

МЕТОДЫ ЗАМЕНЫ

Суть: символы шифруемого текста
заменяются другими символами,
взятыми из одного или нескольких
алфавитов.

Методы шифрования заменой:

1. Простая (одноалфавитная)
2. Многоалфавитная одноконтурная
обыкновенная
3. Многоалфавитная одноконтурная
монофоническая
4. Многоалфавитная
многоконтурная

1. Простая одноалфавитная замена

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

Пример

Используя эту таблицу, зашифруем текст:

In this book the reader will find a comprehensive survey...

Получим следующее зашифрованное сообщение:

At omiy pbbe omr nrsirnfadd zail s xbwgnrmrtjafr jcnfru...

2. Многоалфавитная одноконтурная обыкновенная.

Суть: для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически.

Схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита.

Пример

Рабочая матрица для ключа САЛЬЕРИ.

Исходный текст - максимально допустимой ценой является пятьсот...

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	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
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	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Шифротекст - захмныын пифгцчичио жнюоф...

Последовательность шифрования:

- 1) Под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз.
- 2) Каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящиеся под ними букв ключа.
- 3) Полученный текст может разбиваться на группы по несколько знаков.

Пример расшифрования

Рабочая матрица для ключа САЛЬЕРИ.

Исходный текст - максимально...

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	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
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	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Ключ: сальерисальерисальерисальери

Шифротекст - захмныиын пифгцчичио жнюоф...

Рис. 3.4. Порядок расшифровки по таблице Вижинера

Недостаток шифрования по таблице

Вижинера: при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

3. Многоалфавитная монофоническая замена

Суть метода: количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки.

Монофоническая замена для английского языка

Алфавит открытого текста																										
А л ф а в и т ш и ф р о т е к с т а	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
	f	N	Q	.	G	T	,	D	A	e	L	-	R	(C	x	l	Z	V	--	W	S	h	u	K	t
	*	N	Q	b	+	[p	D)	e	L	O	R	y	/	x	l	=	\$	j	W	S	h	u	K	t
	k	N	Q	i]	W	r	D	q	e	L	и	R	(#	x	l	a	d	:	W	S	h	u	K	t
	f	N	Q	.	l	T	,	D	A	e	L	A	R	y	п	x	l	Z	V	C	W	S	h	u	K	t
	*	N	Q	b	G	[p	D)	e	L	O	R	(C	x	l	=	\$	--	W	S	h	u	K	t
	R	N	Q	i	+	W	r	D	q	e	L	и	R	y	/	x	l	a	d	j	W	S	h	u	K	t
	f	N	Q	.]	T	,	D	A	e	L	A	R	(#	x	l	Z	V	:	W	S	h	u	K	t
	*	N	Q	b	l	[p	D)	e	L	O	R	y	п	x	l	=	\$	C	W	S	h	u	K	t
	k	N	Q	i	G	W	r	D	q	e	L	и	R	(C	x	l	a	d	--	W	S	h	u	K	t
	f	N	Q	.	+	T	,	D	A	e	L	A	R	y	/	x	l	Z	V	j	W	S	h	u	K	t
	*	N	Q	b]	[p	D)	e	L	O	R	(#	x	l	=	\$:	W	S	h	u	K	t
	К	Н	Q	i	l	W	r	D	q	e	L	и	R	y	п	x	l	a	d	C	W	S	h	u	K	t

Пример

Исходный текст – In this book the reader will find a comprehensive survey...

Шифрованный текст – A(-,)

VNG/LjpGZ+F.=hg...

4. Многоалфавитная многоконтурная замена.

Суть: для шифрования используется циклически несколько наборов (контуров) алфавитов, причем каждый контур в общем случае имеет свой индивидуальный период применения.