Лабораторная работа № 3
Элементы блочных криптосистем

Базовое задание (6 *баллов, дата сдачи* ≤ *21.04.2022*).

Реализовать модельную блочную криптосистему *G* (см. стр. 47 [1]) в режиме простой замены (Electronic Codebook (ECB)). Проверить шифртекст на случайность с помощью статистического теста из [2] (см. вариант в таблице) для различного числа тактов (от 1 до 8): т.е. необходимо реализовать модельную криптосистему *G* с одним тактом и для нее протестировать шифртекст, реализовать *G* с двумя тактами и для нее протестировать шифртекст, и так далее – до восьми тактов включительно.

Вход программы: файл с открытым текстом, файл с ключом, файл с синхропосылкой (при необходимости), выход программы – файл с шифртекстом.

Программа должна позволять зашифровывать и расшифровывать любые файлы независимо от формата, разрешения, *etc*. То есть файл рассматривается как последовательность бит – шифрование должно применяться именно к ней. Типичный пример неправильного выполнения этого задания – программа может шифровать только текстовые файлы, данные из которых считываются посимвольно. Если в текстовом файле записано ABC, то на вход алгоритма шифрования должна подаваться следующая последовательность (в шестнадцатеричном виде): 0x414243). Программа должна уметь шифровать и расшифровывать файлы размером не менее 100 МБ. Время шифрования 100 МБ не должно превышать 1 минуты.

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,...).

– 1. (2 *балла, дата сдачи* ≤ *14.04.2022*). Помимо режима простой замены реализовать еще 3 режима шифрования (на ваш выбор).

– 2. (1 *балл, дата сдачи* ≤ *07.04.2022*). Для базового задания вычислить энтропию открытого текста и энтропию шифртекста для различного числа тактов (от 1 до 8). Размер файла с открытым текстом должен составлять не менее 1 МБ.

– 3. (1 *балл + 4 бонусных, дата сдачи* ≤ *31.03.2022*). Вычислить (оценить) энтропию и избыточность белорусского языка.

Литература

1. 1. Криптографические методы. С.В. Агиевич. – 2014.
http://apmi.bsu.by/assets/files/agievich/cm.pdf
2. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST Special Publication 800-22 Rev. 1a. – National Institute of Standards and Technology, 2010. – 131 p.

Фамилия, имя, отчество	Номер теста из [2]

Быстрова Вероника Алесандровна	2
Василючек Даниил Александрович	3
Венедиктов Никита Валерьевич	4
Веренич Владислав Николаевич	7
Голубович Маргарита Михайловна	8
Емельяненко Павел Дмитриевич	11
Карпов Даниил Александрович	12
Козинская Екатерина Андреевна	13
Кривленя Анастасия Валерьевна	14
Кулешевич Тимофей Витальевич	15
Мальцев Максим Дмитриевич	2
Орлович Алексей Юрьевич	3
Поживилко Федор Андреевич	4
Полывяный Глеб Андреевич	7
Рудой Андрей Игоревич	8
Рыжков Ярослав Александрович	11
Серапина Марина Викторовна	12
Черненков Артем Витальевич	13
Шевчёнок Дарья Игоревна	14