Національний технічний університет України
«Київський політехнічний інститут»

Фізико технічний інститут

Кафедра математичних методів захисту інформації

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

Лабораторна робота №3

Тема: “Реалізація основних асиметричних криптосистем.”

Виконали:
Драга Владислав ФІ-12мп
Чіхладзе Вахтанг ФІ-12мн

Перевірила
Селюх П.В.

Київ 2021

Мета роботи: Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

Завдання:
Використовуючи бібліотеку PyCrypto під Linux платформу реалізувати стандарт ДСТУ 4145-2002.

Посилання на вихідний код:
https://github.com/d-laslo/MPKM-21-22/tree/main/lab3

Хід роботи

ДСТУ 4145-2002 стандарт, що ґрунтується на еліптичних кривих який описує механізм формування та перевірки електронного цифрового підпису, що базується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$ та правилах застосування цих механізмів 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 ході роботи зі стандарту було скопійовано рекомендовані параметри у json файли, що знаходяться в папці elliptic_curve_parameters . Для тесту було використано таке представлення:

```
{
        "p": "0x800000000000000000000000000000000000000c9",
        "m": "0xa3",
        "a": "0x1",
        "b": "0x5FF6108462A2DC8210AB403925E638A19C1455D21",
        "n": "0x400000000000000000002BEC12BE2262D39BCF14D"
    }
```

Перш за все було реалізовано клас точки еліптичної кривої EllipticCurvePoint, що приймає на вхід рекомендовані параметри зі стандарту у вигляді json об’єкту. Методи класу мають операції суми точок, множення точок та порівняння точок.

Далі реалізували клас еліптичної кривої EllipticCurve, що інкапсулює клас точки еліптичної кривої. Даний клас реалізовує операції над точками еліптичної кривої. Такі як множення точок, обчислення сліду, обчислення полусліду, функцію стиснення, функцію розтиснення та генерування випадкової точки еліптичної кривої.

Маючи базу для побудови криптографічного механізму було реалізовано клас DSTU що реалізовує механізми підпису та перевірки підпису. Алгоритм використання даної криптосистеми такий:
1.сформувати dstu об’єкт DSTU де вказуємо json з параметрами.
2.взяти повідомлення m як строкову змінну та передати її методу sign(m,dstu.private_key) і отримаємо об’єкт підпису s
3.для перевірки повідомлення викликаємо функцію verify(s,dstu.public_key), що повертає true, якщо підпис вірний.Інакше поверне false.

Висновок: нами було досліджено ДСТУ 4145-2002 та реалізовано за допомогою бібліотеки PyCrypto криптографічні механізм цифрового підпису, що описані в цьому стандарті. Також реалізували операції над точками еліптичної кривої, які є базисом для обчислення цифрового підпису.

Посилання:

1. ДСТУ 4145-2002 https://itender-online.ru/wp-content/uploads/2017/09/dstu-4145-2002-1.pdf