Секція 1

АНАЛІЗ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ ДЛЯ РОЗРОБЛЕННЯ ЗАХИЩЕНОЇ СИСТЕМИ ПІДПИСАННЯ ФАЙЛІВ З МОЖЛИВІСТЮ ВИБОРУ АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ

Проценко Є. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні, в умовах зростаючого використання електронних документів та обміну інформацією в мережі, питання забезпечення безпеки та цілісності даних стають дедалі більш актуальними. Захищена система підписування файлів, яка надає можливість вибору алгоритму цифрового підпису, відіграє важливу роль у цьому контексті. Дані, що передаються та зберігаються в електронному форматі, повинні бути надійно захищеними від несанкціонованого доступу, змін та підробки. Тому аналіз алгоритмів цифрового підпису для розробки захищеної системи підписування файлів з можливістю вибору алгоритму цифрового підпису є надзвичайно актуальною та важливою темою для досліджень, що сприяє підвищенню рівня безпеки та довіри в інформаційному середовищі [1].

Мета роботи полягає в аналізі алгоритмів цифрового підпису для розроблення та впровадження захищеної системи підписування файлів, яка надає користувачам можливість вибору алгоритму цифрового підпису.

Основні положення. В роботі пропонується розглянути чотири основні алгоритми цифрового підпису [2-4]:

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.

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.

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).

Edwards-curve Digital Signature Algorithm – криптографічно захищена схема цифрового підпису, заснована на кривих Едвардса. EdDSA використовує стійкість відносно проблеми дискретного логарифмування на кривій Едвардса та надає високий рівень безпеки при невеликих розмірах ключів. Алгоритм детерміністичний, забезпечуючи ефективність та захист від різноманітних атак, і дозволяє підписувати повідомлення без попереднього обчислення хешу. EdDSA є ефективним і безпечним рішенням для цифрового підпису в різних сценаріях застосування.

Вибір чотирьох алгоритмів дозволяє представити ландшафт сучасного документообігу. Серед цих алгоритмів важливо звернути увагу на аспекти, такі як генерація ключів, процеси створення та перевірки підпису, а також ретельно розглянути математичну основу кожного алгоритму. Це дозволяє нам визначити їхню криптостійкість, що є ключовим параметром для повного та об'єктивного порівняння.

Висновки. Робота присвячена порівняльному аналізу алгоритмів цифрового підпису для подальшої розробки системи підписання файлів з можливістю вибору цифрового підпису. Було проведено аналіз кожного з чотирьох алгоритмів, які використовують метод відкритого ключа. Після проведення досліджень недоліків та переваг кожного з запропонованих алгоритмів було зроблено висновок, що алгоритм RSA є найбільш підходящим та надає гарантії цілісності даних та аутентифікацію власника, а також має невеликий розмір пари ключів.

Список літератури

1. Digital signatures. *Cryptobook*. URL – https://cryptobook.nakov.com/digital-signatures/ (дата звернення: 10.20.23);
2. What Are the Differences Between RSA, DSA, and ECC Encryption Algorithms? *Sectigo*. URL – https://sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption (дата звернення: 13.20.23);
3. Comparing SSH Keys – RSA, DSA, ECDSA, or EdDSA? *Goteleport*. URL – https://goteleport.com/blog/comparing-ssh-keys (дата звернення: 13.20.23);
4. What are the advantages and disadvantages of RSA, DSA, and ECDSA for SSH? *Linkedin*. URL – https://www.linkedin.com/advice/1/what-advantages-disadvantages-rsa-dsa-ecdsa-ssh (дата звернення: 15.20.23).

Відомості про авторів

Проценко Єгор Сергійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.protsenko@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, o.morozova@csn.khai.edu