

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Методи реалізації криптографічних механізмів

## ЛАБОРАТОРНА РОБОТА №3

Виконали студенти  
групи ФІ-12мн  
Ковалевський Олександр  
Ткаченко Артем  
Чашницька Марина

## **1 Мета роботи**

Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем

## **2 Постановка задачі та варіант завдання**

Розробити реалізацію асиметричної криптосистеми за допомогою бібліотеки PyCrypto під Linux платформу. Стандарт ДСТУ 4145-2002.

## **3 ДСТУ 4145-2002**

Цей стандарт установлює механізм цифрового підписування, оснований на властивостях груп точок еліптичних кривих над полями  $GF(2^m)$ , та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства.

У цьому стандарті є посилання на такі стандарти:

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ 34.311-95 Информационная технология. Криптографическая функция хеширования.

## **4 Реалізація**

DigitalSignature.py – механізм цифрового підпису

EllipticCurve.py – операції з еліптичною кривою

GOST28147-89.py – шифр ГОСТ 28147-89

GaloisField.py – операції з полями Галуа

Generator.py – генератор випадкових послідовностей

User.py – дії користувача

main.py – сценарій взаємодії між користувачами

```
Alice's signed message: Hello, Bob! 0xafe6bf60e172d58688d84f93461fa2d5c90f0612603500000000000000000164d63563fc64541c76fc1b7bc06ed570398ff3d80353
Bob verification: True
Bob's signed message: Hey! 0x3d7f3fd24fb71f0b2dd3bde31b5fa48d17751a194712300000000000000000003fc692ba464eedb6340f05f4bcbf120556a15c4e7e58
Alice verification: True
Eva's signed message: Go kill yourself, Bob! 0x261559f3ee3620ff091a61f89415991bb4dfa757efd970000000000000000001eb18defb5eabd6da059e6e0e3be15c7d1f6beded6a0c
Bob verification Eva's message via Alice's public key: False
Bob verification Eva's message via Eva's public key: True

real    3m27.614s
user    3m27.180s
sys     0m0.093s
```

**Рисунок 1** – Результат виконання

## ВИСНОВКИ

Було досліджено можливості побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем. Зокрема, розроблена реалізація асиметричної криптосистеми за допомогою бібліотеки PyCrypto під Linux платформу (стандарт ДСТУ 4145-2002).