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.

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

Пример
Рабочая матрица для ключа САЛЬЕРИ.

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 находящихся под ними букв ключа.

3) Полученный текст может разбиваться на группы по несколько знаков.

Пример расшифрования
Рабочая матрица для ключа САЛЬЕРИ.

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																								
Алфавит шифротекста	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	т	,	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	т	,	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	.	]	т	,	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	.	+	т	,	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
	K	**N**	**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.