Практика №7. Шифрование и дешифровка произвольного сообщения с помощью шифров перестановки и замены..

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Шифрами замены называют такие шифры, которые осуществляются путем замены каждого символа открытого сообщения на другие символы – шифрообозначения, причем порядок следования шифрообозначений совпадает с порядком следования соответствующих им символов открытого сообщения.

Пусть, например, зашифровывается сообщение на русском языке и при этом замене подлежит каждая буква сообщения. Формально в этом случае шифр замены можно описать следующим образом. Для каждой буквы ⟨ исходного алфавита строится некоторое множество символов M⟨, которое называется множеством шифрообозначений для буквы ⟨.

Таблица является ключом шифра замены. Зная ее можно осуществить как зашифрование, так и расшифрование.

При зашифровании каждая буква ⟨ открытого сообщения, начиная с первой, заменяется любым символом из множества M⟨. За счет этого можно получить различные варианты зашифрованного сообщения для одного и того же открытого сообщения.

В простейшем случае множество шифрообозначений M⟨ состоит из одного элемента. Такой шифр называется шифром простой замены.

Шифры простой замены

Система шифрования Цезаря

В качестве ключа шифра Цезаря используют таблицу, первая строка которой содержит буквы исходного алфавита, а вторая строка – последовательность букв, записанных в алфавитном порядке, но начинающаяся не с буквы А, а с какой-либо другой:

А	Б	…	Э	Ю	Я
Д	Е	…	Б	В	Г

При шифровании букву исходного сообщения находят в первой строке и заменяют ее на соответствующую букву второй строки. Запомнить ключ достаточно просто – надо лишь запомнить первую букву второй строки.

Серьезный недостаток данного шифра – ограниченное число ключей, которое равно числу букв в алфавите.

Афинная система подстановок Цезаря

Здесь буквы исходного сообщения преобразуются следующим образом:

$T_1=AT+B \pmod m$,

где T – порядковый номер буквы исходной последовательности,

T_1 - порядковый номер соответствующей буквы зашифрованной последовательности,

m – размер алфавита,

A,B – целые числа, причем A и m взаимно простые.

Пример.

Зашифруем фразу КОРАБЛИ ОТПЛЫВАЮТ ВЕЧЕРОМ, используя афинную систему подстановок при A=13, B=5. Размер алфавита m=32 (будем считать, что в исходном алфавите в качестве буквы Й используется И, а в качестве Ё – Е, и добавим 32-ым символом пробел). В результате преобразований получим:

Сообщение К О Р А Б Л И О Т П Л Ы В А Ю Т В Е Ч Е Р О М

Шифртекст Ы П И Е У З О Щ П В Ь З Ш Е Я В Щ Ж Г Ж И П Х

Система омофонов

Данный шифр характеризуется тем, что буквы исходного сообщения имеют несколько замен. Число замен берется пропорциональным вероятности появления буквы в открытом тексте. Данные о распределениях вероятностей букв в русском тексте приведены в таблице.

Буква	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-Ность	Буква	Вероят-ность
Пробел	0.175	Р	0.040	Я	0.018	Х	0.009
О	0.090	В	0.038	Ы	0.016	Ж	0.007
Е	0.072	Л	0.035	З	0.016	Ю	0.006
А	0.062	К	0.028	Ъ	0.014	Ш	0.006
И	0.062	М	0.026	Б	0.014	Ц	0.004
Н	0.053	Д	0.025	Г	0.013	Щ	0.003
Т	0.053	П	0.023	Ч	0.012	Э	0.003
С	0.045	У	0.021	Й	0.010	Ф	0.002

Шифруя букву исходного сообщения, выбирают случайным образом одну из ее замен. Замены (часто называемые омофонами) могут быть представлены трехразрядными числами от 000 до 999. Например, букве О присваиваются 90 случайных номеров, буквам Б и Ъ – по 14 номеров. Если омофоны присваиваются случайным образом различным появлениям одной и той же буквы, тогда каждый омофон появляется в шифртексте равновероятно. Система омофонов обеспечивает простейшую защиту от криптоаналитических атак, основанных на подсчете частот появления букв в шифртексте.

Шифры сложной замены

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исхдного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно циклически меняет используемые алфавиты.

При r-алфавитной подстановке символ x_0 исходного сообщения заменяется символом y_0 из алфавита B_0, символ x_1 - символом y_1 из алфавита B_1, и так далее, символ x_{r-1} заменяется символом y_{r-1} из алфавита B_{r-1}, символ x_r заменяется символом y_r снова из алфавита B_0, и т.д.

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита может быть преобразован в несколько различных символов шифровальных алфавитов B_i.

Шифр Гронсфельда

Шифрование осуществляется следующим образом. Под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Для замены выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа *e* (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

Сообщение В О С Т О Ч Н Ы Й Э К С П Р Е С С
Ключ 2 7 1 8 2 7 1 8 2 7 1 8 2 7 1 8 2
Шифртекст Д Х Т Ь Р Ю О Г Л Д Л Щ С Ч Ж Щ У

Шифр Гронсфельда представляет собой частный случай системы шифрования Вижинера.

Система шифрования Вижинера

Этот шифр сложной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. Таблица Вижинера используется для зашифрования и расшифрования.

Ключ	А	Б	В	Г	Д	…	Э	Ю	Я
0	А	Б	В	Г	Д	…	Э	Ю	Я
1	Б	В	Г	Д	Е	…	Ю	Я	А
2	В	Г	Д	Е	Ж	…	Я	А	Б
3	Г	Д	Е	Ж	З	…	А	Б	В
…	…	…	…	…	…	…	…	…	…
30	Ю	Я	А	Б	В	…	Ы	Ъ	Э
31	Я	А	Б	В	Г	…	Ъ	Э	Ю

Таблица имеет два входа:

верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Пример.

Зашифруем сообщение **ПРИЛЕТАЮ СЕДЬМОГО** с использованием ключа **АМБРОЗИЯ**.

Сообщение П Р И Л Е Т А Ю С Е Д Ь М О Г О
Ключ А М Б Р О З И Я А М Б Р О З И Я
Шифртекст ПЪ Й ЫУЩ И Э С С Е К Ь Х Л Н

ЗАДАНИЯ

Провести предварительную обработку произвольного текста. Привести все слова к нижнему регистру, удалить знаки препинания.

Зашифровать текст методом простой замены, запросив ключ шифрования у пользователя.

Дешифровать текст, используя тот же самый ключ.

Зашифровать текст методом сложной замены, запросив ключ шифрования у пользователя.

Дешифровать текст, используя тот же самый ключ.