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:
Корж Нікіта ФІ-12мн
Тафтай Анастасія ФІ-12мп
Мазур Анастасія ФІ-12мн

Перевірила
Селюх П.В.

Київ - 2021

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

Завдання: Розробити реалізацію асиметричної криптосистеми – **криптосистема Эль Гамаля під Windows платформу використовуючи бібліотеку BouncyCastle**. Оформлення результатів. Контрольний приклад роботи з асиметричною криптосистемою.

Хід роботи

Для реалізації криптосистеми Ель-Гамаля був використаний екземпляр класу `Cipher` та `KeyPairGenerator` бібліотеки Bouncy Castle.

Генерування ключів:

1. Обирається випадкове просте число p довжини ;
2. Обирається випадковий примітивний елемент g>1 з поля Z_p;
3. Обирається випадкове ціле число x>1 з поля Z_p;
4. Обчислюється $y = g^x mod p$;
5. Відкритий ключ це трійка (y,g,p), секретний ключ – x;

метод класу `KeyPairGenerator` визивав метод классу ***`ElGamalEngine - ElGamalKeyPairGenerator()`***, який генерує ключі, узгоджені для використання в криптосистемі, як описано на сторінці 164 (33 стр. у посиланні) «Handbook of Applied Cryptography».

Шифрування:

На вхід M – відкритий текст:

1. Обираємо випадковий ключ k: 1<k<p-1;
2. Обчислюються числа $c_1 = g^k mod p$ і $c_2 = y^k M mod p$;
3. Пара чисел (c_1, c_2) – шифротекст.

Вихід: (c_1, c_2)

Відбувається за допомогою методів класу `Cipher`: `init(boolean forEncryption, CipherParameters param)` - ініціалізація режиму(шифрування(1) та передавання ключа) і `doFinal()` - зашифрування тексту.

Розшифрування:

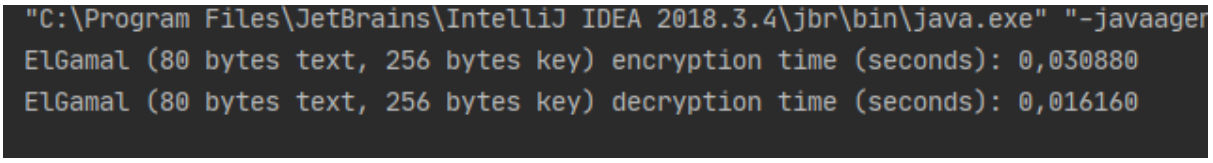
На вхід (c_1, c_2) – шифротекст:

1. $M = c_2 (c_1^x)^{-1} mod p$;

Вихід: M

Відбувається за допомогою методів класу *Cipher*: `init(boolean forEncryption,CipherParameters param)` - ініціалізація режиму (розшифрування(0) та передавання ключа) і `doFinal()` - розшифрування тексту.

Результат роботи програми:



Висновок:

Отже, було досліджено реалізацію зашифрування та розшифрування в бібліотеці `BouncyCastle.` Реалізовано роботу криптосистеми Ель-Гамаля, а саме: генерування ключів, зашифрування та розшифрування.