Лабораторная работа № 3
Элементы блочных криптосистем

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

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 ≤ 29.04.2021*). Помимо режима простой замены реализовать еще 3 режима шифрования (на ваш выбор).

– 2. (2 *балла, дата сдачи ≤ 22.04.2021*). Временем размножения ошибки криптосистемы E называется минимальное r такое, что для r-тактового преобразования изменение (ошибка) в любом символе (бите) открытого текста может привести к изменению любого символа (бита) шифртекста. Оценить время размножения ошибки криптосистемы G при различных величинах циклического сдвига (<<<) в тактовой функции.

– 3. (1 *балл + 8 бонусных, дата сдачи ≤ 15.04.2021*). Реализовать атаку на криптосистему G на основе метода баланса «время-память» (метода Хеллмана) (подробнее см. стр. 52 [1]).

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	Номер теста из [2]
Белицкий Евгений	2
Бислюк Артём	3
Бокун Адам	4
Виноградова Анастасия	7
Врублевская Екатерина	8
Доскоч Роман	11
Ищенко Иван	12
Козунов Алексей	13
Кукса Андрей	14
Левданская Елизавета	15
Мигас Злата	2
Никончик Даниил	3
Руткевич Родион	4
Семенович Дмитрий	7
Икромов Джовид	8