10. Шифрование методами замены: полибианский квадрат, шифр Цезаря, шифр Цезаря с ключевым словом, аффинная система подстановок Цезаря, диск Альберти, шифр Гронсфельда, шифр Виженера, одноразовый блокнот

Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. **Естественным развитием шифра Цезаря стал шифр Виженера**. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.

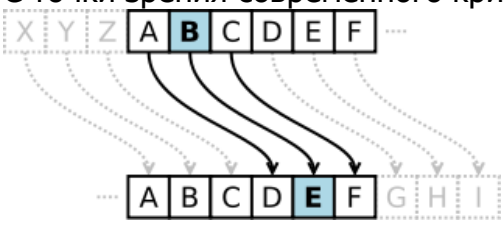

Рисунок 1 Шифр Цезаря

Математическая модель

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

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

где x — символ открытого текста
y — символ шифрованного текста
n — мощность алфавита (кол-во символов)
k — ключ.

Можно заметить, что суперпозиция двух шифрований на ключах k1 и k2 — есть просто шифрование на ключе k1+k2. Более общее, множество шифрующих преобразований шифра Цезаря образует группу Z.

Алфавит:

Буква	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**
Номер	1	2	3	4	5	6	7	8	9	10	11
Буква	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**
Номер	12	13	14	15	16	17	18	19	20	21	22
Буква	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**	**Э**	**Ю**	**Я**
Номер	23	24	25	26	27	28	29	30	31	32	33

Пример:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Ответ: «Пхнфчузхещнд»

Система Цезаря с ключевым словом.

В этой системе шифрования наряду с числовым ключом K, 0 ? K ? (M-1), задающим смещение, используется ключевое слово для изменения порядка символов в заменяющем алфавите.

В качестве ключевого слова необходимо выбирать слово или короткую фразу (не более длины алфавита). Все буквы ключевого слова должны быть различными.

Для создания таблицы замены ключевое слово записываем под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числовым ключом K. Оставшиеся буквы алфавита замены записываем в алфавитном порядке (избегая повтора букв) после ключевого слова. При достижении конца таблицы циклически переходим на ее начало и дописываем последние буквы алфавита не встречавшиеся ранее.

Пример 9. Пусть задан ключ K=3, ключевое слово «ШИФРОВКА» и русский алфавит из 32 букв. Необходимо создать таблицу замен для системы шифрования Цезаря с ключевым словом и с ее помощью зашифровать слово «НЕПТУН».

Первую букву ключевого слова («Ш») записываем под символом «Г» открытого текста с числовым кодом, определенным ключом K=3. Остальные буквы слова «ШИФРОВКА» записываем подряд. Оставшиеся ячейки заполняем теми буквами алфавита, которые не вошли в ключевое слово: «Б», «Г», «Д», «Е» и т.д. до буквы «Ь». Оставшиеся буквы «Э», «Ю», «Я» вписываем в начало таблицы под буквами «А», «Б» и «В», соответственно (табл. 4).

код	0	1	2	**3**	4	5	6	7	8	9	10	11	12	13	14	15
исх. текст	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
шифртекст	Э	Ю	Я	**Ш**	**И**	**Ф**	**Р**	**О**	**В**	**К**	**А**	Б	Г	Д	Е	Ж
код	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
исх. текст	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
шифртекст	З	Й	Л	М	Н	П	С	Т	У	Х	Ц	Ч	Щ	Ъ	Ы	Ь

Таблица 4. Таблица замен символов для системы шифрования Цезаря при K=3, M=32 и ключевом слове «ШИФРОВКА»

Далее с помощью табл. 4 шифруем побуквенно слово «НЕПТУН». В результате получаем шифртекст: «ДФЖЛМД».

Аффинная система подстановок Цезаря. В данном методе используется ключ шифрования в виде пары целых чисел (A, K). Число A задает переход при шифровании вперед на A?J букв, а число K – дополнительное смещение по алфавиту на K букв. Следовательно, аффинную систему подстановок Цезаря можно описать следующей формулой:

I = (A?J+K) mod M. (3)

Формула (3) может быть использована только при выполнении следующих условий: 0 ? (A, J)? (M-1), 0 ? K ? (M-1), НОД (A, M)=1.

Наибольший общий делитель чисел A и M должен быть равен единице, чтобы избежать ситуации повтора, когда разным символам открытого текста соответствует один и тот же символ шифртекста.

Пример 8. Создадим таблицу замен для аффинной системы подстановок Цезаря с ключом (5, 4) на примере русского алфавита. Возьмем алфавит из 32 букв (все кроме буквы «Ё»). Таким образом, A = 5, K = 3, M = 32 и все условия (в том числе и НОД (5, 32) = 1) необходимые для использования (3) выполняются. Код буквы шифртекста находим из соотношения I = (5?J+4) mod 32.

Сведем числовые коды букв открытого и зашифрованного текстов в таблицу (табл. 2).

J	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
I	3	8	13	18	23	28	1	6	11	16	21	26	31	4	9	14
J	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
I	19	24	29	2	7	12	17	22	27	0	5	10	15	20	25	30

Таблица 2. Таблица кодов для аффинных подстановок при A=5, K=3, M=32

Преобразуем числовые коды в соответствующие буквы русского алфавита и получим соответствие для символов открытого текста и шифртекста (табл. 3).

J	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Исх. текст	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Шифртекст	Г	И	Н	Т	Ч	Ь	Б	Ж	Л	Р	Х	Ъ	Я	Д	Й	О
J	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Исх. текст	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Шифртекст	У	Ш	Э	В	З	М	С	Ц	Ы	А	Е	К	П	Ф	Щ	Ю

Таблица 3. Таблица символов для аффинных подстановок при A=5, K=3, M=32

С помощью табл. 3 или формулы (3) слово «МИР» преобразуется в шифртекст «ЯЛУ».

Система Вижинера

В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. 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. Например, предположим, что исходный текст имеет вид:

ATTACKATDOWN

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

LEMONLEMONLE

	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

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.

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.

Если буквы A—Z соответствуют числам 0—25, то шифрование Виженера можно записать в виде формулы:

$$C_i = (P_i + K_i) \bmod 26$$

Расшифровка:

$$P_i = (C_i - K_i + 26) \bmod 26$$