У сучасному світі технологій та інформаційних систем, питання безпеки та захисту даних стали надзвичайно важливими. Кожен день ми взаємодіємо з різними цифровими ресурсами, від соціальних мереж до банківських послуг, і всі ці операції повинні бути захищені від несанкціонованого доступу або змін. Одним з основних інструментів для забезпечення безпеки є криптографія, яка дозволяє захищати передавання даних і забезпечує конфіденційність, цілісність та аутентичність інформації.

Криптографія — це наука про методи захисту інформації. Вона застосовується для забезпечення безпеки даних, їхнього шифрування та підпису. Існує кілька основних видів криптографії, зокрема симетрична, асиметрична та гібридна криптографія. Симетрична криптографія використовує один і той самий ключ для шифрування та дешифрування інформації, що створює певні ризики, пов’язані з безпекою цього ключа. Асиметрична криптографія, навпаки, використовує пару ключів — публічний та приватний, що дозволяє значно знизити ризики при обміні ключами.

Одним з найбільш популярних та ефективних методів асиметричної криптографії є алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm), який використовує еліптичні криві для підпису повідомлень. Цей метод дозволяє забезпечити високу безпеку навіть при використанні порівняно коротших ключів, що робить його дуже привабливим для використання в сучасних мобільних та веб-технологіях. Однією з основних переваг ECDSA є його висока ефективність, що дозволяє здійснювати підпис та верифікацію підписів з мінімальними витратами ресурсів.