Лабораторна робота №6 (Варіант 3)

**Тема**: Дослідження криптоалгоритму шифрування Ель-Гамаля

**Мета роботи**: дослідження структури алгоритму і методики практичної реалізації криптосистеми шифрування Ель-Гамаля.

Хід роботи

```python
import random

# Функція для пошуку найбільшого спільного дільника
def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a

# Функція для пошуку оберненого по модулю
def mod_inverse(a, p):
    return pow(a, p-2, p)

# Функція для шифрування повідомлення
def encrypt_elgamal(p, g, y, M):
    k = random.randint(1, p-2)
    while gcd(k, p-1) != 1:
        k = random.randint(1, p-2)

    a = pow(g, k, p)
    b = (M * pow(y, k, p)) % p
    return (a, b)

# Функція для дешифрування повідомлення
def decrypt_elgamal(p, x, a, b):
    s = pow(a, x, p)
    s_inv = mod_inverse(s, p)
    M = (b * s_inv) % p
    return M

# Перетворення тексту в числа (підтримка кирилиці)
def text_to_numbers(text):
    return [ord(char) for char in text]

# Перетворення чисел назад у текст
def numbers_to_text(numbers):
    return ''.join(chr(num) for num in numbers)
```

```python
# Основна програма
p = 467  # Велике просте число
g = 2    # Твірне по модулю p
x = random.randint(1, p-2)  # Секретний ключ
y = pow(g, x, p)  # Відкритий ключ

# Текст для шифрування
text = "El Gamal encryption"

# Шифрування тексту
M_numbers = text_to_numbers(text)
encrypted = [encrypt_elgamal(p, g, y, M) for M in M_numbers]
print("Зашифрований текст:", encrypted)

# Дешифрування тексту
decrypted_numbers = [decrypt_elgamal(p, x, a, b) for (a, b) in encrypted]
decrypted_text = numbers_to_text(decrypted_numbers)
print("Розшифрований текст:", decrypted_text)
```

Результат виконання програми:

```
PS C:\Users\G_I> & C:/Python312/python.exe "d:/Labs/KI-42/Захист Інформації (Павлюк)/Solution.py"
Зашифрований текст: [(125, 208), (376, 447), (44, 93), (107, 341), (282, 256), (439, 121), (274, 360), (60, 100), (322, 446), (330, 246), (20, 268), (
437, 171), (77, 137), (194, 122), (271, 300), (107, 419), (226, 440), (87, 200), (125, 203)]
Розшифрований текст: El Gamal encryption
PS C:\Users\G_I>
```

**Висновки**

Під час виконання лабораторної роботи вивчив та застосував на практиці принципи структури алгоритму і методики практичної реалізації криптосистеми шифрування Ель-Гамаля.