Дата: 2022/02/21
Предмет: Защита информации
Тема: Полиграммный шифр
Тип занятия: Лабораторная работа
Группа: ИВТ-18-1, ИВТ-18-2

Теоретическая часть
Ознакомиться с лекционным материалом, размещённым в группе ВК по адресу:
https://vk.com/zainf

Практическая часть
Составить компьютерную программу (на любом языке программирования), которая выполняет следующие действия:

1. По заданной текстовой строке, состоящей из символов указанного алфавита, возвращает строку, зашифрованную с помощью полиграммного шифра.
2. По заданной строке, зашифрованной с помощью полиграммного шифра и состоящей из символов указанного алфавита, возвращает строку-оригинал.

В программе предусмотреть:

1. Подпрограмму, которая по заданной квадратной матрице A размерности m и модулю N возвращает матрицу A^{-1}, обратную к матрице A по модулю N.
2. Подпрограмму, которая по заданному порядку m и модулю N подбирает случайную матрицу A, у которой есть обратная по модулю N.
3. Подпрограмму, которая по заданному порядку m и модулю N подбирает случайный вектор сдвига B.
4. Подпрограмму, которая по заданной текстовой строке, порядку m, алфавиту (размер которого N), матрице преобразования A и вектору сдвига B возвращает зашифрованную текстовую строку.
5. Подпрограмму, которая по заданной зашифрованной строке, порядку m, алфавиту (размер которого N), матрице преобразования A и вектору сдвига B возвращает строку-оригинал.
6. Возможно, придётся реализовать вспомогательные подпрограммы: сложения, вычитания, умножения, деления целых чисел по заданному модулю; сложения вычитания, умножения матриц по модулю; вычисления определителя квадратной матрицы; получения минора или алгебраического дополнения элемента матрицы (все операции выполняются по модулю).

Можно, но не обязательно: файлы проекта выложить в личный кабинет, упаковав их в архив

Алфавит, размерность m матрицы A и входную строку подберите самостоятельно.