Лабораторна робота №2
Методи класичної криптології.

Лабораторна робота містить 2 завдання (6 варіантів для першого завдання і один варіант для другого). Вибрати варіант у кожному завданні відповідно до номера студента у списку своєї групи.

Завдання 1.

Створити програму шифрування та розшифрування вказаним методом. Програма шифрування повинна задовольняти таким умовам: читати файл з набраним текстом; шифрувати текст з довільними параметрами, значення яких вводиться з клавіатури; виводити зашифрований текст у файл. Програма розшифровування повинна задовольняти таким умовам: читати файл із зашифрованим текстом; розшифровувати його; виводити на екран розшифрований текст.

Варіант № 1. Шифр Полібія

1. Зашифрувати текст з використанням шифру Полібія **з** довільним ключовим словом, яке вводиться з клавіатури. Використати ускладнений варіант, який передбачає повторне шифрування зсунутого криптотексту.
2. Розшифрувати текст з відомим ключем.

Варіант № 2. Шифр Гронсфельда

1. Зашифрувати текст з довільним ключем, який вводиться з клавіатури, використовуючи шифр Гронсфельда.
2. Розшифрувати текст з відомим ключем.

Варіант № 3. Шифр Віженера

1. Зашифрувати текст використовуючи шифр Віженера.
2. Розшифрувати текст.

Варіант № 4. Шифр Плейфера

1. Зашифрувати текст з довільним ключовим словом, яке вводиться з клавіатури, використовуючи шифр Плейфера.
2. Розшифрувати текст з відомим ключовим словом.

Варіант № 5. Шифр «подвійний квадрат Уітстона»

1. Зашифрувати текст, використовуючи шифр Уітстона з довільними ключовими словами, які вводиться з клавіатури,.
2. Розшифрувати текст, використовуючи ключові слова.

Варіант № 6. Шифр чотирьох квадратів

1. Зашифрувати текст, використовуючи шифр чотирьох квадратів з довільними ключовими словами, які вводиться з клавіатури.
2. Розшифрувати текст, використовуючи ключові слова.

Завдання 2. ШИФРУВННЯ МЕТОДОМ ХІЛЛА

Теоретичні відомості. Спочатку символи алфавіту кодуємо числами, наприклад порядковими номерами символів. Далі вибираємо матрицю n × n, яка буде ключем шифру. Вихідне повідомлення розбиваємо на блоки розміром n букв, числові значення яких розглядаємо як вектори розміру n. Кожний з векторів множимо на матрицю шифрування n × n. Результуючий блок (вектор) розміру n — відповідний вихідному блоку зашифрований

текст. Операції додавання і множення виконуються за модулем m, де m — потужність алфавіту.

Ключ, можна задавати матрицею, але вигідніше задавати кодовим словом, числове представлення якого трансформують у матрицю. Для того, щоб отримати квадратну матрицю n x n, довжина кодового речення має бути квадратом цілого числа, наприклад 4, 9, 16, 25, і т. д.

Для розшифрування необхідно шифротекст помножити на обернену матрицю.

$$BA = C \rightarrow CA^{-1} = BAA^{-1} = BE = B$$

Щоб операція розшифрування була можливою, матриця шифрування повинна мати обернену в Z_m^n.

Отже:

1. детермінант матриці повинен бути відмінним від 0,
2. детермінант матриці повинен мати обернений елемент в кільці Z_m^n. Необідною умовою існування оберненого елемента є: детермінант і модуль (довжина алфавіту) повинні бути взаємно простими числами.

Практична частина.

1. Створіть криптографічну систему, яка використовує шифр Хілла, описаний у теоретичній частині.
2. Система шифрування повинна задовольняти наступним вимогам: 1) читати відкрите повідомлення з текстового файлу і перетворювати його у цифрове представлення; 2) запитувати ключове слово (9 і більше літер); 3) генерувати ключ-матрицю по ключовому слову; 4) шифрувати за допомогою алгоритму Хілла відкрите повідомлення і записувати його у файл.
3. Система розшифровування повинна задовольняти таким вимогам: 1) читати шифрограму з текстового файлу; 2) запитувати ключове слово; 3) генерувати ключ-матрицю; 4) розшифровувати шифрограму і виводити її у файл та на екран монітора.