

Теоретический материал

Криптография — наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, шифрования.

Криптография изучает методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в зашифрованный текст (шифротекст).

Многие современные алгоритмы шифрования, работающие на компьютере, используют идеи, на которых основывались способы шифрования информации в докомпьютерную эпоху. Наиболее простой шифр — это шифр Цезаря.

Шифр Цезаря

Шифр Цезаря — это преобразование информации методом замены букв на другие, стоящие от данных через определенное количество символов в алфавите. Следовательно, зашифровать можно сообщение на любом языке, имеющем алфавит.

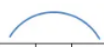
Рассмотрим это графически на примере:

Дано сообщение: «В эту минуту дверь тихо отворилась, и в комнату вошла одна девушка».

1. Написано оно на русском языке, значит, будем использовать русский алфавит.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

2. Теперь двигаем буквы в сторону в зависимости от ключа (цифры). Если ключ положительный, то двигаем влево, если отрицательный — вправо. Пусть ключом будет число 2.



А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

3. Получаем новый алфавит, начинающийся с буквы В. Для удобства шифрования записываем буквы друг под другом и меняем текст.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
↓	↓	↓	↓				↓		↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓		↓					↓	↓			
В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б

Было: В эту минуту дверь тихо отворилась, и в комнату вошла одна девушка

Стало: В яфх окпхфх ёджтю фкчр рфдрткнвую, к д мропвфх дрънв рёпв ёждхъмв.

Дешифрование – преобразование зашифрованного текста в исходный вид. Данный процесс происходит по такому же алгоритму, как и шифрование, только в обратном направлении. Из смещенного алфавита буквы будут заменяться соответствующими буквами исходного.

Шифр замены

Основной недостаток шифра сдвига (шифра Цезаря) заключается в том, что существует слишком мало возможных ключей, всего 25 для английского языка. В целях устранения указанного недостатка был изобретен *шифр замены*. Чтобы описать ключ такого шифра, сначала выписывается алфавит, а непосредственно под ним — тот же алфавит, но с переставленными буквами. Это дает нам правило, по которому буквы открытого текста замещаются символами шифровки. Например,

a b c d e f g h i j k l m n o p q r s t u v w x y z
 GOYDSIPELUAVCRJWXZNHBQFTMK

Шифрование состоит в замене каждой буквы в открытом тексте на соответствующую ей нижнюю букву. Чтобы расшифровать шифротекст, нужно каждую его букву найти в нижней строке таблицы и заменить ее соответствующей верхней. Таким образом, криптограмма слова «hello» будет выглядеть как ESVVJ, если пользоваться приведенным соответствием.

Задание 1

Зашифровать текст (на русском или английском языке) с помощью шифра Цезаря. Текст может вводиться с клавиатуры, может храниться в статическом виде в программе. Ключ для шифрования вводится с клавиатуры.



Решение:



Ответ:

Задание 2*

Предпринять атаку на шифр Цезаря с целью определения ключа шифрования (для шифрования используется текст на русском языке). Таблица встречаемости букв в русском языке:

Номер по частоте употребления	Буква	Частотность	Частотность %	Номер по частоте употребления	Буква	Частотность	Частотность %	Номер по частоте употребления	Буква	Частотность	Частотность %
1	о	0,10983	10,983%	12	м	0,03203	3,203%	24	х	0,00966	0,966%
2	е	0,08483	8,483%	13	д	0,02977	2,977%	25	ж	0,0094	0,94%
3	а	0,07998	7,998%	14	п	0,02804	2,804%	26	ш	0,00718	0,718%
4	и	0,07367	7,367%	15	у	0,02615	2,615%	27	ю	0,00639	0,639%
5	н	0,067	6,7%	16	я	0,02001	2,001%	28	ц	0,00486	0,486%
6	т	0,06318	6,318%	17	ы	0,01898	1,898%	29	щ	0,00361	0,361%
7	с	0,05473	5,473%	18	ь	0,01735	1,735%	30	э	0,00331	0,331%
8	р	0,04746	4,746%	19	г	0,01687	1,687%	31	ф	0,00267	0,267%
9	в	0,04533	4,533%	20	з	0,01641	1,641%	32	ъ	0,00037	0,037%
10	л	0,04343	4,343%	21	б	0,01592	1,592%	33	ё	0,00013	0,013%
11	к	0,03486	3,486%	22	ч	0,0145	1,45%				
				23	й	0,01208	1,208%				

Для шифрования использовать достаточно большой текст (не менее 500 символов).

Идея и пример взлома описаны в книге <https://disk.yandex.ru/i/ABHNCe202IEYNw> со стр. 73 (шифр сдвига).

Решение:

Ответ:

Задание 3

Задача:

Зашифровать текст (на русском или английском языке) с помощью шифра замены. Текст может вводиться с клавиатуры, может храниться в статическом виде в программе. Таблицу замены задать самостоятельно, например:

a b c d e f g h i j k l m n o p q r s t u v w x y z
GOYDSIPELUAVCRJWXZNHBQFTMK

Решение:

Ответ:

Задание 4*

Задача:

Реализовать алгоритм шифрования ГОСТ 28147-89 в режиме простой замены.

В основе лежит схема шифрования Фейстеля (подробно в книге <https://disk.yandex.ru/i/ABHNCe202IEYNw> на стр. 131):



Всё исходное сообщение разбивается на блоки по 64 бита. Каждые 64 бита обрабатываются отдельно согласно схеме Фейстеля в течение 32 раундов.

Для зашифровывания 64-битный блок открытого текста сначала разбивается на две половины: $T_0 = (A_0, B_0)$. На i -м раунде схемы Фейстеля используется подключ X_i :

$$A_{i+1} = B_i \oplus f(A_i, X_i)$$

$$B_{i+1} = A_i.$$

(Плюс в кружочке – это сложение по модулю 2 / исключающее или / XOR)

Для генерации подключей исходный секретный 256-битный ключ разбивается на восемь 32-битных чисел: $K_0 \dots K_7$.

Подключи $X_0 \dots X_{23}$ являются циклическим повторением $K_0 \dots K_7$.

Подключи $X_{24} \dots X_{31}$ являются $K_7 \dots K_0$.

Результатом выполнения 32 раундов алгоритма является 64-битный блок шифртекста: $T_{ш} = (A_{32}, B_{32})$.

Расшифрование осуществляется по тому же алгоритму, что и зашифрование, с тем изменением, что инвертируется порядок подключей: $X_0 \dots X_7$ являются $K_0 \dots K_7$, а $X_8 \dots X_{31}$ являются циклическим повторением $K_7 \dots K_0$.

Функция F схемы Фейстеля реализуется по следующей схеме:



S-блоки в стандарте не определены, но должны быть одни и те же S-блоки для шифрования и расшифровки. Например, можно использовать следующую таблицу:

Номер S-блока	Значение															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3
2	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9
3	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B
4	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3
5	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2
6	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E
7	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C
8	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C

4 бита, идущие на вход S-блоку, представляют собой число от 0 до F (в шестнадцатеричной системе). В зависимости от S-блока, на выход также идет число от 0 до F (в шестнадцатеричной системе), т.е. 4 бита.

Циклический сдвиг (побитовый) выполняется с помощью операции << (примеры: <https://www.techiedelight.com/ru/circular-shift-integer-k-positions/>).

Для реализации сложения по модулю 2^{32} можно, например, оперировать слагаемыми, записанными в 64-битные переменные, а из результата взять только 32 младших бита.

Реализуйте алгоритм дешифрования шифротекста.

Решение:



Ответ:

