Лабораторные работы по курсу Защита информации (часть 1).

МГТУ им. Баумана
Кафедра ИУ-9
Юдаев П.В., 2014

Лабораторная работа №1. Реализация взлома шифра Виженера.

1 Задание

Дан текст на английском языке в нижнем регистре с удаленными пробелами, знаками препинания и цифрами, зашифрованный шифром Виженера. Длина ключа - не более 15 символов. Дана таблица частоты встречаемости букв английского алфавита. Найти ключ и расшифровать первые 100 символов текста.

2 Рекомендации по выполнению задания

Язык программирования - по выбору студента.

Метод взлома. Построить предположения о длине ключа методом Касиски или с помощью индекса совпадений. (Они рассказаны на лекции.) Пусть длина ключа равна n. Тогда шифротекст разбивается на n последовательностей, каждая из которых зашифрована одним символом ключа (сдвиг, шифр Цезаря). Для каждой последовательности провести частотный анализ встречаемости букв и построить предположения об этом символе ключа. Получить предполагаемый ключ. Расшифровать шифротекст. Из выдвинутых гипотез о ключе выбрать ту, при которой получится осмысленный текст.

Ответ - две строки:
первая строка - ключ
вторая строка - начало расшифрованного текста указанной длины.

Пример ответа:
superkey
thistextwasencryptedandthendecrypted

Таблица частоты встречаемости букв.

Буква	Частота (в %)
E	12.02
T	9.10
A	8.12
O	7.68
I	7.31
N	6.95
S	6.28
R	6.02
H	5.92
D	4.32
L	3.98
U	2.88
C	2.71
M	2.61
F	2.30
Y	2.11
W	2.09
G	2.03
P	1.82
B	1.49
V	1.11
K	0.69
X	0.17
Q	0.11
J	0.10
Z	0.07