МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Кібербезпеки

ЛАБОРАТОРНА РОБОТА

з дисципліни «Методи реалізації криптографічних механізмів»

Тема: Бібліотека PyCrypto під Linux платформу. Стандарт ДСТУ 4145-2002

Виконав:
студент 2 курсу
групи ФБ-11мн
Мохонько М.М.

Мета:
Отримання практичних навичок побудови гібридних криптосистем.

Завдання:
Розробити реалізацію асиметричної криптосистеми у відповідності до стандартних вимог Crypto API або стандартів PKCS та дослідити стійкість стандартних криптопровайдерів до атак, що використовують недосконалість механізмів захисту операційної системи.

Бібліотека PyCrypto під Linux платформу. Стандарт ДСТУ 4145-2002.

Хід роботи:
Для реалізації криптосистеми у відповідності до стандартних вимог Crypto API використаємо реалізовану в лабораторній роботі №3 систему цифрового підпису за стандартом ДСТУ 4145-2002.

Для виконання цього завдання було написано клас обгортка, що викликає функції класу DSTU. А саме:

1. generate_private_key()
2. generate_public_key()
3. export_private_key()
4. export_public_key()
5. import_private_key()
6. import_public_key()
7. sign()
8. verify()
9. del_private_key()
10. del_public_key()

Як недолік операційної системи можна виділити генерацію випадкових чисел на основі ентропії. Відомо, що ентропія в Linux залежить від випадкових дій користувача. Якщо написати програму емулятор користувача, та взяти під контроль ентропію, то можна впливати на генерацію ключів і з великою точністю робити прогноз щодо бітів ключа. Знаючи які біти в ключі, перебір ключів значно зменшується, а це впливає на стійкість криптосистеми.

ВИСНОВКИ
Було досліджено один з векторів атак на генератор випадкових чисел, яким можна скомпрометувати генерацію ключів. Також було реалізовано клас обгортка над реалізованою криптосистемою з лабораторної роботи №3, що реалізує вимоги Crypto API.