

Міністерство освіти і науки України
Харківський радіотехнічний фаховий коледж

ЛАБОРАТОРНА РОБОТА №2

Найпростіші способи шифрування даних, шифруючі таблиці.

з дисципліни

«Технології захисту інформації»

Виконала:

студентка групи ПІ-431

Узун Діана Дмитрівна

Керівник роботи:

Бриксін В.О.

Харків 2024

ЗАХИСТ ІНФОРМАЦІЇ

ЛАБОРАТОРНА РОБОТА №2

Найпростіші способи шифрування даних, шифруючі таблиці.

Мета роботи: застосувати практично найпростіші оборотні перетворення вихідних даних із метою шифрування інформації.

Завдання

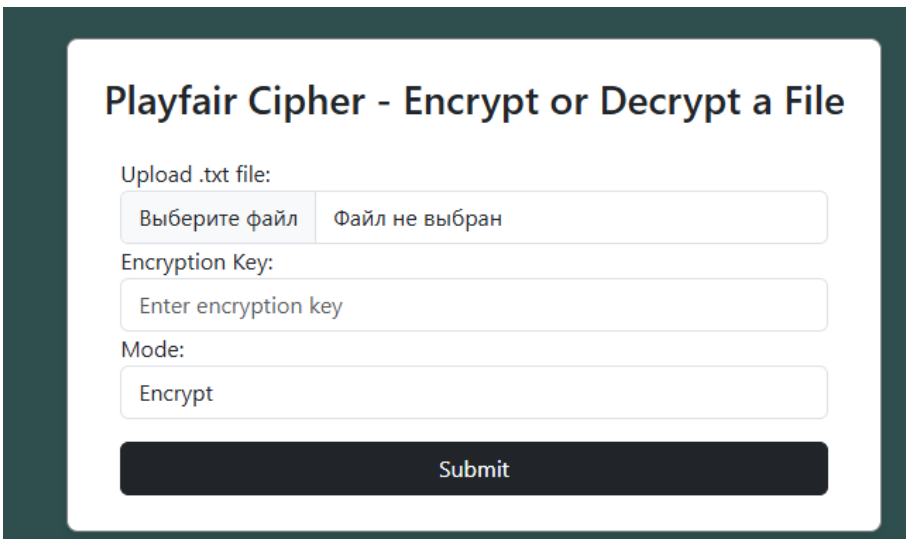
1. Підготувати тестовий приклад: текстовий файл (англійською чи українською мовами), що містить 25 символів. На початку файлу мають бути вказані прізвища студентів, які виконують це завдання.
2. Реалізувати додаток, що перевіряє оборотність шифрування/дешифрування (шляхом порівняння файлів).
3. Реалізувати додаток, що демонструє шифрування та дешифрування інформації. Переконатися у оборотності шифрування.

Варіант	Метод шифрування	Перемішування столбців та строк	Ключ
19	Таблиця 5x5		випадкове

Результати виконання завдань

Додаток був написаний на мові програмування Python, за допомогою фреймворку Flask. Вихідний код програми був викладений на GitHub: <https://github.com/ddianaoo/Caesar-Cipher.git>.

Графічний вигляд:



Playfair Cipher - Encrypt or Decrypt a File

Upload .txt file:

Выберите файл Файл не выбран

Encryption Key:

Enter encryption key

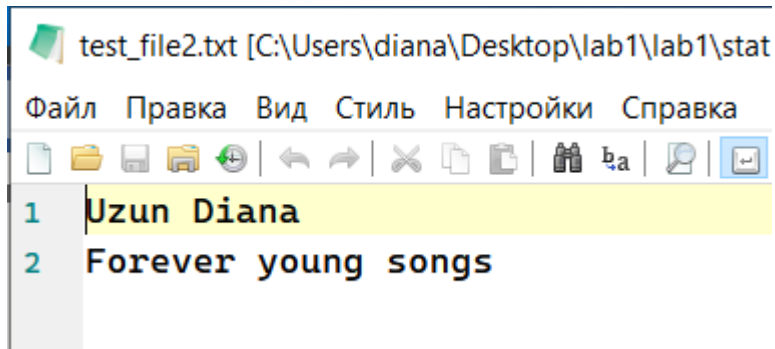
Mode:

Encrypt

Submit

Тестування додатку

1. Файл для шифрування:



2. Заповнення та відправка форми:

Playfair Cipher - Encrypt or Decrypt a File

Upload .txt file:

Выберите файл test_file1.txt

Encryption Key:

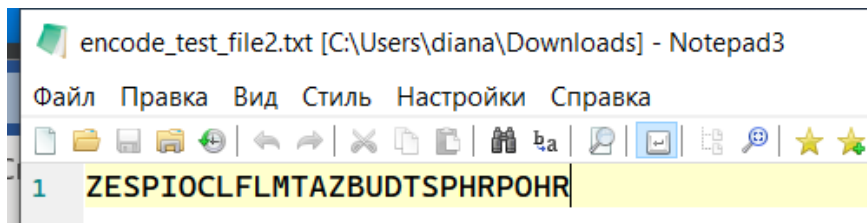
abc

Mode:

Encrypt

Submit

3. Отриманий файл після шифрування:



4. Візьмемо отриманий файл для дешифрування:

Playfair Cipher - Encrypt or Decrypt a File

Upload .txt file:

Выберите файл encode_test_file2.txt

Encryption Key:

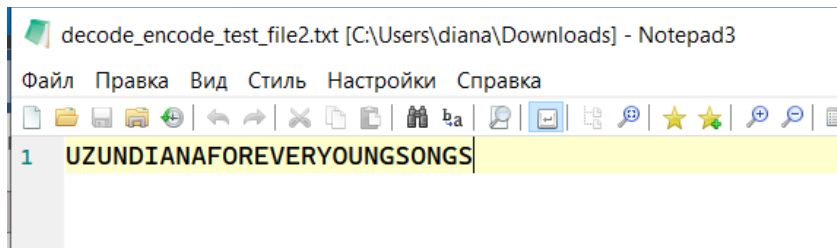
abc

Mode:

Decrypt

Submit

5. Отриманий файл після дешифрування:



Опис отриманих результатів

В процесі тестування програми було проведено шифрування та дешифрування текстових файлів за допомогою шифруючих таблиць із заданим ключем.

Після застосування операції дешифрування до зашифрованого файлу, вміст було відновлено до початкового стану. Це дозволяє зробити висновок, що програма успішно реалізує необхідну логіку, зокрема коректну оборотність процесів шифрування та дешифрування. Початковий і кінцевий файли в результаті виявились ідентичними, що підтверджує правильність роботи програми.

Висновки

У процесі виконання лабораторної роботи №2 було досліджено один із найпростіших методів шифрування даних — шифруючих таблиць з ключем.

Результати роботи показали, що шифруючі таблиць і дійсно дозволяє здійснювати оборотне перетворення інформації, тобто після шифрування дані можуть бути коректно відновлені шляхом дешифрування. Це підтверджує функціональність і простоту цього методу для базового захисту інформації.

Мета роботи, яка полягала в практичному застосуванні найпростіших оборотних перетворень для шифрування даних, була досягнута.