Лабораторна робота №3 (Варіант 3)

Тема: Мережі Фейштеля

Мета роботи: вивчити принципи роботи мережі Фейштеля, навчитись шифрувати інформацію за допомогою використання блокового криптоалгоритму.

Хід роботи

```
# Лінійний конгруентний генератор
def linear_congruential_generator(A, C, M, T0, length):
    numbers = [T0]
    for _ in range(1, length):
        T_next = (A * numbers[-1] + C) % M
        numbers.append(T_next)
    return numbers

# Функція для перетворення тексту в Unicode-коди (підтримка кирилиці)
def text_to_unicode(text):
    return [ord(char) for char in text]

# Функція для перетворення Unicode-кодів назад у текст
def unicode_to_text(unicode_list):
    return ''.join(chr(code) for code in unicode_list)

# Шифрування тексту
def encrypt(text, gamma):
    text_unicode = text_to_unicode(text)
    encrypted = []
    for i in range(len(text_unicode)):
        # Шифрування за допомогою операції XOR
        encrypted_char = text_unicode[i] ^ gamma[i % len(gamma)]
        encrypted.append(encrypted_char)
    return unicode_to_text(encrypted)

# Дешифрування тексту
def decrypt(encrypted_text, gamma):
    encrypted_unicode = text_to_unicode(encrypted_text)
    decrypted = []
    for i in range(len(encrypted_unicode)):
        decrypted_char = encrypted_unicode[i] ^ gamma[i % len(gamma)]
        decrypted.append(decrypted_char)
    return unicode_to_text(decrypted)

# Початкові параметри для генератора ПВЧ
A = 5  # константа A
```

```python
C = 3  # константа C
M = 256  # модуль (2^8 для 8 розрядів)
T0 = 7  # початкове значення T(0)
text = "Мережа Фейштеля"  # текст для шифрування

# Генерація псевдовипадкових чисел (гама)
gamma = linear_congruential_generator(A, C, M, T0, len(text))

# Шифрування
encrypted_text = encrypt(text, gamma)
print(f"Зашифрований текст: {encrypted_text}")

# Дешифрування
decrypted_text = decrypt(encrypted_text, gamma)
print(f"Розшифрований текст: {decrypted_text}")
```

Результат виконання програми:

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

PS C:\Users\G_I> & C:/Python312/python.exe "d:/Labs/KI-42/Захист Інформації (Павлюк)/Solution.py"
Зашифрований текст: ЛГçхЖÇ%иҺгсѲлЫ
Розшифрований текст: Мережа Фейштеля
PS C:\Users\G_I>
```

Висновки

Під час виконання лабораторної роботи вивчив та застосував на практиці принципи роботи мережі Фейштеля, навчитись шифрувати інформацію за допомогою використання блокового криптоалгоритму.