10.2022);

5. Xianmeng Meng, Xuexin Zheng, Cryptanalysis of RSA with a small parameter revisited. Information Processing Letters, Elsevier, p. 858–862.

Відомості про авторів

Лісних Олександр Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0638118220, o.lisnykh@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., професор, o.morozova@csn.khai.edu