

Лабораторная работа № 1

Введение в криптологию

Базовое задание (6 баллов, дата сдачи $\leq 10.03.2022$).

Реализовать шифр простой замены (подстановки) для текстов на английском языке. 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 $1, \dots, i-1$, $i = 2, 3, \dots$). Под реализацией шифра подразумевается и зашифрование, и расшифрование.

– **1** (1 балл, дата сдачи $\leq 03.03.2022$). Реализовать шифр Вижинера.

– **2** (1 балл, дата сдачи $\leq 03.03.2022$). Реализовать шифр Хилла.

– **3** (1 балл, дата сдачи $\leq 24.02.2022$). Дешифровать текст, зашифрованный шифром простой замены (файл прилагается). Текст на английском языке, пробелы и знаки препинания отсутствуют.

– **4** (1+4 балла, дата сдачи $\leq 24.02.2022$). Разработать программу, дешифрующую шифр простой замены для английского алфавита. Для зачета задания необходимо за 15 минут расшифровать текст, аналогичный предлагаемому в дополнительном задании № 3.

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.