Шифр простой замены (моноалфавитный шифр). Полиалфовитный шифр

Основы информационной безопасности

Определение

- **Шифр простой замены, простой подстановочный шифр (моноалфавитный шифр) — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста.**
- **Само шифрование заключается в замене букв согласно таблице.**
- **Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которой она генерируется.**

Примеры моноалфавитного шифра

- **К шифрам простой замены относятся многие способы шифрования, возникшие в древности или средневековье, как, например, *Атбаш* (этбаш) или *Шифр Цезаря*.**
- **Для вскрытия подобных шифров используется частотный криптоанализ.**
- **Частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка.**

Примеры моноалфавитного шифра

- Шифр простой замены не всегда подразумевает замену буквы на какую-то другую букву.
- Допускается использовать замену буквы на цифру.
- К примеру представим некий шифр-алфавит: **А - 33; Б - 17; В - 8; Г - 16; Д - 2; Е - 15; Ё - 14; Ж - 13; З - 12; И - 98; Й - 10; К - 97; Л - 96; М - 24; Н - 0; О - 11; П - 5; Р - 25; С - 7; Т - 3; У - 64; Ф - 26; Х - 66; Ц - 69; Ч - 4; Ш - 6; Щ - 36; Ь - 21; Ъ - 22; Ы - 23; Э - 37; Ю - 39; Я - 18.**
- В данном шифре применяются цифры, заменяющие буквы. Никакой логики в этих цифрах нет.
- Такой простой шифр можно расшифровать, только имея таблицу шифров.

Атбаш

- **Атбаш - простой шифр подстановки для иврита.**
- **Правило шифрования состоит в замене «i»-й буквы алфавита буквой с номером «n» − «i» + 1, где «n» — число букв в алфавите.**
- **Пример для латинского алфавита выглядит так:**

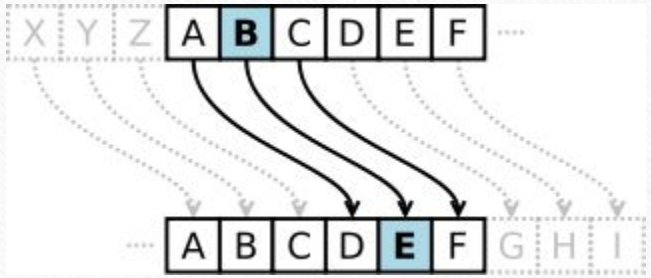
```
Исходный текст:      abcdefghijklmnopqrstuvwxyz
Зашифрованный текст: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Шифр Цезаря

- **Шифр Цезаря**, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.
- Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.
- Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр Цезаря

- **Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.**
- **Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера.**



Шифр Цезаря

- **Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики**

$$y = (x + k) \mod n$$
$$x = (y - k + n) \mod n,$$

- **где *x* - символ открытого текста, *y* – символ шифрованного текста, *n* – мощность алфавита, *k* - ключ**

Пример шифра Цезаря

- ***Шифрование с использованием ключа k = 3.***
- Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З».
- Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее:

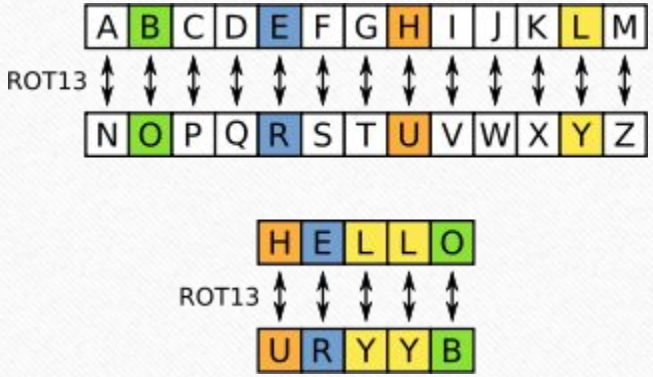
```
Исходный алфавит:  АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифрованный:       ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
```

ROT13

- **ROT13** (*rotate*; «сдвинуть на 13 позиций») представляет собой ~~шифр подстановки простой заменой, используемый~~ в интернет-форумах, как средство для сокрытия спойлеров, основных мыслей, решений загадок и оскорбительных материалов от случайного взгляда.
- ROT13 был охарактеризован как «сетевой эквивалент того, как в журналах печатают ответы на вопросы викторин — перевёрнутыми буквами».
- ROT13 — это вариация шифра Цезаря, разработанного ещё в Древнем Риме.

ROT13

- **ROT13 является обратным алгоритмом, то есть отменить ROT13 можно, применив тот же алгоритм; одни и те же действия могут быть использованы для кодирования и декодирования**



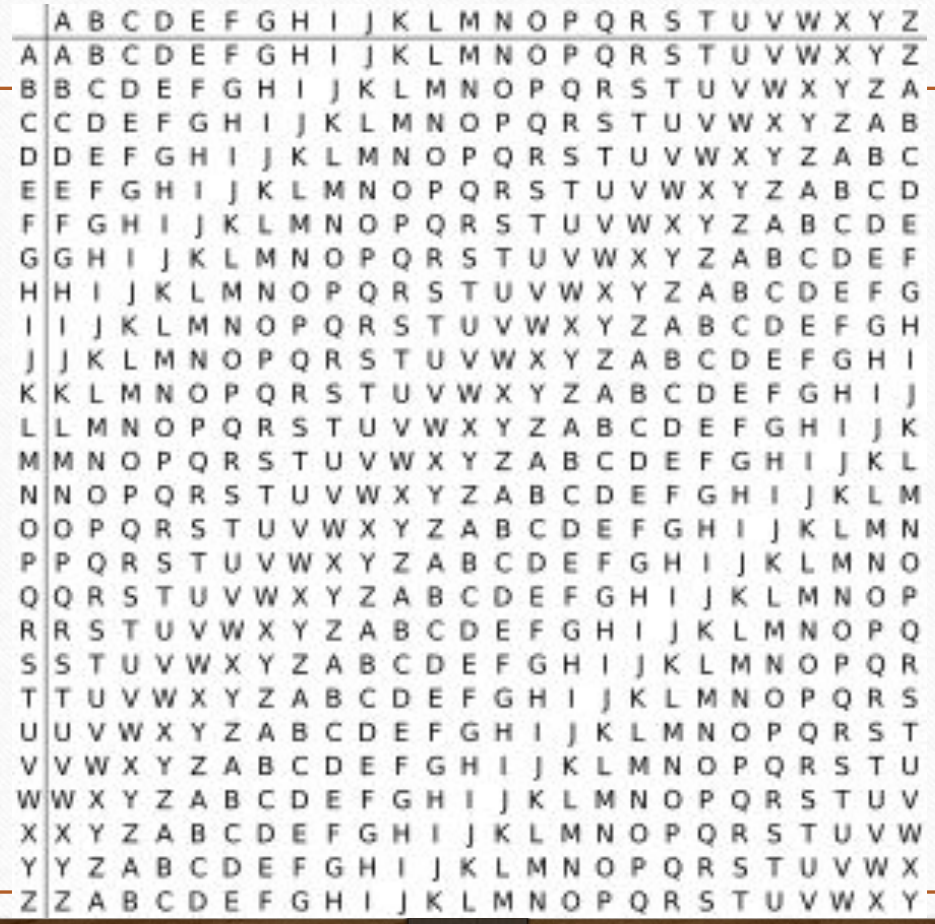
Шифр Виженера

- **Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.**
- **Этот метод является простой формой многоалфавитной замены.**
- **Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата.**
- **Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.**

Шифр Виженера

- **Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига.**
- **Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или квадрат (таблица) Виженера.**
- **Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций.**
- **Таким образом, в таблице получается 26 различных шифров Цезаря.**
- **На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.**

Шифр Виженера



	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Шифр Виженера

- **Например, предположим, что исходный текст имеет вид:**

ATTACKATDAWN

- **Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:**

LEMONLEMONLE

Шифр Виженера

- Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа.
- Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера.
- Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T.
- Остальная часть исходного текста шифруется подобным способом.

Шифр Виженера

Исходный текст: **ATTACKATDAWN**
Ключ: **LEMONLEMONLE**
Зашифрованный текст: **LXFOPVEFRNHR**

- Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста.
- Столбец, в котором находится данный символ, соответствует первому символу исходного текста.
- Следующие символы зашифрованного текста расшифровываются подобным образом.