ПІДВИЩЕННЯ КРИПТОСТІЙКОСТІ СХЕМИ ШИФРУВАНИЯ ECIES У СИСТЕМАХ БЕЗПЕКИ

Виконав: Зварич А. О.
Керівник: Яремчук Ю. Є.

АКТУАЛЬНІСТЬ ТЕМИ

- Серед математичних апаратів на яких побудовані сучасні криптоалгоритми особливої уваги заслуговує математичний апарат на основі еліптичних кривих.
- Серед великої кількості криптосистем, заснованих на ECC, найбільш відома схема інтегрованого шифрування з еліптичною кривою (ECIES).
- У даній роботі розглядається недолік ECIES, пов’язаний з вразливістю до атак малими підгрупами і можливість використання алгоритму знаходження контрольної суми, для перевірки ключів на цілісність.

ПОСТАНОВКА ЗАДАЧІ

- **Метою** є підвищення криптостійкості алгоритму шифрування на еліптичних кривих ECIES.
- **Об’єкт дослідження** – публічний ключ алгоритму ECIES.
- **Предмет дослідження –** метод обчислення контрольної суми публічного ключа алгоритму ECIES за допомогою циклічного надлишкового коду.
- **Новизна результатів.** Новизна одержаних результатів полягає в новому методі перевірки публічних ключів на справжність, що значно підвищує криптостійкість алгоритму ECIES.
- **Практична цінність.** Практична цінність полягає в розробці ПЗ, що дозволяє надійно шифрувати інформацію без можливостей взлому для зловмисника.

АНІЛІЗ ІНСНУЮЧИХ АСИМЕТРИЧНИХ МЕТОДІВ ШИФРУВАННЯ ДАНИХ

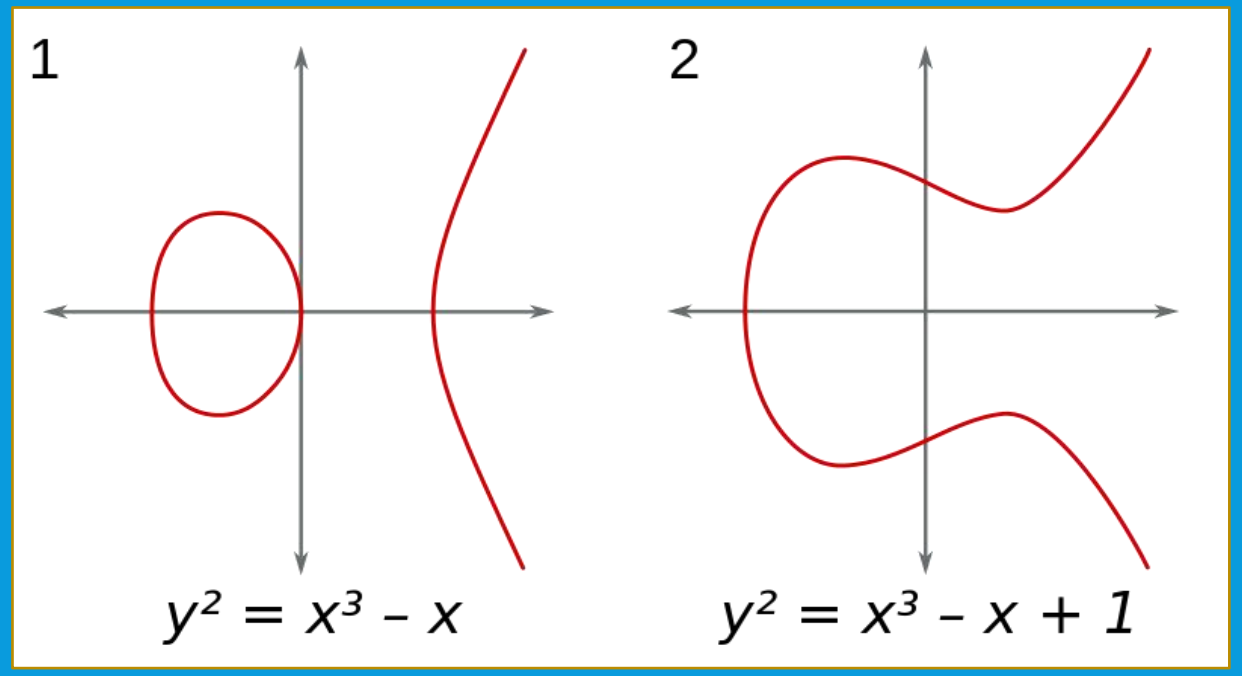
Рівень безпеки (біт)	Довжина ключа RSA (біт)	Довжина ключа ECIES (біт)
80	1024	160-223
112	2048	224-255
128	3072	256-283
192	7680	384-511
256	15360	512-571

ЕЛІПТИЧНІ КРИВІ

Асиметрична криптографія заснована на складності рішення деяких математичних задач. Ранні криптосистеми з відкритим ключем, такі як алгоритм RSA, криптостійкі завдяки тому, що складно розкласти велике число на прості множники. При використанні алгоритмів на еліптичних кривих припускається, що не існує субекспоненційних алгоритмів для вирішення завдання **дискретного логарифмування в групах їх точок**.

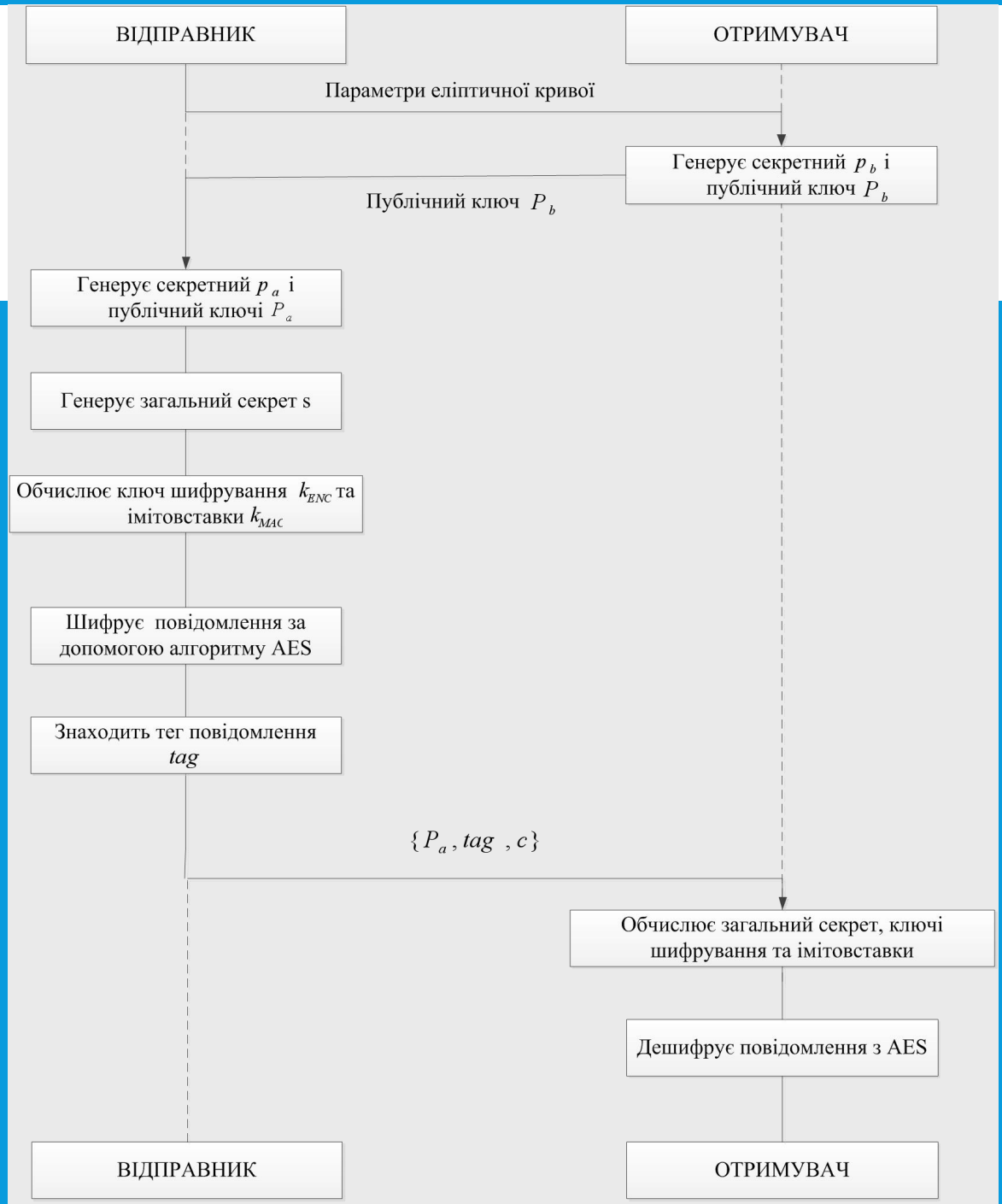
Еліптична крива над полем K — це множина точок проективної площини над K, що задовольняють рівнянню

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$



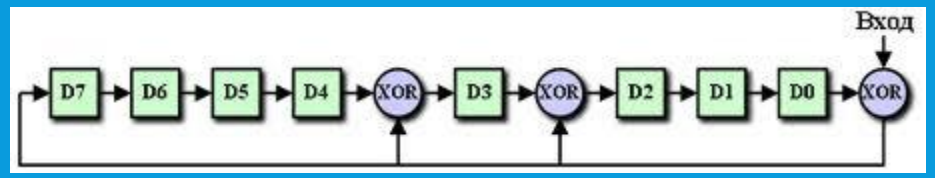
ECIES

- ECIES — це схема шифрування на відкритих ключах, що ґрунтується на еліптичних кривих. Цю схему запропонував Віктор Шоуп 2001. ECIES використовується в різних стандартах, наприклад ANSI X9.63, IEEE 1363a, ISO 18033-2 і SECG SEC 1.



CRC-32

Циклічний надлишковий код — алгоритм обчислення контрольної суми, призначений для перевірки цілісності даних. CRC є практичним додатком завадостійкого кодування, заснованому на певних математичних властивостях циклічного коду.



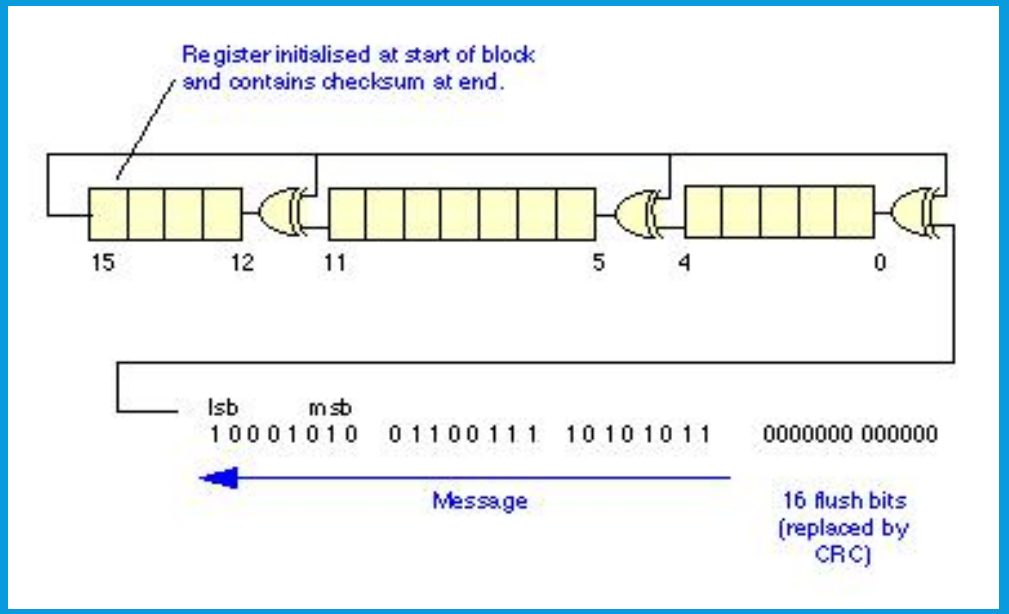
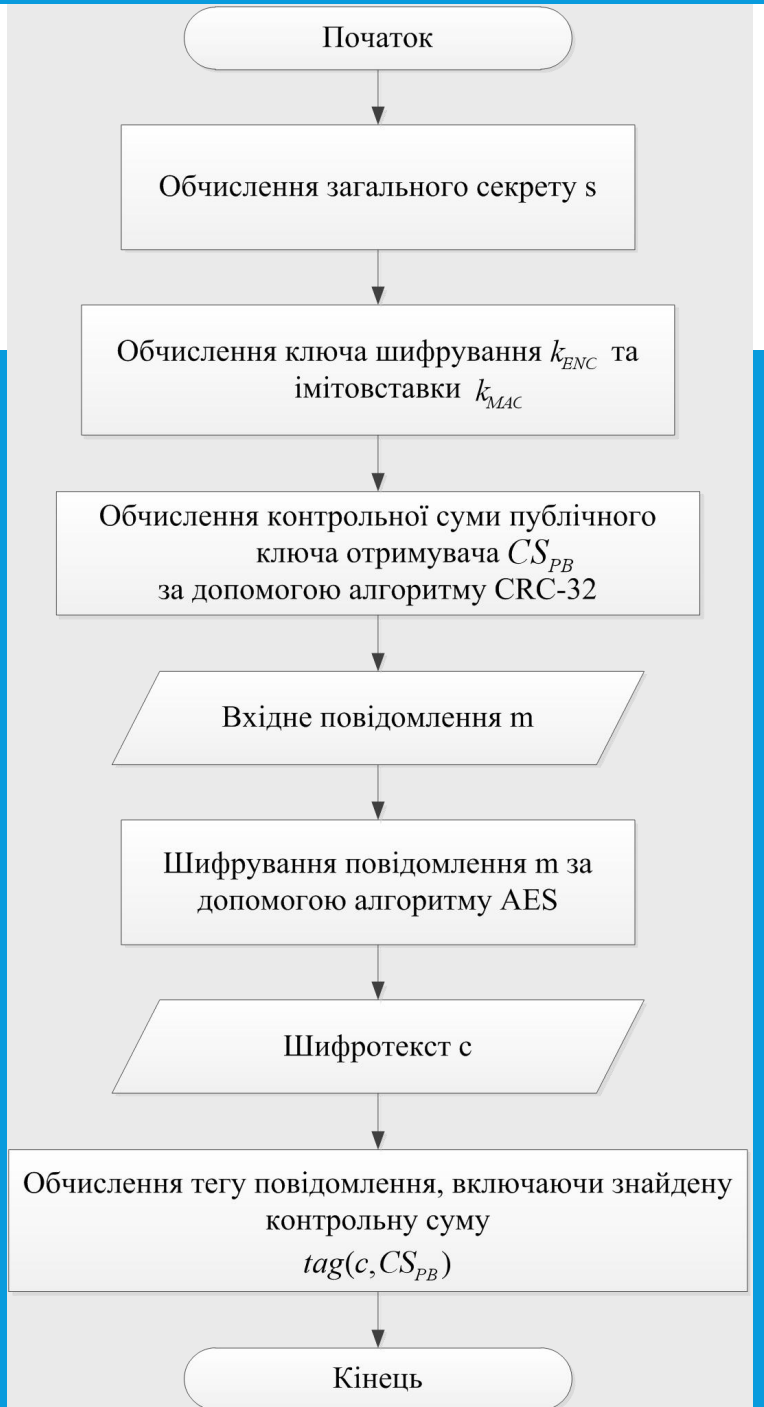


СХЕМА УДОСКОНАЛЕНОГО АЛГОРИТМУ ECIES

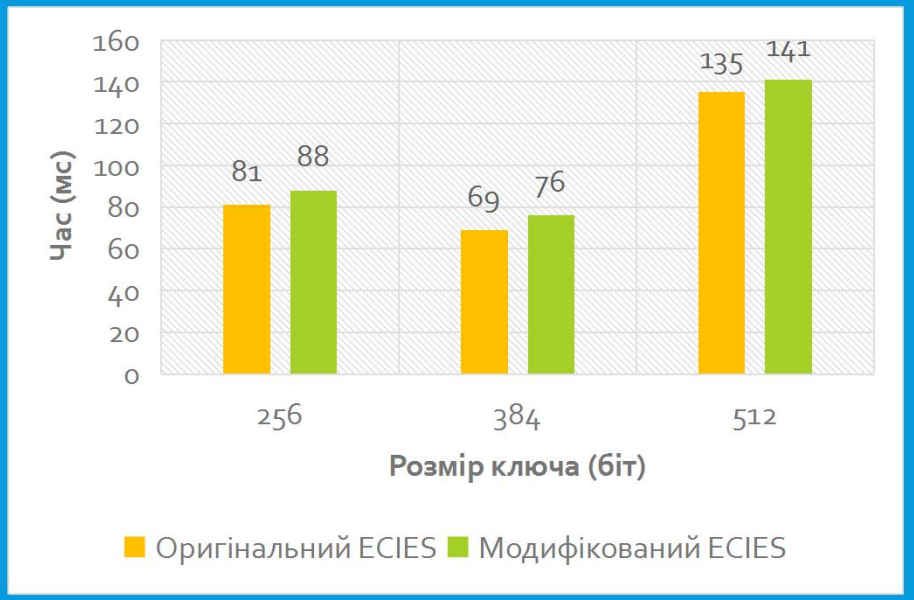
Модифікація полягає у обчисленні контрольної суми ключа отримувача і подальшого її використання в функції MAC разом із k_{MAC} та зашифрованим повідомленням.

Для перевірки тега отримувач також має обчислити тег повідомлення, використовуючи контрольну суму.

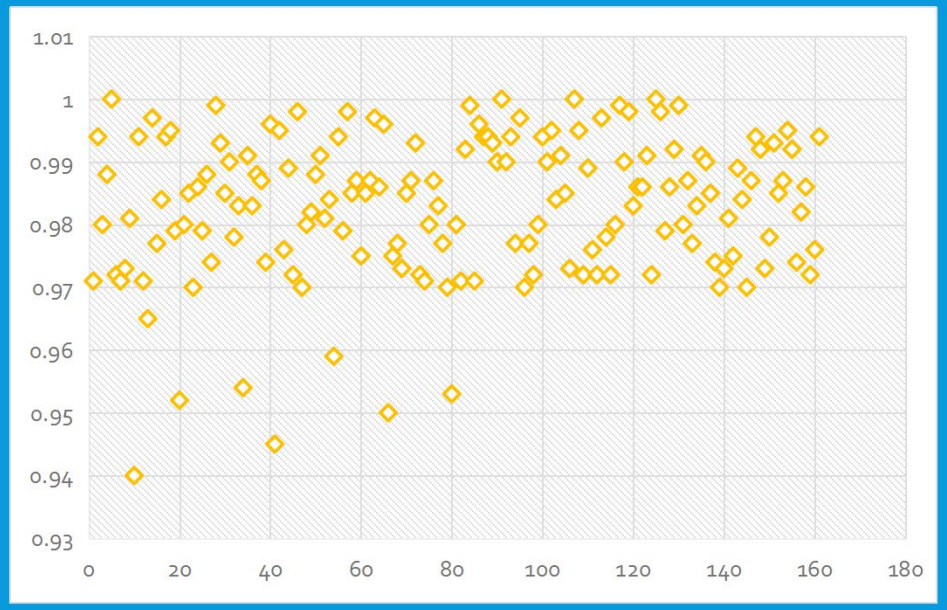


ПОРІВНЯННЯ ШВИДКОСТІ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ОРИГІНАЛЬНОГО АЛГОРИТМУ ТА МОДИФІКОВАНОГО

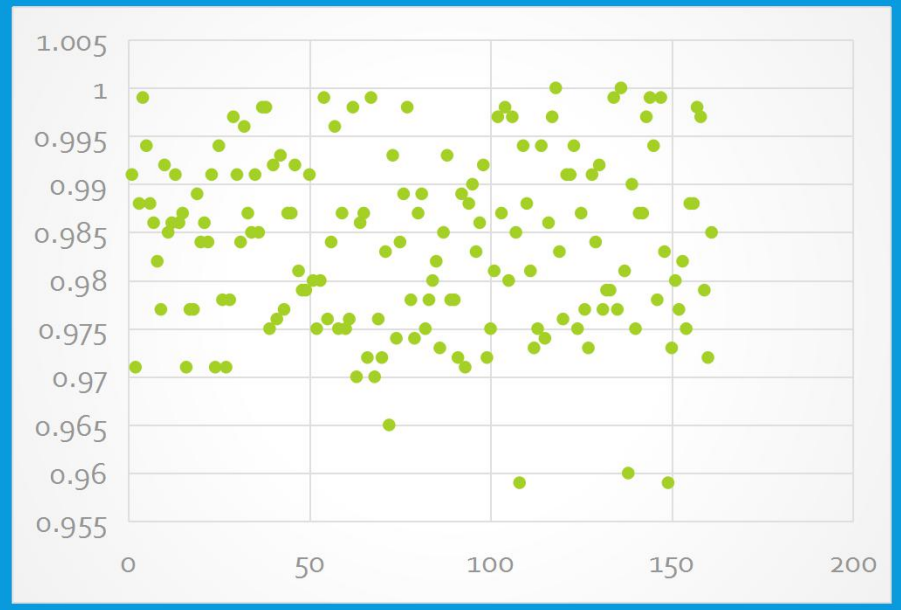
	Час (мс)			
Довжина ключа (біт)	Шифрування		Дешифрування	
	Оригінальний ECIES	Модифікований ECIES	Оригінальний ECIES	Модифікований ECIES
256	81	88	61	63
384	69	76	50	54
512	135	141	109	112



ПОРІВНЯННЯ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ОРИГІНАЛЬНОГО ТА МОДИФІКАОВАНОГО АЛГОРИТМІВ



Результати тестування оригінального алгоритму ECIES



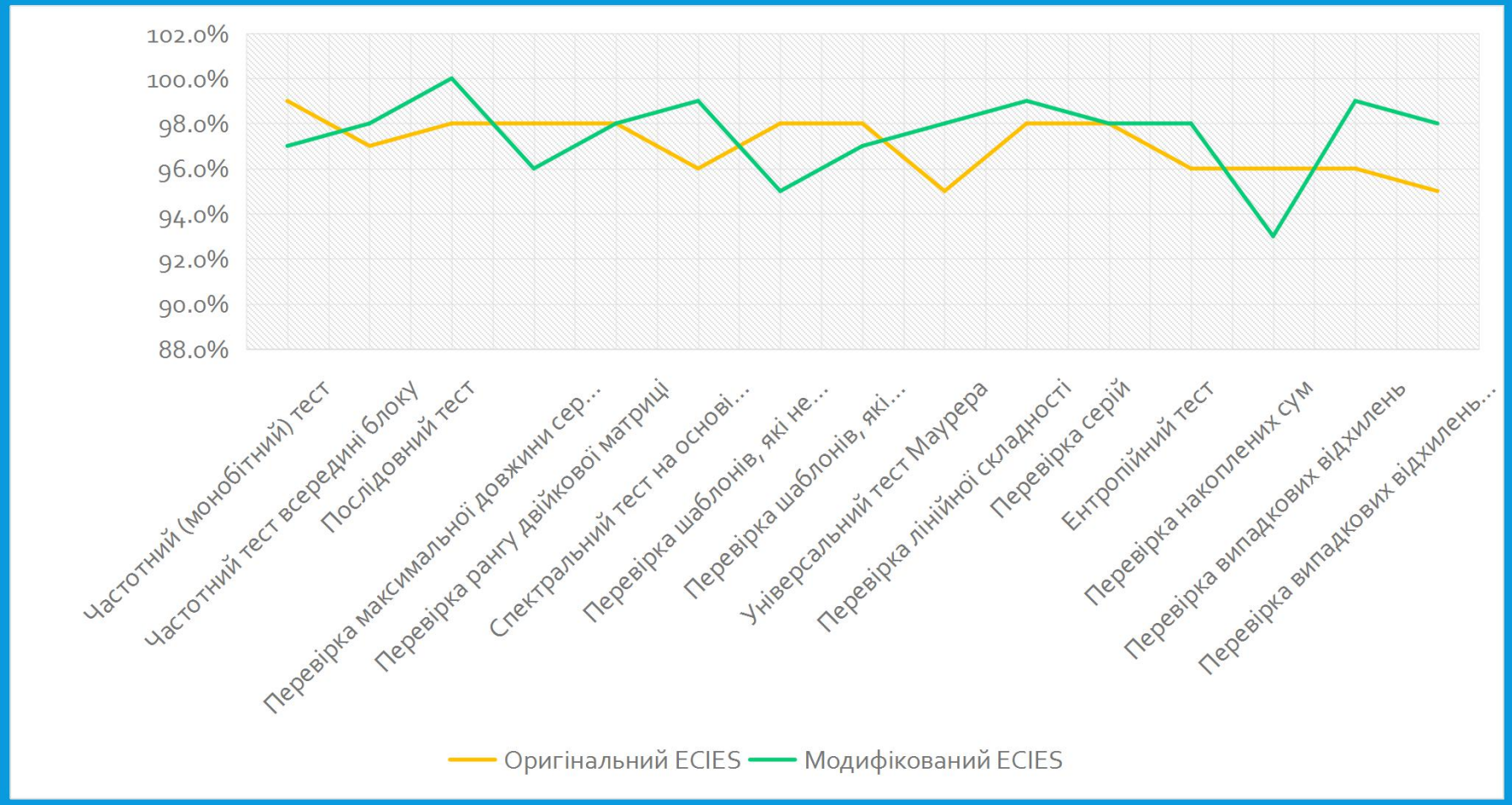
Результати тестування модифікованого алгоритму ECIES

РЕЗУЛЬТАТ ПРОВЕДЕННЯ СТАТИСТИЧНОГО АНАЛІЗУ НА ОСНОВІ ПАКЕТУ ТЕСТІВ NIST

Назва статистичного тесту	Оригінальний ECIES	Модифікований ECIES
Частотний (монобітний) тест	99%	97%
Частотний тест всередині блоку	97%	98%
Послідовний тест	98%	100%
Перевірка максимальної довжини серії в блоці	98%	96%
Перевірка рангу двійкової матриці	98%	98%
Спектральний тест на основі дискретного перетворення Фур'є	96%	99%
Перевірка шаблонів, які не перекриваються	98%	95%
Перевірка шаблонів, які перекриваються	98%	97%
Універсальний тест Маурера	95%	98%
Перевірка лінійної складності	98%	99%
Перевірка серій	98%	98%
Ентропійний тест	96%	98%
Перевірка накоплених сум	96%	93%
Перевірка випадкових відхилень	96%	99%
Перевірка випадкових відхилень (модифікація)	95%	98%

- Алгоритм із вбудованим запропонованим методом перевірки публічного ключа на справжність показав кращі результати в більшості тестів на 1-3%, що свідчить про його вищий рівень статистичної безпеки.

ГРАФІЧНЕ ВІДОБРАЖЕННЯ РЕЗУЛЬТАТУ ПРОХОДЖЕННЯ СТАТИСТИЧНИХ ТЕСТІВ



ВИСНОВКИ

- Було розглянуто та досліджено проблему вразливості асиметричної криптосхеми ECIES до атаки малими підгрупами, а також підвищено її криптостійкість шляхом використання циклічного надлишкового коду.
- Проведено статистичний аналіз модифікованого та оригінального алгоритму ECIES, а також проведено порівняння їх статистичних портретів. Алгоритм із вбудованим запропонованим методом перевірки публічного ключа на справжність показав кращі результати в більшості тестів на 1-3%, що свідчить про його вищий рівень статистичної безпеки

ДЯКУЮ ЗА УВАГУ