Лабораторная работа № 1
Введение в криптологию

Базовое задание (5 *баллов, дата сдачи ≤ 03.06.2021*).

Реализовать шифр простой замены (подстановки) для английского алфавита. Вход программы – текстовый файл с открытым текстом для режима зашифрования или текстовый файл с шифртекстом для режима зашифрования, текстовый файл с ключом (подстановкой). Ключ (одна из 26! возможных подстановок) генерировать случайным образом, для генерации не использовать функции типа *shuffle*. Выход программы – текстовый файл с шифртекстом для режима зашифрования или с открытым текстом для режима расшифрования.

Дополнительные задания (принимаются при условии, что сдано основное задание, *i*-ое дополнительное задание принимается при условии, что сданы дополнительные задания 1,..., *i*–1, *i* = 2, 3,...). Под реализацией шифра подразумевается и зашифрование, и расшифрование.

– 1 (1 *балл, дата сдачи ≤ 11.03.2021*). Реализовать шифр Вижинера.

– 2 (1 *балл, дата сдачи ≤ 11.03.2021*). Реализовать аффинный шифр.

– 3 (1 *балл, дата сдачи ≤ 11.03.2021*). Реализовать шифр Хилла.

– 4 (1 *балл, дата сдачи ≤ 04.03.2021)*. Дешифровать текст, зашифрованный шифром простой замены (файл прилагается). Текст на английском языке, пробелы и знаки препинания отсутствуют.

– 5 (1+4 *балла, дата сдачи ≤ 25.02.2021)*. Разработать программу, дешифрующую шифр простой замены для английского алфавита. Для получения балла необходимо за 15 минут расшифровать текст, аналогичный предлагаемому в дополнительном задании № 4.

Литература:

1. The Codebreakers – The Story of Secret Writing. D. Kahn.

2. Криптология. Харин Ю.С. и др.

3. Основы криптографии. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.