



Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ Лабораторна  
робота №3 Тема: “Реалізація основних асиметричних криптосистем”

Виконали:

Студенти групи ФІ-12мн

Мітрофанова Еліна

Морозюк Анастасія

Гетьман Дмитро

Перевірила:

Селюх П.В.

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

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

## Хід роботи

### Генерування ключів:

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

Для генерування простого числа  $p$  використовувався RNGCrypto Service Provider.

**RNGCrypto Service Provider** - реалізує криптографічний генератор випадкових чисел, використовуючи реалізацію, яку надає постачальник служб шифрування (CSP).

Для перевірки числа на простоту, було реалізовано тест простоти Міллера — Рабіна.

Для знаходження примітивного елемента ( *GeneratePrimitiveRoot*), додатково було реалізовано алгоритм факторізації ( *Factorize*).

### Шифрування:

На вхід  $M$  – відкритий текст:

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

Вихід:  $(c_1, c_2)$

Шифрування реалізовано в класі ElGamal у методі *Encryption*.

### Розшифрування:

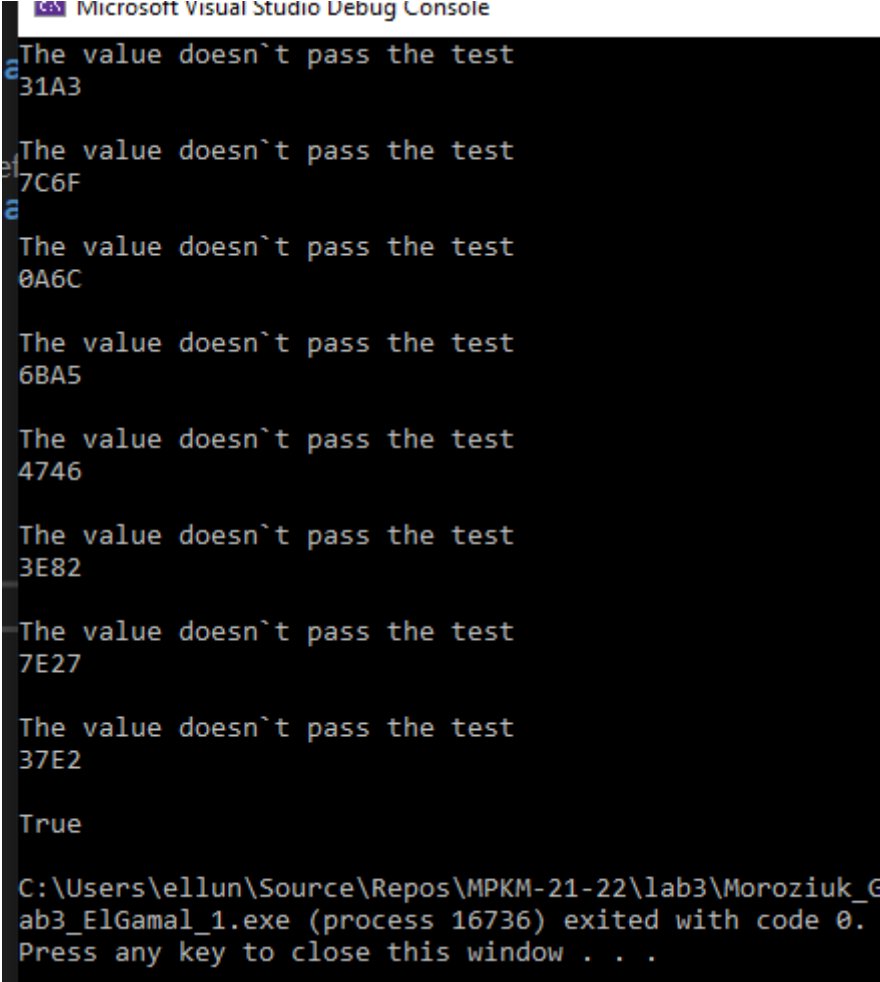
На вхід  $(c_1, c_2)$  – шифротекст:

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

Вихід:  $M$

Розшифрування виконується за допомогою методу *Decryption*.

Також, у консоль були виведені числа, які не пройшли тест Міллера-Рабіна та перевірка розшифрування ( якщо true: розшифрований тест співпадає з початковими даними).



```
Microsoft Visual Studio Debug Console

The value doesn't pass the test
31A3

The value doesn't pass the test
7C6F

The value doesn't pass the test
0A6C

The value doesn't pass the test
6BA5

The value doesn't pass the test
4746

The value doesn't pass the test
3E82

The value doesn't pass the test
7E27

The value doesn't pass the test
37E2

True

C:\Users\ellun\Source\Repos\MPKM-21-22\lab3\Moroziuk_G
ab3_ElGamal_1.exe (process 16736) exited with code 0.
Press any key to close this window . . .
```

**Висновок:** Отже, було досліджено реалізовано та досліджено роботу криптосистеми Ель-Гамал, а саме: генерування ключів, зашифрування та розшифрування.