Лабораторна робота №7 (Варіант 3)

Тема: Дослідження електронного цифрового підпису (ЕЦП) Ель Гамаля

Мета роботи: дослідження структури алгоритму і методики практичної реалізації (ЕЦП) Ель Гамаля.

Хід роботи

```
import random

# Функція для обчислення модульного множення
def mod_exp(base, exp, mod):
    result = 1
    while exp > 0:
        if exp % 2 == 1:
            result = (result * base) % mod
        base = (base * base) % mod
        exp //= 2
    return result

# Генерація ключів
def generate_keys(p, g):
    x = random.randint(1, p-2)  # секретний ключ
    y = mod_exp(g, x, p)  # відкритий ключ
    return x, y

# Функція для створення підпису
def sign_message(p, g, x, M):
    k = random.randint(1, p-2)
    while gcd(k, p-1) != 1:  # Потрібно знайти взаємно просте число
        k = random.randint(1, p-2)
    a = mod_exp(g, k, p)
    k_inv = mod_inv(k, p-1)
    b = (k_inv * (M - x * a) % (p - 1)) % (p - 1)
    return a, b

# Функція для перевірки підпису
def verify_signature(p, g, y, M, a, b):
    left = mod_exp(y, a, p) * mod_exp(a, b, p) % p
    right = mod_exp(g, M, p)
    return left == right

# Обчислення НСД для пошуку взаємно простого числа
def gcd(a, b):
    while b != 0:
```

```
        a, b = b, a % b
    return a

# Функція для обчислення оберненого елемента
def mod_inv(a, m):
    m0, x0, x1 = m, 0, 1
    while a > 1:
        q = a // m
        m, a = a % m, m
        x0, x1 = x1 - q * x0, x0
    return x1 + m0 if x1 < 1 else x1

# Параметри криптосистеми Ель Гамаля
p = 467  # Просте число
g = 2    # Генератор

# Генерація ключів
x, y = generate_keys(p, g)
print(f"Секретний ключ: {x}")
print(f"Відкритий ключ: {y}")

# Повідомлення для підпису (використовуємо кириличний текст)
message = "Повідомлення"
M = sum([ord(c) for c in message])  # Перетворення в числове значення

# Створення підпису
a, b = sign_message(p, g, x, M)
print(f"Підпис: a = {a}, b = {b}")

# Перевірка підпису
is_valid = verify_signature(p, g, y, M, a, b)
print(f"Підпис дійсний: {is_valid}")
```

Результат виконання програми:

```
PS C:\Users\G_I> & C:/Python312/python.exe "d:/Labs/KI-42/Захист Інформації (Павлюк)/Solution.py"
Секретний ключ: 353
Відкритий ключ: 393
Підпис: a = 18, b = 26
Підпис дійсний: True
```

Висновки

Під час виконання лабораторної роботи вивчив та застосував на практиці принципи структури алгоритму і методики практичної реалізації (ЕЦП) Ель Гамаля.