Шифры замены

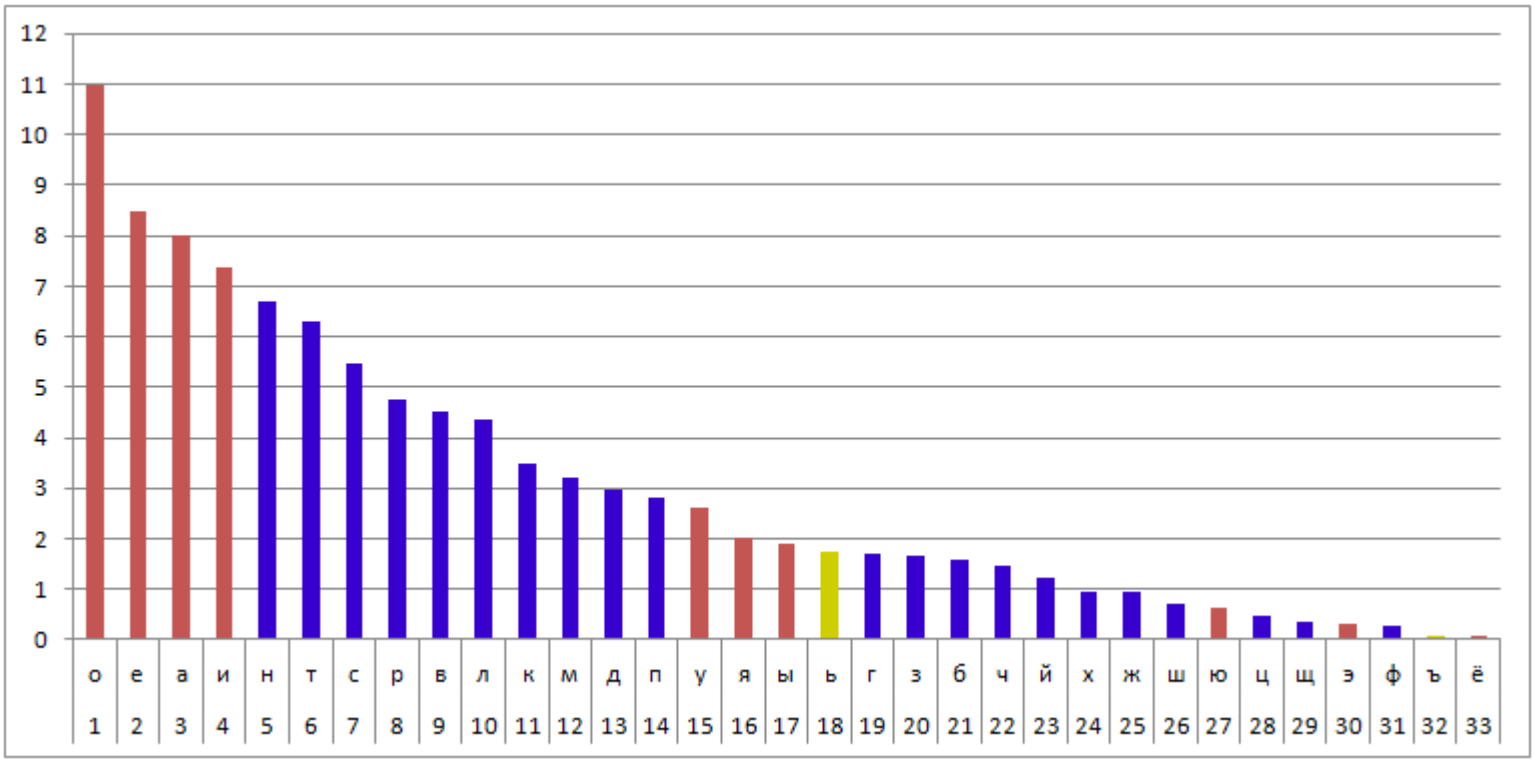
В шифрах замены (или шифрах подстановки), в отличие от **перестановочных шифров**, элементы текста не меняют свою последовательность, а изменяются сами, т.е. происходит замена исходных букв на другие буквы или символы (один или несколько) по неким правилам.

На этой странице описаны шифры, в которых замена происходит на буквы или цифры. Когда же замена происходит на какие-то другие не буквенно-цифровые символы, на комбинации символов или рисунки, это называют прямым **кодированием**.

Моноалфавитные шифры

В шифрах с моноалфавитной заменой каждая буква заменяется на одну и только одну другую букву/символ или группу букв/символов. Если в алфавите 33 буквы, значит есть 33 правила замены: на что менять А, на что менять Б и т.д.

Такие шифры довольно легко расшифровать даже без знания ключа. Делается это при помощи **частотного анализа** зашифрованного текста - надо посчитать, сколько раз каждая буква встречается в тексте, и затем поделить на общее число букв. Получившуюся частоту надо сравнить с эталонной. Самая частая буква для русского языка - это буква О, за ней идёт Е и т.д. Правда, работает частотный анализ на больших литературных текстах. Если текст маленький или очень специфический по используемым словам, то частотность букв будет отличаться от эталонной, и времени на разгадывание придётся потратить больше. Ниже приведена таблица частотности букв (то есть относительной частоты встречаемых в тексте букв) русского языка, рассчитанная на базе **НКРЯ**.



место	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
буква	о	е	а	и	н	т	с	р	в	л	к	м	д	п	у	я	ы	ь	г	з	б	ч	й	х	ж	ш	ю	ц	щ	э	ф	ъ	ё
%	10,98	8,48	8,00	7,37	6,70	6,32	5,47	4,75	4,53	4,34	3,49	3,20	2,98	2,80	2,62	2,00	1,90	1,74	1,69	1,64	1,59	1,45	1,21	0,97	0,94	0,72	0,64	0,49	0,36	0,33	0,27	0,04	0,01

Использование метода частотного анализа для расшифровки шифрованных сообщений красиво описано во многих литературных произведениях, например, у Артура Конана Дойля в романе «**Пляшущие человечки**» или у Эдгара По в «**Золотом жуке**».

Составить кодовую таблицу для шифра моноалфавитной замены легко, но запомнить её довольно сложно и при утере восстановить практически невозможно, поэтому обычно придумывают какие-то правила составления таких кодовых страниц. Ниже приведены самые известные из таких правил.

Случайный код

Как я уже писал выше, в общем случае для шифра замены надо придумать, какую букву на какую надо заменять. Самое простое - взять и случайным образом перемешать буквы алфавита, а потом их выписать под строчкой алфавита. Получится кодовая таблица. Например, вот такая:

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

Число вариантов таких таблиц для 33 букв русского языка = 33! ≈ $8.683317618811886*10^{36}$. С точки зрения шифрования коротких сообщений - это самый идеальный вариант: чтобы расшифровать, надо знать кодовую таблицу. Перебрать такое число вариантов невозможно, а если шифровать короткий текст, то и частотный анализ не применишь.

Но для использования в квестах такую кодовую таблицу надо как-то по-красивее преподнести. Разгадывающий должен для начала эту таблицу либо просто найти, либо разгадать некую словесно-буквенную загадку. Например, отгадать **ключевое слово** или решить **лабиринт-алфавит**.

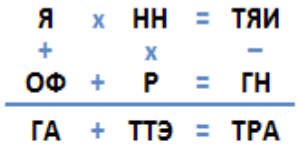
Ключевое слово

Один из вариантов составления кодовой таблицы - использование ключевого слова. Записываем алфавит, под ним вначале записываем ключевое слово, состоящее из неповторяющихся букв, а затем выписываем оставшиеся буквы. Например, для слова **«манускрипт»** получим вот такую таблицу:

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

Как видим, начало таблицы перемешалось, а вот конец остался неперемешенным. Это потому, что самая «старшая» буква в слове «манускрипт» - буква «У», вот после неё и остался неперемешенный «хвост». Буквы в хвосте останутся незакодированными. Можно оставить и так (так как большая часть букв всё же закодирована), а можно взять слово, которое содержит в себе буквы А и Я, тогда перемешаются все буквы, и «хвоста» не будет.

Само же ключевое слово можно предварительно тоже загадать, например при помощи **ребусов** или **рамок**. Например, вот так:



Исходный 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
Алфавит замены	0	1	2	3	4	5	6	7	8	9	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Разгадав арифметический ребус-рамку и сопоставив буквы и цифры зашифрованного слова, затем нужно будет получившееся слово вписать в кодовую таблицу вместо цифр, а оставшиеся буквы вписать по-порядку. Получится вот такая кодовая таблица:

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

Атбаш

Изначально шифр использовался для еврейского алфавита, отсюда и название. Слово атбаш (

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

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

Фраза «ВОЗЬМИ ЕГО В ЭКСЕПШН» превращается при помощи этого шифра в «ЭРЧГТЦ ЪЬР Э ВФНЪПЖС».
Онлайн-калькулятор шифра Атбаш

ROT1

Этот шифр известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на Б, Б на В и т.д., а Я заменяется на А. «ROT1» значит «ROTate 1 letter forward through the alphabet» (англ. «поверните/сдвиньте алфавит на одну букву вперед»). Сообщение «Хрюклокотам хрюклокотамит по ночам» станет «Цсялмплпубн цсялмплпубнйу рп опшбн». ROT1 весело использовать, потому что его легко понять даже ребёнку, и легко применять для шифрования. Но его так же легко и расшифровать.

Онлайн-калькулятор всех русских ROT-шифров

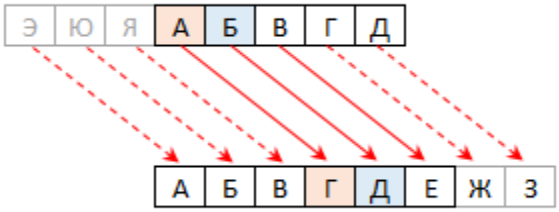
Исходный алфавит	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Алфавит замены	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А

Исходный алфавит	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
Алфавит замены	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

Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждая буква заменяется другой, отстоящей от

неё в алфавите не на одну, а на большее число позиций. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. Он использовал сдвиг на три буквы (ROT3). Шифрование для русского алфавита с использованием такого сдвига:



Исходный 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
Алфавит замены	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	В

Исходный алфавит	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
Алфавит замены	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

Но сдвиг ведь можно делать на произвольное число букв - от 1 до 33. Поэтому для удобства можно сделать диск, состоящий из двух колец, вращающихся относительно друг друга на одной оси, и написать на кольцах в секторах буквы алфавита. Тогда можно будет иметь под рукой ключ для кода Цезаря с любым смещением. А можно совместить на таком диске шифр Цезаря с атбашем, и получится что-то вроде этого:

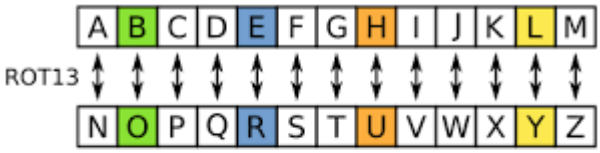
Собственно, поэтому такие шифры и называются ROT - от английского слова «rotate» - «вращать».

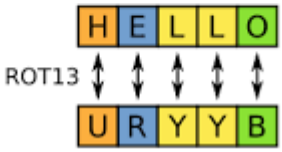
ROT5

В этом варианте кодируются только цифры, остальной текст остаётся без изменений. Производится 5 замен, поэтому и ROT5: 0↔5, 1↔6, 2↔7, 3↔8, 4↔9.

ROT13

ROT13 — это вариация шифра Цезаря для латинского алфавита со сдвигом на 13 символов. Его часто применяют в интернете в англоязычных форумах как средство для сокрытия спойлеров, основных мыслей, решений загадок и оскорбительных материалов от случайного взгляда.





Латинский алфавит из 26 букв делится на две части. Вторая половина записывается под первой. При кодировании буквы из верхней половины заменяются на буквы из нижней половины и наоборот.

ROT18

Всё просто. ROT18 - это комбинация ROT5 и ROT13 :)

ROT47

Существует более полный вариант этого шифра - ROT47. Вместо использования алфавитной последовательности A–Z, ROT47 использует больший набор символов, почти все отображаемые символы из первой половины ASCII-таблицы. При помощи этого шифра можно легко кодировать url, e-mail, и будет непонятно, что это именно url и e-mail :)

!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	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	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	{	|	}	~

Квадрат Полибия

Полибий - греческий историк, полководец и государственный деятель, живший в III веке до н.э. Он предложил оригинальный код простой замены, который стал известен как «квадрат Полибия» (англ. Polybius square) или шахматная доска Полибия. Данный вид кодирования изначально применялся для греческого алфавита, но затем был распространен на другие языки. Буквы алфавита вписываются в квадрат или подходящий прямоугольник. Если букв для квадрата больше, то их можно объединять в одной ячейке.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я			

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е/Ё
2	Ж	З	И/Й	К	Л	М
3	Н	О	П	Р	С	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ы	Ъ/Ь	Э	Ю	Я

	1	2	3	4	5	6
1	**М**	**О**	**С**	**К**	**В**	**А**
2	Б	Г	Д	Е/Ё	Ж	З
3	И/Й	Л	Н	П	Р	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ы	Ъ/Ь	Э	Ю	Я

Такую таблицу можно использовать как в шифре Цезаря. Для шифрования на квадрате находим букву текста и вставляем в шифровку нижнюю от неё в том же столбце. Если буква в нижней строке, то берём верхнюю из того же столбца. Для кириллицы можно использовать таблицу **POT11** (аналог шифра Цезаря со сдвигом на 11

символов:

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

Буквы первой строки кодируются в буквы второй, второй - в третью, а третьей - в первую.

Но лучше, конечно, использовать «фишку» квадрата Полибия - координаты букв:

- Под каждой буквой кодируемого текста записываем в столбик две координаты (верхнюю и боковую). Получится две строки. Затем выписываем эти две строки в одну строку, разбиваем её на пары цифр и используя эти пары как координаты, вновь кодируем по квадрату Полибия.
- Можно усложнить. Исходные координаты выписываем в строку без разбиений на пары, сдвигаем на нечётное количество шагов, разбиваем полученное на пары и вновь кодируем.

Квадрат Полибия можно создавать и с использованием кодового слова. Сначала в таблицу вписывается кодовое слово, затем остальные буквы. Кодовое слово при этом не должно содержать повторяющихся букв.

Вариант шифра Полибия используют в тюрьмах, выстукивая координаты букв - сначала номер строки, потом номер буквы в строке.

Стихотворный шифр

Этот метод шифрования похож на шифр Полибия, только в качестве ключа используется не алфавит, а стихотворение, которое вписывается построчно в квадрат заданного размера (например, 10×10). Если строка не входит, то её «хвост» обрезается. Далее полученный квадрат используется для кодирования текста побуквенно двумя координатами, как в квадрате Полибия. Например, берём хороший стих «Бородино» Лермонтова и заполняем таблицу. Замечаем, что букв Ё, Й, Х, Ш, Щ, Ъ, Э в таблице нет, а значит и зашифровать их мы не сможем. Буквы, конечно, редкие и могут не понадобиться. Но если они всё же будут нужны, придётся выбирать другой стих, в котором есть все буквы.

	0	1	2	3	4	5	6	7	8	9	
0	С	К	А	Ж	И	К	А	Д	Я	Д	я ведь не даром
1	М	О	С	К	В	А	С	П	А	Л	ённая пожаром
2	Ф	Р	А	Н	Ц	У	З	У	О	Т	дана
3	В	Е	Д	Ь	Б	Ы	Л	И	Ж	С	хватки боевые
4	Д	А	Г	О	В	О	Р	Я	Т	Е	щё какие
5	Н	Е	Д	А	Р	О	М	П	О	М	нит вся Россия
6	П	Р	О	Д	Е	Н	Ь	Б	О	Р	одина
7	Д	А	Б	Ы	Л	И	Л	Ю	Д	И	в наше время
8	Н	Е	Т	О	Ч	Т	О	Н	Ы	Н	ешнее племя
9	Б	О	Г	А	Т	Ы	Р	И	Н	Е	вы

Ё Й Х Ш Щ Ъ Э - ?

РУС/LAT

Наверное, самый часто встречающийся шифр :) Если пытаться писать по-русски, забыв переключиться на русскую раскладку, то получится что-то типа этого: *Tckb gsnfnmcz gbcfnm gj-heccrb? pf,sd gthtrk.xbnmcz yf heccre. hfcrkflre? nj gjkexbncz xnj-nj nbgf 'njuj^* Ну чем не шифр? Самый что ни на есть шифр замены. В качестве кодовой таблицы выступает клавиатура.

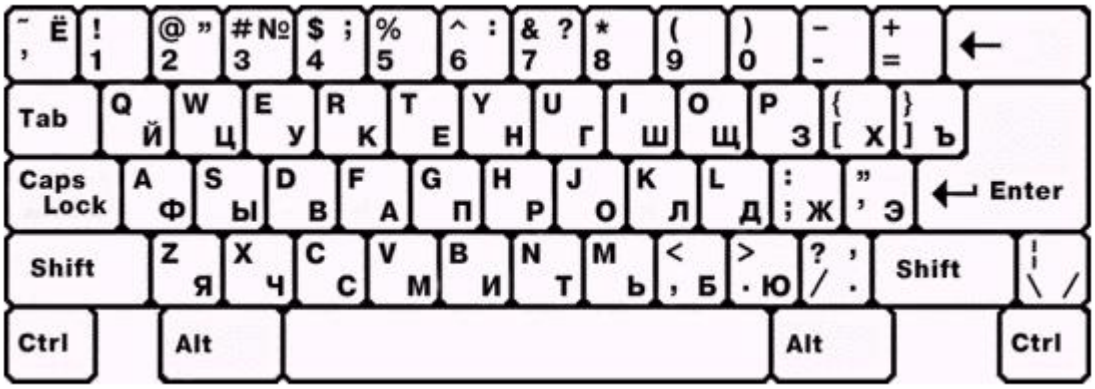


Таблица перекодировки выглядит вот так:

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
F	,	D	U	L	T	`	;	P	B	Q	R	K	V	Y	J	G	H	C	N	E	A	[	W	X	I	O	]	S	M	'	.	Z

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
f	,	d	u	l	t	`	;	p	b	q	r	k	v	y	j	g	h	c	n	e	a	[	w	x	i	o	]	s	m	'	.	z

Литорея

Литорея (от лат. littera — буква) — тайнописание, род шифрованного письма, употреблявшегося в древнерусской рукописной литературе. Известна литорея двух родов: простая и мудрая. Простая, иначе называемая тарабарской грамотой, заключается в следующем. Если «е» и «ё» считать за одну букву, то в русском алфавите остаётся тридцать две буквы, которые можно записать в два ряда — по шестнадцать букв в каждом:

А	Б	В	Г	Д	Е	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

Получится русский аналог шифра ROT13 — **РОТ16** :) При шифровке верхнюю букву меняют на нижнюю, а нижнюю — на верхнюю. Ещё более простой вариант литореи — оставляют только двадцать согласных букв:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Получается шифр **РОТ20**. При шифровании меняют только согласные, а гласные и остальные, не попавшие в таблицу, оставляют как есть. Получается что-то типа «словарь → лсошамь» и т.п.

Мудрая литорея предполагает более сложные правила подстановки. В разных дошедших до нас вариантах используются подстановки целых групп букв, а также числовые комбинации: каждой согласной букве ставится в соответствие число, а потом совершаются арифметические действия над получившейся последовательностью чисел.

Шифрование биграммами

Шифр Плейфера

Шифр Плейфера - ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном. Шифр предусматривает шифрование пар символов (биграмм), вместо одиночных символов, как в шифре подстановки и в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ.

Шифр Плейфера использует таблицу 5x5 (для латинского алфавита, для русского алфавита необходимо увеличить размер таблицы до 6x6), содержащую ключевое слово или фразу. Для создания таблицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую таблицу, в первую очередь нужно заполнить пустые ячейки таблицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки таблицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке таблицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5x5 и является ключом шифра.

Для того, чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой таблице. Определяем положения углов этого прямоугольника относительно друг друга. Затем руководствуясь следующими 4 правилами зашифровываем пары символов исходного текста:

1. 1) Если два символа биграммы совпадают, добавляем после первого символа «X», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «X» используется «Q».
2. 2) Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
3. 3) Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
4. 4) Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «X» (или «Q») , если они не несут смысла в исходном сообщении.

Рассмотрим пример составления шифра. Используем ключ «Playfair example», тогда матрица примет вид:

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

Зашифруем сообщение «Hide the gold in the tree stump». Разбиваем его на пары, не забывая про правило [1]. Получаем: «HI DE TH EG OL DI NT HE TR EX ES TU MP». Далее применяем правила [2]-[4]:

1. Биграмма HI формирует прямоугольник, заменяем её на BM.
2. Биграмма DE расположена в одном столбце, заменяем её на ND.
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.
4. Биграмма EG формирует прямоугольник, заменяем её на XD.
5. Биграмма OL формирует прямоугольник, заменяем её на KY.
6. Биграмма DI формирует прямоугольник, заменяем её на BE.
7. Биграмма NT формирует прямоугольник, заменяем её на JV.
8. Биграмма HE формирует прямоугольник, заменяем её на DM.
9. Биграмма TR формирует прямоугольник, заменяем её на UI.
10. Биграмма EX находится в одной строке, заменяем её на XM.
11. Биграмма ES формирует прямоугольник, заменяем её на MN.
12. Биграмма TU находится в одной строке, заменяем её на UV.
13. Биграмма MP формирует прямоугольник, заменяем её на IF.

Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF». Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF».

Двойной квадрат Уитстона

Чарльз Уитстон разработал не только шифр Плейфейра, но и другой метод шифрования биграммами, который называют «двойным квадратом». Шифр использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра.

Имеется две таблицы со случайно расположенными в них русскими алфавитами.

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

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

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

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

Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста. Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста ОВ.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение ПР ИЛ ЕТ АЮ _Ш ЕС ТО ГО

Шифртекст ПЕ ОВ ЩН ФМ ЕШ РФ БЖ ДЦ

Шифрование методом «двойного квадрата» дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста «двойного квадрата» требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк, а без компьютера вообще не реально.

Полиалфавитные шифры

Шифр Виженера

Естественным развитием шифра Цезаря стал шифр Виженера. В отличие от моноалфавитных это уже полиалфавитный шифр. 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». На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от буквы ключевого слова.

Для латиницы таблица Виженера выглядит вот так:

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

Для русского алфавита вот так:

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

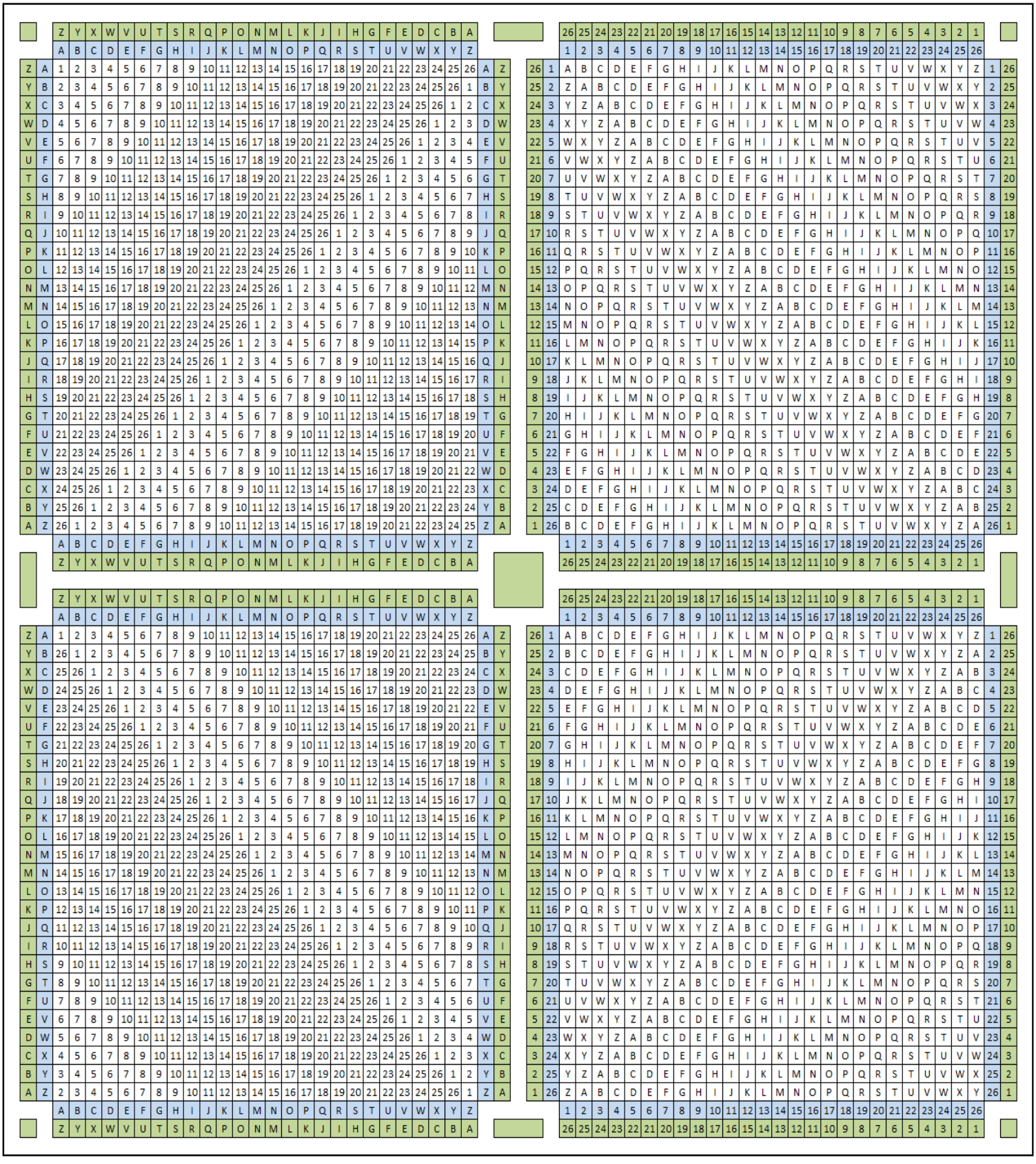
Легко заметить, что строки этой таблицы - это ROT-шифры с последовательно увеличивающимся сдвигом.

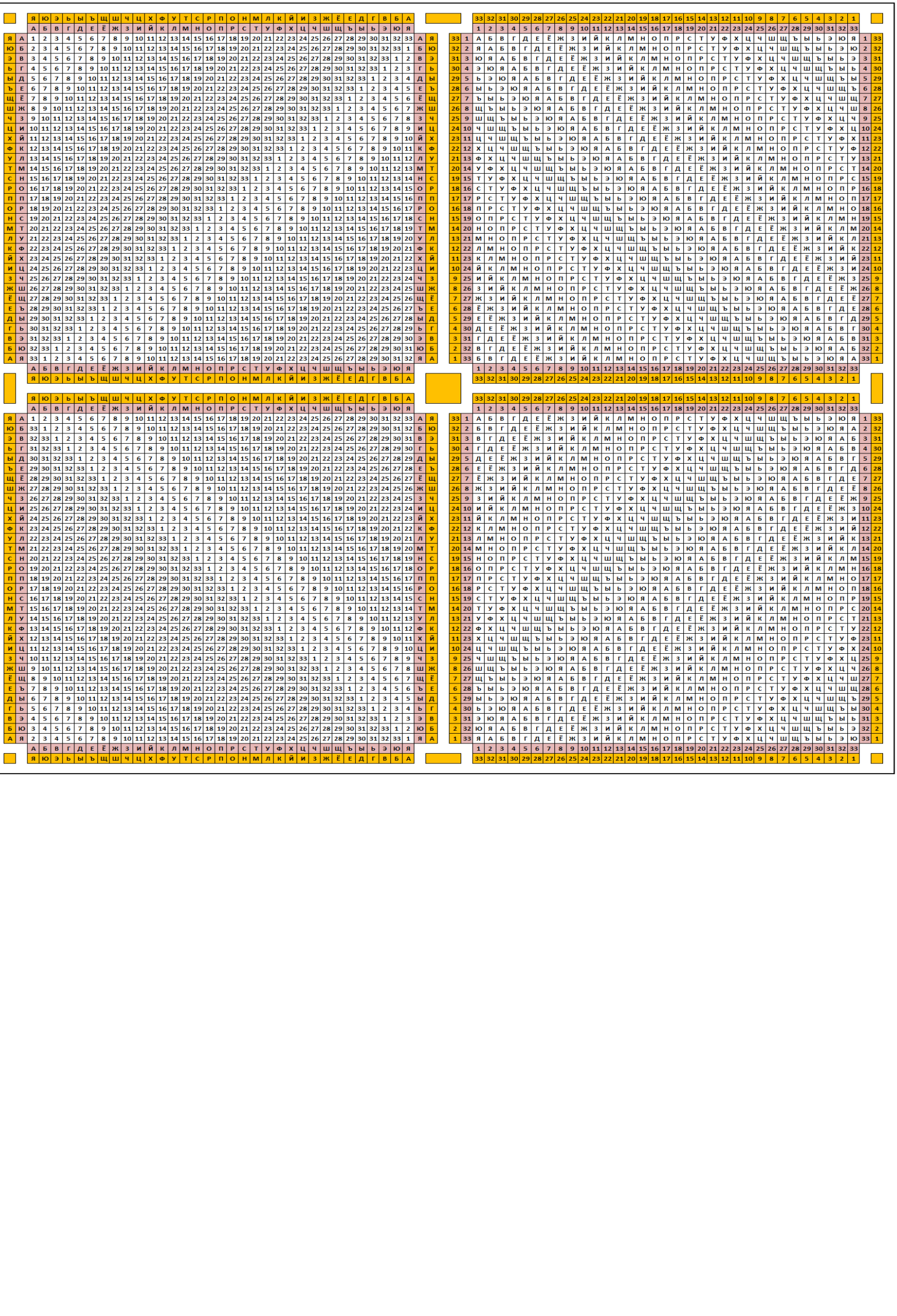
Шифруют так: под строкой с исходным текстом во вторую строку циклически записывают ключевое слово до тех пор, пока не заполнится вся строка. У каждой буквы исходного текста снизу имеем свою букву ключа. Далее в таблице находим кодируемую букву текста в верхней строке, а букву кодового слова слева. На пересечении столбца с исходной буквой и строки с кодовой буквой будет находиться искомая шифрованная буква текста.

Исходный текст	М	Е	Ч	Т	Ы	К	О	Т	О	Р	Ы	Е	С	Б	Ы	В	А	Ю	Т	С	Я	Н	Е	М	Е	Ч	Т	Ы	А	П	Л	А	Н	Ы
Ключ	В	И	Ж	Е	Н	Е	Р	В	И	Ж	Е	Н	Е	Р	В	И	Ж	Е	Н	Е	Р	В	И	Ж	Е	Н	Е	Р	В	И	Ж	Е	Н	Е
Зашифрованный текст	О	Н	Ю	Ч	И	П	Я	Ф	Ч	Ч	А	Т	Ц	С	Э	К	Ж	Г	А	Ц	П	П	Н	У	Й	Е	Ч	Л	В	Ш	Т	Е	Ы	А

Важным эффектом, достигаемым при использовании полиалфавитного шифра типа шифра Виженера, является маскировка частот появления тех или иных букв в тексте, чего лишены шифры простой замены. Поэтому к такому шифру применить частотный анализ уже не получится.

Для шифрования шифром Виженера можно воспользоваться **Онлайн-калькулятором шифра Виженера**. Для различных вариантов шифра Виженера со сдвигом вправо или влево, а также с заменой букв на числа можно использовать приведённые ниже таблицы:





Шифр Гронсвельда

Это вариация шифра Виженера, где вместо ключевого слова применяется ключевое число, цифры которого показывают, какой из ROT-шифров применять (на сколько позиций сдвигать букву).

Буквы исходного текста

Цифра ключа	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	
0	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	0
1	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	А	1
2	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	2
3	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	В	3
4	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	В	Г	4
5	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	В	Г	Д	5
6	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	В	Г	Д	Е	6
7	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	В	Г	Д	Е	Ё	7
8	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	В	Г	Д	Е	Ё	Ж	8
9	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	В	Г	Д	Е	Ё	Ж	З	9

Книжный шифр

Суть метода **книжного шифра** - это выбор любого текста из книги, и замена каждой буквы шифруемого слова номером слова в выбранном тексте, начинающегося на нужную букву. Можно заменять не на номер слова, а на координату буквы (строка, номер в строке). При этом одной исходной букве может соответствовать несколько разных кодов, ведь одна и та же буква может находиться в разных местах. Для кодирования обычно используют страницу из какой-то заранее оговоренной книги. Без знания кодовой страницы расшифровать такие зашифрованные послания практически невозможно.

Можно использовать не конкретное издание, а какой-то классический текст, который не менялся от одного издания к другому. Например, стихотворную поэму Пушкина «**Гавриилиада**» или **Декларацию независимости США**.

Если же в качестве ключа использовать целую книгу (например, словарь), то можно зашифровывать не отдельные буквы, а целые слова и даже фразы. Тогда координатами слова будут номер страницы, номер строки и номер слова в строке. На каждое слово получится три числа. Можно также использовать внутреннюю нотацию книги - главы, абзацы и т.п. Например, в качестве кодовой книги удобно использовать Библию, ведь там есть четкое разделение на главы, и каждый стих имеет свою маркировку, что позволяет легко найти нужную строку текста. Правда, в Библии нет современных слов типа «компьютер» и «интернет», поэтому для современных фраз лучше, конечно, использовать энциклопедический или толковый словарь.