Лабораторна робота №4 (Варіант 3)

Тема: Дослідження криптоалгоритму шифрування RSA

Мета роботи: дослідження структури алгоритму і методики практичної реалізації криптосистеми шифрування RSA.

Хід роботи

Для виконання лабораторної роботи використовувалось зовнішню бібліотеку sympy

```
# Імпорт необхідних модулів
from sympy import mod_inverse
import math

# Функція для генерації ключів RSA
def generate_keys(p, q):
    n = p * q
    phi = (p - 1) * (q - 1)
    e = 65537  # загальновживане відкрите значення для e
    d = mod_inverse(e, phi)
    return (e, n), (d, n)

# Функція для шифрування
def encrypt_rsa(public_key, plaintext):
    e, n = public_key
    encrypted = [pow(ord(char), e, n) for char in plaintext]
    return encrypted

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

# Функція для підтримки кирилиці
def to_unicode(text):
    return [ord(char) for char in text]

def from_unicode(unicode_list):
    return ''.join(chr(num) for num in unicode_list)

# Початкові прості числа для RSA (підставте свої значення)
p = 61  # просте число
q = 53  # просте число
```

```
# Генерація ключів
public_key, private_key = generate_keys(p, q)

# Текст для шифрування (кирилиця)
plaintext = "Алгоритм RSA"

# Шифрування
ciphertext = encrypt_rsa(public_key, plaintext)
print(f"Зашифрований текст: {ciphertext}")

# Дешифрування
decrypted_text = decrypt_rsa(private_key, ciphertext)
print(f"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: [2065, 1666, 2660, 1625, 2930, 1804, 2839, 1904, 1992, 1859, 2680, 2790]
Розшифрований текст: Алгоритм RSA
PS C:\Users\G_I>
```

Висновки

Під час виконання лабораторної роботи вивчив та застосував на практиці принципи структури алгоритму і методик практичної реалізації криптосистеми шифрування RSA.