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

Кафедра математичних методів захисту інформації

ЛАБОРАТОРНА РОБОТА №3

на тему: "Реалізація основних асиметричних криптосистем"

Виконали: студенти 5 курсу, групи ФІ-12мп
Бублик Єгор, Волинський Євгеній та Слуцький Андрій

Київ — 2021

1. Мета роботи

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

2. Завдання на лабораторну роботу

Розробити реалізацію асиметричної криптосистеми (Ель-Гамаля під Windows платформу, на основі PyCrypto).

3. Хід роботи

Під час першої спроби реалізації криптосистеми, використовуючи модуль $Crypto.PublicKey.ElGamal$, ми зіткнулися з великою кількістю проблем, пов'язаних з незручністю бібліотечної реалізації (наприклад — неможливість шифрувати відкритий безпосередньо), а також з частковою імплементацією C-коду в модулі $Crypto.Hash$.

Після безрезультатних спроб привести поточну програму до нормального та придатного вигляду, було прийняте рішення створити форк модуля $Crypto.PublicKey.ElGamal$ та допрацювати його, для максимізації UX та задоволення власного перфекціонізму.

Отже, наша релізація використовує лише модуль $Crypto.Util.number$, весь функціонал криптосистеми був або переписаний, або допрацьований. Серед особливостей власної реалізації схем шифрування та ЦП Ель-Гамаля: можливість зберігати та використовувати згенеровані ключі, автоматична генерація сесійного ключа з можливістю його оновлення, можливість шифрувати та підписувати *plaintext* а також видаляти ключі після використання.

4. Приклад роботи

Наведено у файлі $flow - tests.py$.

5. Висновки

Під час виконання лабораторної роботи ми створили власну реалізації схеми шифрування та цифрового підпису Ель-Гамаля, використовуючи лише модуль *Util.number* бібліотеки PyCrypto.

Коректність нашої реалізації підтвердили за допомогою $flow$-тестів, результат виконання кожного з яких збігається з очікуванням.

Під час виконання роботи ми набули навичок з дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.