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

Київ — 2021

1 Мета роботи

Дослідження можливостей побудови загальних та спеціалних 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

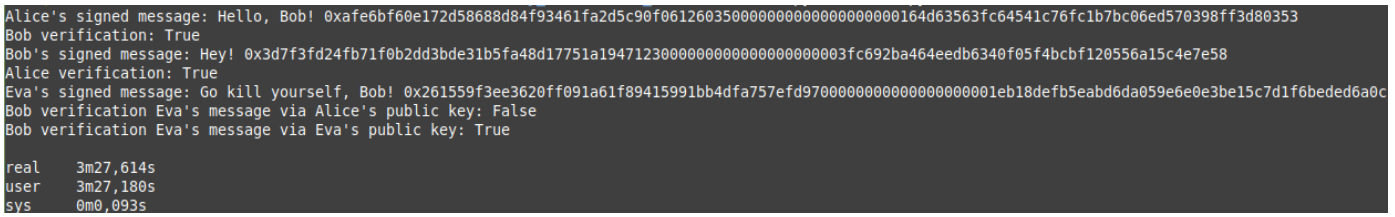

Рисунок 1 – Результат виконання

ВИСНОВКИ

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