Лабораторна робота №5 (Варіант 3)

Тема: Дослідження електронного цифрового підпису (ЕПЦ) RSA

Мета роботи: дослідження структури алгоритму і методики практичної реалізації (ЕПЦ) RSA.

Хід роботи

```python
import random

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

# Функція для розширеного алгоритму Евкліда (обернене по модулю)
def modinv(a, m):
    m0, x0, x1 = m, 0, 1
    if m == 1:
        return 0
    while a > 1:
        q = a // m
        m, a = a % m, m
        x0, x1 = x1 - q * x0, x0
    if x1 < 0:
        x1 += m0
    return x1

# Генерація простих чисел p і q
def generate_keys():
    p = 61  # Перше просте число
    q = 53  # Друге просте число
    n = p * q  # Модуль n
    phi = (p - 1) * (q - 1)  # Функція Ейлера

    # Вибір e такого, що 1 < e < phi і НСД(e, phi) = 1
    e = random.randrange(1, phi)
    while gcd(e, phi) != 1:
        e = random.randrange(1, phi)

    # Обчислення d
    d = modinv(e, phi)

    return ((e, n), (d, n))  # Повертаємо відкритий і секретний ключі

# Функція для шифрування
```

```python
def encrypt(public_key, plaintext):
    e, n = public_key
    cipher = [pow(ord(char), e, n) for char in plaintext]
    return cipher

# Функція для дешифрування
def decrypt(private_key, ciphertext):
    d, n = private_key
    plain = [chr(pow(char, d, n)) for char in ciphertext]
    return ''.join(plain)

# Основний код
public_key, private_key = generate_keys()

message = "Електронний підпис"  # Текст для шифрування (кирилиця)
print("Початкове повідомлення:", message)

# Шифрування
encrypted_msg = encrypt(public_key, message)
print("Зашифроване повідомлення:", encrypted_msg)

# Дешифрування
decrypted_msg = decrypt(private_key, encrypted_msg)
print("Розшифроване повідомлення:", decrypted_msg)
```

Результат виконання програми:

```
PS C:\Users\G_I> & C:/Python312/python.exe "d:/Labs/KI-42/Захист Інформації (Павлюк)/Solution.py"
Початкове повідомлення: Електронний підпис
Зашифроване повідомлення: [1334, 2733, 517, 2049, 2143, 897, 1754, 746, 746, 1942, 1775, 875, 3122, 137, 2886, 3122, 1942, 2004]
Розшифроване повідомлення: Електронний підпис
```

Висновки

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