Лабораторна робота №1 (Варіант 3)

Тема: Шифрування даних методами підстановки (заміни), перестановки і поліабетними шифрами

Мета роботи: Набуття навичок шифрування інформації з використанням простих методів шифрування. У рамках цієї роботи, третій варіант передбачає використання багатоабеткових шифрів і української абетки для шифрування та дешифрування тексту.

Теоретичні відомості:

Багатоабеткові шифри — це шифри, у яких для шифрування повідомлення періодично використовується кілька різних абеток підстановки. Це дозволяє знизити ймовірність дешифрування шифру за допомогою частотного аналізу, який є ефективним для моноабеткових шифрів, таких як шифр Цезаря.

Основний принцип роботи багатоабеткового шифру полягає у тому, що кожна літера відкритого тексту шифрується за різними абетками залежно від її позиції та ключа, який визначає, яку саме абетку слід використовувати для кожної літери.

Алгоритм багатоабеткового шифру:

- Для шифрування використовується кілька варіантів абетки (таблиця 2).
- Ключ впливає на вибір абетки для шифрування кожної конкретної літери.
- Дешифрування виконується за допомогою тих самих абеток та ключа.

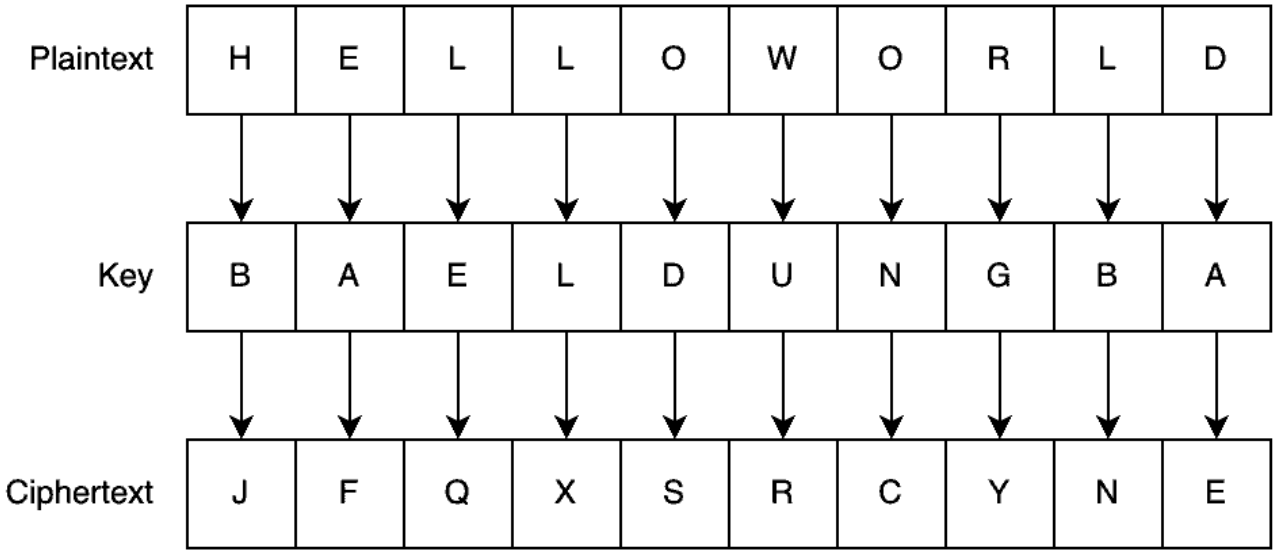
Опис варіанту:

Згідно з таблицею 1, для варіанту 3 необхідно використовувати багатоабетковий шифр на основі української абетки. В якості ключа в лабораторній роботі використовується довільне слово, що визначає порядок використання різних абеток підстановки.

Алгоритм роботи програми:

1. *Шифрування*: Для кожної літери тексту вибирається відповідна абетка залежно від ключа. Літера тексту замінюється на літеру із відповідної абетки.
2. *Дешифрування*: Зашифрований текст обробляється так само, як і в процесі шифрування, проте заміна здійснюється у зворотному порядку — із зашифрованої абетки на оригінальну.
3. *Виведення*: Програма виводить зашифрований і розшифрований текст.

Блок-схема алгоритму:



Код програми (Python):

```
# Алфавіт для шифрування
alphabet = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ"
alphabet2 = "ЙЦУКЕНГШШЩЗХФІВАПРОЛДЖЯЧСМИТЬБЮ"

# Функція для генерації ключа потрібної довжини
def generate_key(text, key):
    key = list(key)
    if len(text) == len(key):
        return key
    else:
        for i in range(len(text) - len(key)):
            key.append(key[i % len(key)])
    return "".join(key)

# Функція для шифрування тексту
def encrypt_vigenere(plain_text, key):
    cipher_text = []
    for i in range(len(plain_text)):
        if plain_text[i] in alphabet:
            x = (alphabet.index(plain_text[i]) + alphabet.index(key[i])) % len(alphabet)
            cipher_text.append(alphabet[x])
        else:
            cipher_text.append(plain_text[i])  # Додаємо символи, яких немає в алфавіті
    return "".join(cipher_text)

# Функція для дешифрування тексту
def decrypt_vigenere(cipher_text, key):
    plain_text = []
    for i in range(len(cipher_text)):
        if cipher_text[i] in alphabet:
            x = (alphabet.index(cipher_text[i]) - alphabet.index(key[i]) + len(alphabet))
% len(alphabet)
            plain_text.append(alphabet[x])
        else:
            plain_text.append(cipher_text[i])  # Додаємо символи, яких немає в алфавіті
    return "".join(plain_text)

# Початкові дані
plain_text = "ПРИКЛАДТЕКСТУ"
key = "КЛЮЧ"  # Введіть свій ключ тут

# Генерація ключа
key = generate_key(plain_text, key)
```

```python
# Шифрування
cipher_text = encrypt_vigenere(plain_text, key)
print(f"Зашифрований текст: {cipher_text}")

# Дешифрування
decrypted_text = decrypt_vigenere(cipher_text, key)
print(f"Розшифрований текст: {decrypted_text}")
```

Результати:

Аналіз результатів:

Програма успішно виконує шифрування та дешифрування багатоабетковим шифром на основі заданого ключа. Оригінальний текст було успішно відновлено після шифрування, що свідчить про правильну реалізацію алгоритму.

Висновки:

Під час виконання лабораторної роботи було розглянуто та реалізовано багатоабетковий шифр на основі української абетки. Алгоритм продемонстрував свою працездатність для шифрування та дешифрування тексту з використанням кількох різних абеток підстановки. Це дозволяє значно підвищити стійкість шифру порівняно з моноабетковими методами.