Варианты заданий на лабораторную работу

Вариант 1

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма симметричного шифрования TEA. Входные и выходные данные запишите в файл типа .txt.

Вариант 2

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма симметричного шифрования ГОСТ 28147-89. Входные и выходные данные запишите в файл типа .txt.

Вариант 3

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма симметричного шифрования DES. Входные и выходные данные запишите в файл типа .txt.

Вариант 4

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма симметричного шифрования RC4. Входные и выходные данные запишите в файл типа .txt.

Вариант 5

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма тройного DES шифрования с использованием двух ключей, т.е. k_1, k_2 не зависимые, а $k_3 = k_1$. Входные и выходные данные запишите в файл типа .txt.

Вариант 6

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма тройного DES шифрования с использованием трёх ключей, т.е. k_1, k_2, k_3 не зависимые. Входные и выходные данные запишите в файл типа .txt.

Вариант 7

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием упрощенного алгоритма симметричного шифрования DES (DES Lightweight). Его отличие от исходного алгоритма DES состоит лишь в том, что вместо восьми таблиц замен используется только одна. Таблица замены выглядит так:

14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

Входные и выходные данные запишите в файл типа .txt.

Вариант 8

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и расшифровывать сообщения с использованием алгоритма DESX (Des extended) с использованием трёх ключей, т.е. k_1, k_2, k_3 не зависимые. Входные и выходные данные запишите в файл типа .txt.

Вариант 9

Два друга хотят обмениваться зашифрованными сообщениями, но у них нет подходящей программы. Напишите программу позволяющую шифровать и дешифровать сообщения с использованием алгоритма симметричного шифрования AES. Входные и выходные данные запишите в файл типа .txt.