Шифр Цезаря

Постановка задачи:

Шифр цезаря был придуман для защиты информации от злоумышленников, при помощи кодирования сообщения циклическим сдвигом алфавита.

Суть кодирования - букве ставится в соответствие другая буква при помощи циклического сдвига.

Для циклического сдвига пронумеруем буквы алфавита от 0 до n-1 (где n мощность алфавита)

Кодирование - такое отображение буквы в букву из оригинального алфавита в зашифрованный, в которой каждой букве под номером i (какой-нибудь номер буквы из оригинального алфавита) будет ставится в соответствие буква под номером (i+r)%n (где r - ключ сдвига, т. е. число , на которое мы смещаем индексы)( или под номером в кольце по вычету n - (i+r));

Суть декодирования - восстановить соответствие букв и их номеров из оригинального алфавита (Взлом != декодирование, в декодировании пользователь знает всю нужную для расшифровки информацию: оригинальный алфавит, зашифрованный алфавит, величина сдвига)

Декодирование - такое отображение буквы в букву из зашифрованного алфавита в оригинальный, в котором каждой букве под номером i (какой-нибудь номер буквы из зашифрованного алфавита) будет ставится в соответствие буква под номером (n+i-r)%n (где r - ключ сдвига, о котором отправитель и получатель договорились заранее, так что r - известная в данном контексте величина);

Суть взлома - подобрать сдвиг r при помощи перебора ключа(ключ - величина сдвига, неизвестная для взломщика величина). Величина ключа находится в определённом диапазоне [0;n-1], остальные значения ключа будут сводится к результатам этого диапазона. Для понимания, какой ключ лучше, какой ключ хуже, для каждого ключа вычисляется некоторую числовую характеристику, определяющая, на сколько соответствующий ключ походит.

Числовая характеристика - функция g(r) @РИС 1@Б где n - мощность алфавита, p - таблица канонических частот, в которой номеру буквы из оригинального алфавита ставится в соответствие частота повторений этой буквы в языке, f - таблица фактических частот, в которой номеру буквы из переданного алфавита ставится в соответствие частота появления этой буквы в сообщении. В функции вычисляется сумма всех квадратов разностей частот из p и частот с некоторым сдвигом из f. Чем меньше сумма, тем меньше различие между частотами соответствующих номеров букв, тем больше ключ r подходит для декодирования. В итоге находится тот сдвиг r, при котором значение суммы меньше. Найденное r и есть взломанный ключ.

Решение задачи представлено кодированием текста книги Гари Поттера, а частоты английского языка взяты с картинки.