Задание 1 по криптографии

cr-ts123.tex

В текстовом файле inp.txt хранится текст, состоящий из русских букв, цифр, знаков препинания, пробелов (объем текста не менее 2 кБт). Необходимо составить две программы, первая из которых шифрует текст из файла inp.txt и записывает результат в файл out1.txt, а вторая расшифровывает текст из файла out1.txt и записывает результат в файл out2.txt.

При шифровании используется один из следующих методов (шифров, кодов):

1. Код Цезаря (величина сдвига вводится с клавиатуры).

2. Код изгороди (высота вводится с клавиатуры).

3. Азбука Морзе.

4. Шифр перестановок (перестановка вводится с клавиатуры).

5. Модулярный шифр ($f(x) = ax+b(mod\, n)$), a и b вводятся с клавиатуры).

6. Шифрование по маске (маска вводится с клавиатуры; длина маски — не менее 5 символов).

7. Шифр "квадрат с прорезями"(конфигурация квадрата задается в отдельном текстовом файле).

8. Квадрат Плейфера.

9. Шифр одноразового блокнота (блокнот задается в отдельном текстовом файле).

10. Маршрутное шифрование.

Срок сдачи работы — 10.03.09.

Номер варианта определяется по остатку при делении на 10 числа, составленного из двух последних цифр номера зачетной книжки студента. Если остаток равен нулю, то выбирается вариант 10.

`E:\VVP\PREDMETS\Crypto\2_Pract\Laborat\CR-TS123.TEX`

Задание по криптографии (2)

1. Составить программу (на основе алгоритма Евклида) для выражения наибольшего общего делителя d чисел a и b в виде $d = ax + by$. Числа a и b задаются с клавиатуры (и имеют тип long int).

2. Составить программу для получения списка простых чисел, не превосходящих 35 000. Список должен быть помещен в файл prime.txt (Использовать решето Эратосфена).

3. Составить программу для разложения на простые множители чисел, не превосходящих 10^8. Программа может использовать список простых чисел, полученных в задаче 2. Разлагаемое на множители число вводится с клавиатуры (и имеет тип long int).

4. Составить программу для вычисления остатка r при делении на m числа a^b. Числа a, b и m — целые (типа long int), $a, m < 30\ 000$, $b \leq 10^7$.

5. Составить программу для вычисления мультипликативного обратного числа a по модулю m. Числа a и m — целые (типа long int), $a, m < 10^7$. **Указание**: следует использовать алгоритм Евклида для получения решения уравнения в целых числах $ax + my = 1$. Программа должна проверять взаимную простоту a и m.

6. Составить программу для решенияы систем трех сравнений первой степени: $a_i x \equiv b_i (\mathrm{mod}\, m)$, $i = 1, 2, 3$. Числа a_i, b_i и m_i —целые, не превосходящие 1 000. Решение x имеет тип long int.

Срок сдачи работы —

Задание 3

cr-ts123.tex

1. Составить программу для шифрования и расшифровки текста методом рюкзака. Исходный текст хранится в текстовом файле inp.txt и имеет объем не менее 2 кБт. Этот текст разбивается на блоки по 8 байт (последний блок дополняется до 8 байт) и каждому блоку ставится в соответствие длинное целое число. Зашифрованный текст записывается в файл out.txt. Расшифрованный текст помещается в файл out1.txt.

2. Составить программу для шифрования и расшифровки текста с помощью системы шифрования RSA. Исходный текст хранится в текстовом файле inp.txt и имеет объем не менее 2 кБт. Простые числа p и q должны быть не меньше 10^{10}. Зашифрованный текст записывается в файл out.txt. Расшифрованный текст помещается в файл out1.txt.

3. Составить программу для шифрования и расшифровки текста методом Эль-Гамаля (простое число p должно быть не меньше 10^{15}). Исходный текст хранится в текстовом файле inp.txt и имеет объем не менее 2 кБт. . Зашифрованный текст записывается в файл out.txt. Расшифрованный текст помещается в файл out1.txt.

Срок сдачи работы —