Лабораторная работа 6

«Симметричные алгоритмы шифрования»

Теоретическая часть

Общая схема симметричного шифрования

Классическая, или одноключевая криптография опирается на использование **симметричных алгоритмов шифрования**, в которых шифрование и расшифрование отличаются только порядком выполнения и направлением некоторых шагов. Эти алгоритмы используют один и тот же секретный элемент (ключ), и второе действие (расшифрование) является простым обращением первого (шифрования). Поэтому обычно каждый из участников обмена может как зашифровать, так и расшифровать сообщение. Схематичная структура такой системы представлена на рис. 2.1.

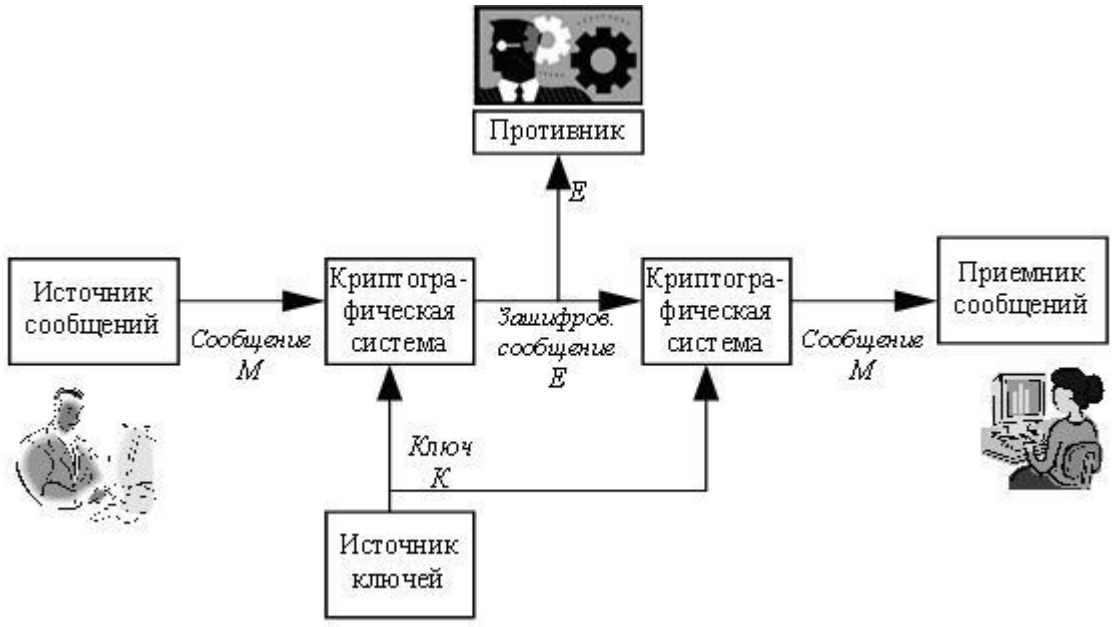

Рис. 2.1. Общая структура секретной системы, использующей симметричное шифрование

На передающей стороне имеются источник сообщений и источник ключей. Источник ключей выбирает конкретный ключ К среди всех возможных ключей данной системы. Этот ключ К передается некоторым способом принимающей стороне, причем предполагается, что его нельзя перехватить, например, ключ передается специальным курьером (поэтому симметричное шифрование называется также шифрованием с *закрытым ключом*). Источник сообщений формирует некоторое сообщение М, которое затем шифруется с использованием выбранного ключа. В результате процедуры шифрования получается зашифрованное сообщение Е (называемое также криптограммой).

Далее криптограмма E передается по каналу связи. Так как канал связи является открытым, незащищенным, например, радиоканал или компьютерная сеть, то передаваемое сообщение может быть перехвачено противником. На принимающей стороне криптограмму E с помощью ключа расшифровывают и получают исходное сообщение M.

Если M – сообщение, K – ключ, а E – зашифрованное сообщение, то можно записать

E=f(M,K)

то есть зашифрованное сообщение E является некоторой функцией от исходного сообщения M и ключа K. Используемый в криптографической системе метод или алгоритм шифрования и определяет функцию f в приведенной выше формуле.

По причине большой избыточности естественных языков непосредственно в зашифрованное сообщение чрезвычайно трудно внести осмысленное изменение, поэтому классическая криптография обеспечивает также защиту от навязывания ложных данных. Если же естественной избыточности оказывается недостаточно для надежной защиты сообщения от модификации, избыточность может быть искусственно увеличена путем добавления к сообщению специальной контрольной комбинации, называемой имитовставкой.

Известны разные методы шифрования с закрытым ключом рис. 2.2. На практике часто используются алгоритмы перестановки, подстановки, а также комбинированные методы.

Рис. 2.2. Методы шифрования с закрытым ключом

В методах перестановки символы исходного текста меняются местами друг с другом по определенному правилу. В методах замены (или подстановки) символы открытого текста заменяются некоторыми эквивалентами шифрованного текста. С целью повышения надежности шифрования текст, зашифрованный с помощью одного метода, может быть еще раз зашифрован с помощью другого метода. В этом случае получается комбинированный или композиционный шифр. Применяемые на практике в настоящее время блочные или поточные симметричные шифры также относятся к комбинированным, так как в них используется несколько операций для зашифрования сообщения.

Основное отличие современной криптографии от криптографии "докомпьютерной" заключается в том, что раньше криптографические алгоритмы оперировали символами естественных языков, например, буквами английского или русского алфавитов. Эти буквы переставлялись или заменялись другими по определенному правилу. В современных криптографических алгоритмах используются операции над двоичными знаками, то есть над нулями и единицами. В настоящее время основными операциями при шифровании также являются перестановка или подстановка, причем для повышения надежности шифрования эти операции применяются вместе (комбинируются) и помногу раз циклически повторяются.

Принципы построения современных блочных шифров сформулированы в "Принципы построения блочных шифров с закрытым ключом" , "Алгоритмы шифрования DES и AES" , "Алгоритм криптографического преобразования данных ГОСТ 28147-89" , а в этой лекции рассматриваются шифры подстановки и перестановки, применяемые человеком с древнейших времен. Мы должны познакомиться с этими шифрами, так как процедуры подстановки и перестановки используются в качестве составных операций и в современных блочных шифрах.

Методы замены

Методы шифрования заменой (подстановкой) основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

Одноалфавитная замена

Одним из важных подклассов методов замены являются *одноалфавитные* (или моноалфавитные) подстановки, в которых устанавливается однозначное соответствие между каждым знаком a_i исходного алфавита сообщений A и

соответствующим знаком e_i зашифрованного текста E. Одноалфавитная подстановка иногда называется также простой заменой, так как является самым простым шифром замены.

Примером одноалфавитной замены является шифр Цезаря, рассмотренный ранее. В рассмотренном в "Основные понятия криптографии" примере первая строка является исходным алфавитом, вторая (с циклическим сдвигом на k влево) – вектором замен.

В общем случае при одноалфавитной подстановке происходит однозначная замена исходных символов их эквивалентами из вектора замен (или таблицы замен). При таком методе шифрования ключом является используемая таблица замен.

Подстановка может быть задана с помощью таблицы, например, как показано на рис. 2.3.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Рис. 2.3. Пример таблицы замен для двух шифров

В таблице на рис. 2.3 на самом деле объединены сразу две таблицы. Одна (шифр 1) определяет замену русских букв исходного текста на другие русские буквы, а вторая (шифр 2) – замену букв на специальные символы. Исходным алфавитом для обоих шифров будут заглавные русские буквы (за исключением букв "Ё" и "Й"), пробел и точка.

Зашифрованное сообщение с использованием любого шифра моноалфавитной подстановки получается следующим образом. Берется очередной знак из исходного сообщения. Определяется его позиция в столбце "Откр. текст" таблицы замен. В зашифрованное сообщение вставляется шифрованный символ из этой же строки таблицы замен.

Попробуем зашифровать сообщение "ВЫШЛИТЕ ПОДКРЕПЛЕНИЕ" с использованием этих двух шифров (рис. 2.4). Для этого берем первую букву исходного сообщения "В". В таблице на рис. 2.3 в столбце "Шифр 1" находим

для буквы "В" заменяемый символ. Это будет буква "О". Записываем букву "О" под буквой "В". Затем рассматриваем второй символ исходного сообщения – букву "Ы". Находим эту букву в столбце "Откр. текст" и из столбца "Шифр 1" берем букву, стоящую на той же строке, что и буква "Ы". Таким образом получаем второй символ зашифрованного сообщения – букву "Н". Продолжая действовать аналогично, зашифровываем все исходное сообщение (рис. 2.4).

Открытое сообщение																			
В	Ы	Ш	Л	И	Т	Е		П	О	Д	К	Р	Е	П	Л	Е	Н	И	Е
Зашифрованное сообщение с использованием шифра 1																			
О	Н	У	Р	Ъ	Х	П	Ф	Ж	.	Щ		Г	П	Ж	Р	П	Ц	Ъ	П
Зашифрованное сообщение с использованием шифра 2																			
)	⊕	∇	♠	*	%	>	∞	=	-	<	♥	(	>	=	♠	>	#	*	>

Рис. 2.4. Пример шифрования методом прямой замены

Полученный таким образом текст имеет сравнительно низкий уровень защиты, так как исходный и зашифрованный тексты имеют одинаковые статистические закономерности. При этом не имеет значения, какие символы использованы для замены – перемешанные символы исходного алфавита или таинственно выглядящие знаки.

Зашифрованное сообщение может быть вскрыто путем так называемого *частотного криптоанализа*. Для этого могут быть использованы некоторые статистические данные языка, на котором написано сообщение.

Известно, что в текстах на русском языке наиболее часто встречаются символы О, И. Немного реже встречаются буквы Е, А. Из согласных самые частые символы Т, Н, Р, С. В распоряжении криптоаналитиков имеются специальные таблицы частот встречаемости символов для текстов разных типов – научных, художественных и т.д.

Криптоаналитик внимательно изучает полученную криптограмму, подсчитывая при этом, какие символы сколько раз встретились. Вначале наиболее часто встречаемые знаки зашифрованного сообщения заменяются, например, буквами О. Далее производится попытка определить места для букв И, Е, А. Затем подставляются наиболее часто встречаемые согласные. На каждом этапе оценивается возможность "сочетания" тех или иных букв. Например, в русских словах трудно найти четыре подряд гласные буквы, слова в русском языке не начинаются с буквы Ы и т.д. На самом деле для каждого естественного языка (русского, английского и т.д.) существует

множество закономерностей, которые помогают раскрыть специалисту зашифрованные противником сообщения.

Возможность однозначного криптоанализа напрямую зависит от длины перехваченного сообщения. Посмотрим, с чем это связано. Пусть, например, в руки криптоаналитиков попало зашифрованное с помощью некоторого шифра одноалфавитной замены сообщение:

ТНФЖ.ИПЩЪРЪ

Это сообщение состоит из 11 символов. Пусть известно, что эти символы составляют целое сообщение, а не фрагмент более крупного текста. В этом случае наше зашифрованное сообщение состоит из одного или нескольких целых слов. В зашифрованном сообщении символ Ъ встречается 2 раза. Предположим, что в открытом тексте на месте зашифрованного знака Ъ стоит гласная О, А, И или Е. Подставим на место Ъ эти буквы и оценим возможность дальнейшего криптоанализа таблица 2.1

Таблица 2.1. Варианты первого этапа криптоанализа

Зашифрованное сообщение										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
После замены Ъ на О										
								О		О
После замены Ъ на А										
								А		А
После замены Ъ на И										
								И		И
После замены Ъ на Е										
								Е		Е

Все приведенные варианты замены могут встретиться на практике. Попробуем подобрать какие-нибудь варианты сообщений, учитывая, что в криптограмме остальные символы встречаются по одному разу (таблица 2.2).

Таблица 2.2. Варианты второго этапа криптоанализа

Зашифрованное сообщение										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
Варианты подобранных дешифрованных сообщений										
Ж	Д	И		С	У	М	Р	А	К	А
Д	Ж	О	Н	А		У	Б	И	Л	И
В	С	Е	Х		П	О	Б	И	Л	И
М	Ы		П	О	Б	Е	Д	И	Л	И

Кроме представленных на таблица 2.2 сообщений можно подобрать еще большое количество подходящих фраз. Таким образом, если нам ничего не

известно заранее о содержании перехваченного сообщения малой длины, дешифровать его однозначно не получится.

Если же в руки криптоаналитиков попадает достаточно длинное сообщение, зашифрованное методом простой замены, его обычно удается успешно дешифровать. На помощь специалистам по вскрытию криптограмм приходят статистические закономерности языка. Чем длиннее зашифрованное сообщение, тем больше вероятность его однозначного дешифрования.

В "Алгоритм криптографического преобразования данных ГОСТ 28147-89" будут более подробно рассмотрены вопросы теоретической стойкости криптосистем, а также принципы построения идеальных криптосистем.

Интересно, что если попытаться замаскировать статистические характеристики открытого текста, то задача вскрытия шифра простой замены значительно усложнится. Например, с этой целью можно перед шифрованием "сжимать" открытый текст с использованием компьютерных программ-архиваторов.

С усложнением правил замены увеличивается надежность шифрования. Можно заменять не отдельные символы, а, например, двухбуквенные сочетания – биграммы. Таблица замен для такого шифра может выглядеть, как на таблица 2.3.

Таблица 2.3. Пример таблицы замен для двухбуквенных сочетаний

Откр. текст	Зашифр. текст	Откр. текст	Зашифр. текст
аа	кх	бб	пш
аб	пу	бв	вь
ав	жа	...	...
...	...	яэ	сы
ая	ис	яю	ек
ба	цу	яя	рт

Оценим размер такой таблицы замен. Если исходный алфавит содержит N символов, то вектор замен для биграммного шифра должен содержать N^2 пар "откр. текст – зашифр. текст". Таблицу замен для такого шифра можно также записать и в другом виде: заголовки столбцов соответствуют первой букве биграммы, а заголовки строк – второй, причем ячейки таблицы заполнены заменяющими символами. В такой таблице будет N строк и N столбцов (таблица 2.4).

Таблица 2.4. Другой вариант задания таблицы замен для биграммного шифра

	а	б	...	я
а	кх	цу	...	...
б	пу	пш	...	...
в	жа	вь	...	...

…	…	…	…	…
ю	…	…	…	ек
я	ис	…	…	рт

Возможны варианты использования триграммного или вообще n-граммного шифра. Такие шифры обладают более высокой криптостойкостью, но они сложнее для реализации и требуют гораздо большего количества ключевой информации (большой объем таблицы замен). В целом, все n-граммные шифры могут быть вскрыты с помощью частотного криптоанализа, только используется статистика встречаемости не отдельных символов, а сочетаний из n символов.

Пропорциональные шифры

К одноалфавитным методам подстановки относятся **пропорциональные** или **монофонические шифры**, в которых уравнивается частота появления зашифрованных знаков для защиты от раскрытия с помощью частотного анализа. Для знаков, встречающихся часто, используется относительно большое число возможных эквивалентов. Для менее используемых исходных знаков может оказаться достаточным одного или двух эквивалентов. При шифровании замена для символа открытого текста выбирается либо случайным, либо определенным образом (например, по порядку).

При использовании пропорционального шифра в качестве замены символам обычно выбираются числа. Например, поставим в соответствие буквам русского языка трехзначные числа, как указано на таблица 2.5.

Таблица 2.5. Таблица замен для пропорционального шифра

Символ	Варианты замены					Символ	Варианты замены				
А	760	128	350	201		С	800	767	105		
Б	101					Т	759	135	214		
В	210	106				У	544				
Г	351					Ф	560				
Д	129					Х	768				
Е	761	130	802	352		Ц	545				
Ж	102					Ч	215				
З	753					Ш	103				
И	762	211	131			Щ	752				
К	754	764				Ъ	561				
Л	132	354				Ы	136				
М	755	742				Ь	562				
Н	763	756	212			Э	750				
О	757	213	765	133	353	Ю	570				

П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035…

В этом случае сообщение

БОЛЬШОЙ СЕКРЕТ

может быть зашифровано следующим образом:

10175713256210321376275180076175413413075 9

В данном примере варианты замен для повторяющихся букв (например, "О") выбирались по порядку.

Интересно, что шифры, в которых производится замена букв несколькими символами, пропорционально встречаемости в открытом тексте, описывали итальянские ученые еще в XIV-XV веках.

Пропорциональные шифры более сложны для вскрытия, чем шифры простой одноалфавитной замены. Однако, если имеется хотя бы одна пара "открытый текст – шифротекст", вскрытие производится тривиально. Если же в наличии имеются только шифротексты, то вскрытие ключа, то есть нахождение таблицы замен, становится более трудоемким, но тоже вполне осуществимым.

Многоалфавитные подстановки

В целях маскирования естественной частотной статистики исходного языка применяется многоалфавитная подстановка, которая также бывает нескольких видов. В **многоалфавитных подстановках** для замены символов исходного текста используется не один, а несколько алфавитов. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке.

Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Вижинера. Этот метод, известный уже в XVI веке, был описан французом Блезом Вижинером в "Трактате о шифрах", вышедшем в 1585 году.

В этом методе для шифрования используется таблица, представляющая собой квадратную матрицу с числом элементов NxN, где N — количество символов в алфавите (таблица 2.6). В первой строке матрицы записывают буквы в порядке очередности их в исходном алфавите, во второй — ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д.

Таблица 2.6. Подготовка таблицы шифрования

АБВГДЕ.....	.....ЭЮЯ
БВГДЕЖ.....	.....ЮЯА
ВГДЕЖЗ.....	.....ЯАБ
ГДЕЖЗИ.....	.....АБВ

ДЕЖЭИК.....	.....БВГ
ЕЖЗИКЛ.....	.....ВГД
.....	.....
ЯАБВГД.....	.....ЬЭЮ

Для шифрования текста выбирают ключ, представляющий собой некоторое слово или набор символов исходного алфавита. Далее из полной матрицы выписывают подматрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются последовательно буквы ключа (например, если выбрать ключ "весна", то таблица шифрования будет такой, как на таблица 2.7).

Таблица 2.7. Первый этап шифрования – составление подматрицы шифрования

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ
СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР

В процессе шифрования (рис. 2.5) под каждой буквой шифруемого текста записывают буквы ключа, повторяющие ключ требуемое число раз, затем шифруемый текст по таблице шифрования (таблица 2.7) заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки таблицы и буквы ключа, находящейся под ней.

Например, под первой буквой исходного текста "М" записана буква "В" ключа. В таблице кодирования находим столбец, начинающийся с "М" и строку, начинающуюся с "В". На их пересечении располагается буква "О". Она и будет первым символом зашифрованного сообщения (на рис. 2.5 эта буква выделена прямоугольной рамочкой). Следующая буква исходного сообщения – "Е", символ ключа – тоже "Е". Находим пересечение строки, начинающейся с "Е", и столбца, начинающегося с "Е". Это будет буква "Л" – второй символ зашифрованного сообщения.

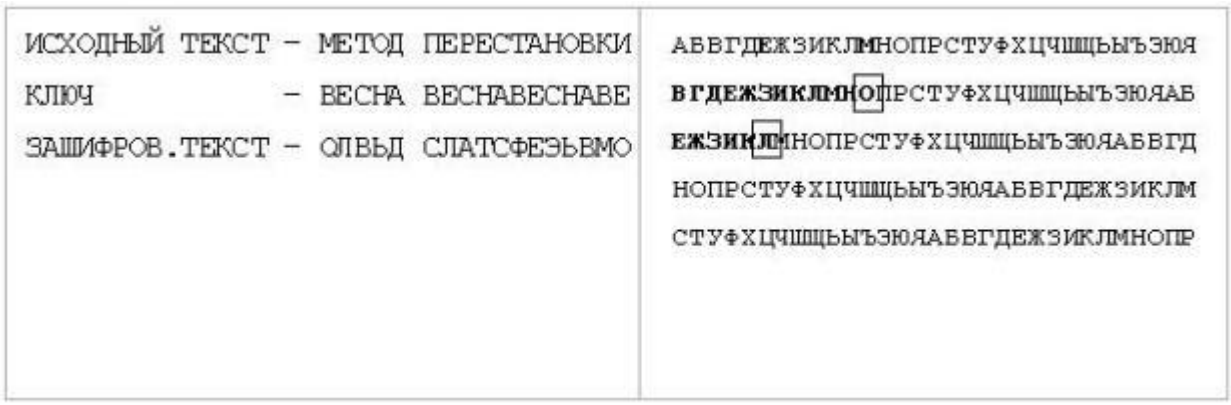

Рис. 2.5. Механизм шифрования многоалфавитной заменой

Рассмотрим на примере процесс расшифрования сообщения по методу Вижинера. Пусть имеется зашифрованное с помощью ключа ВЕСНА сообщение КЕКХТВОЭЦОТССВИЛ (пробелы при шифровании пропущены). Расшифровка текста выполняется в следующей последовательности (таблица 2.8):

- над буквами шифрованного текста сверху последовательно записывают буквы ключа, повторяя ключ требуемое число раз;
- в строке подматрицы таблицы Вижинера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста;
- полученный текст группируется в слова по смыслу.

Таблица 2.8. Механизм расшифрования

КЛЮЧ	ВЕСНАВЕСНАВЕСНАВ
ЗАШИФРОВАННЫЙ ТЕКСТ	КЕКХТВОЭЦОТССВИЛ
РАСШИФРОВАННЫЙ ТЕКСТ	ЗАЩИТАИНФОРМАЦИИ
ИСХОДНЫЙ ТЕКСТ	ЗАЩИТА ИНФОРМАЦИИ

Раскрыть шифр Вижинера, тем же способом, что и шифр одноалфавитной замены, невозможно, так как одни и те же символы открытого текста могут быть заменены различными символами зашифрованного текста. С другой стороны, различные буквы открытого текста могут быть заменены одинаковыми знаками зашифрованного текста.

Особенность данного метода многоалфавитной подстановки заключается в том, что каждый из символов ключа используется для шифрования одного символа исходного сообщения. После использования всех символов ключа,

они повторяются в том же порядке. Если используется ключ из десяти букв, то каждая десятая буква сообщения шифруется одним и тем же символом ключа. Этот параметр называется *периодом* шифра. Если ключ шифрования состоит из одного символа, то при шифровании будет использоваться одна строка таблицы Вижинера, следовательно, в этом случае мы получим моноалфавитную подстановку, а именно шифр Цезаря.

С целью повышения надежности шифрования текста можно использовать подряд два или более зашифрования по методу Вижинера с разными ключами (составной шифр Вижинера).

На практике кроме метода Вижинера использовались также различные модификации этого метода. Например, шифр Вижинера с перемешанным один раз алфавитом. В этом случае для расшифрования сообщения получателю необходимо кроме ключа знать порядок следования символов в таблице шифрования.

Еще одним примером метода многоалфавитной подстановки является *шифр с бегущим ключом* или *книжный шифр*. В этом методе один текст используется в качестве ключа для шифрования другого текста. В эпоху "докомпьютерной" криптографии в качестве ключа для шифра с бегущим ключом выбирали какую-нибудь достаточно толстую книгу; от этого и произошло второе название этого шифра. Периодом в таком методе шифрования будет длина выбранного в качестве ключа произведения.

Методы многоалфавитной подстановки, в том числе и метод Вижинера, значительно труднее поддаются "ручному" криптоанализу. Для вскрытия методов многоалфавитной замены разработаны специальные, достаточно сложные алгоритмы. С использованием компьютера вскрытие метода многоалфавитной подстановки возможно достаточно быстро благодаря высокой скорости проводимых операций и расчетов.

В первой половине XX века для автоматизации процесса выполнения многоалфавитных подстановок стали широко применять *роторные шифровальные машины*. Главными элементами в таких устройствах являлись роторы – механические колеса, используемые для выполнения подстановки. Роторная шифровальная машина содержала обычно клавиатуру и набор роторов. Каждый ротор содержал набор символов (по количеству в алфавите), размещенных в произвольном порядке, и выполнял простую одноалфавитную подстановку. После выполнения первой замены символы сообщения обрабатывались вторым ротором и так далее. Роторы могли смещаться, что и задавало ключ шифрования. Некоторые роторные машины выполняли также и перестановку символов в процессе шифрования. Самым известным устройством подобного класса являлась немецкая шифровальная

роторная машина Энигма (лат. Enigma — загадка), использовавшаяся во время второй мировой войны. Выпускалось несколько моделей Энигмы с разным числом роторов. В шифрмашине Энигма с тремя роторами можно было использовать 16900 разных алфавитов, и все они представляли собой различные перестановки символов.

Методы гаммирования

Еще одним частным случаем многоалфавитной подстановки является **гаммирование**. В этом способе шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33. Такой процесс сложения исходного текста и ключа называется в криптографии *наложением гаммы*.

Пусть символам исходного алфавита соответствуют числа от 0 (А) до 32 (Я). Если обозначить число, соответствующее исходному символу, x, а символу ключа – k, то можно записать правило гаммирования следующим образом:

$$z = x + k \pmod N,$$

где z – закодированный символ, N - количество символов в алфавите, а сложение по модулю N - операция, аналогичная обычному сложению, с тем отличием, что если обычное суммирование дает результат, больший или равный N, то значением суммы считается остаток от деления его на N. Например, пусть сложим по модулю 33 символы Г (3) и Ю (31):

$$3 + 31 \pmod{33} = 1,$$

то есть в результате получаем символ Б, соответствующий числу 1.

Наиболее часто на практике встречается двоичное гаммирование. При этом используется двоичный алфавит, а сложение производится по модулю два. Операция сложения по модулю 2 часто обозначается $\oplus$, то есть можно записать:

$$z = x + k(mod 2) = x \oplus k.$$

Операция сложения по модулю два в алгебре логики называется также "исключающее ИЛИ" или по-английски XOR.

Рассмотрим пример. Предположим, нам необходимо зашифровать десятичное число 14 методом гаммирования с использованием ключа 12. Для этого вначале необходимо преобразовать исходное число и ключ (гамму) в двоичную форму: $14_{(10)}=1110_{(2)}$, $12_{(10)}=1100_{(2)}$. Затем надо записать полученные двоичные числа друг под другом и каждую пару символов сложить по модулю два. При сложении двух двоичных знаков получается 0, если исходные двоичные цифры одинаковы, и 1, если цифры разные:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Сложим по модулю два двоичные числа 1110 и 1100:

```
Исходное число 1 1 1 0
Гамма     1 1 0 0
Результат   0 0 1 0
```

В результате сложения получили двоичное число 0010. Если перевести его в десятичную форму, получим 2. Таким образом, в результате применения к числу 14 операции гаммирования с ключом 12 получаем в результате число 2.

Каким же образом выполняется расшифрование? Зашифрованное число 2 представляется в двоичном виде и снова производится сложение по модулю 2 с ключом:

```
Зашифрованное число 0 0 1 0
Гамма      1 1 0 0
Результат    1 1 1 0
```

Переведем полученное двоичное значение 1110 в десятичный вид и получим 14, то есть исходное число.

Таким образом, при гаммировании по модулю 2 нужно использовать одну и ту же операцию как для зашифрования, так и для расшифрования. Это позволяет использовать один и тот же алгоритм, а соответственно и одну и ту же программу при программной реализации, как для шифрования, так и для расшифрования.

Операция сложения по модулю два очень быстро выполняется на компьютере (в отличие от многих других арифметических операций), поэтому наложение гаммы даже на очень большой открытый текст выполняется практически мгновенно.

Благодаря указанным достоинствам метод гаммирования широко применяется в современных технических системах сам по себе, а также как элемент комбинированных алгоритмов шифрования.

Сформулируем, как производится гаммирование по модулю 2 в общем случае:

- символы исходного текста и гамма представляются в двоичном коде и располагаются один под другим, при этом ключ (гамма) записывается столько раз, сколько потребуется;
- каждая пара двоичных знаков складывается по модулю два;

- полученная последовательность двоичных знаков кодируется символами алфавита в соответствии с выбранным кодом.

На рис. 2.6 показано, как применяется гаммирование к тексту с русскими символами. Символы кодируются в соответствии с принятой кодировкой, а затем производится сложение по модулю 2.

При использовании метода гаммирования ключом является последовательность, с которой производится сложение – гамма. Если гамма короче, чем сообщение, предназначенное для зашифрования, гамма повторяется требуемое число раз. Так в примере на рис. 2.6 длина исходного сообщения равна двенадцати байтам, а длина ключа – пяти байтам. Следовательно, для зашифрования гамма должна быть повторена 2 раза полностью и еще один раз частично.

Рис. 2.6. Механизм гаммирования

Чем длиннее ключ, тем надежнее шифрование методом гаммирования. Связь длины ключа с вероятностью вскрытия сообщения, а также некоторые принципы дешифрования сообщений, закрытых методом гаммирования, обсуждаются в "Поточные шифры и генераторы псевдослучайных чисел. Часть 2" и "Шифрование, помехоустойчивое кодирование и сжатие

информации" . На практике длина ключа ограничена возможностями аппаратуры обмена данными и вычислительной техники, а именно выделяемыми объемами памяти под ключ, временем обработки сообщения, а также возможностями аппаратуры подготовки и записи последовательностей ключей. Кроме того, для использования ключа вначале необходимо каким-либо надежным способом доставить его обеим сторонам, обменивающимся сообщениями. Это приводит к возникновению проблемы распределения ключей, сложность решения которой возрастает с увеличением длины ключа и количества абонентов в сети передачи сообщений.

Методы перестановки

При использовании шифров **перестановки** входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов. Перестановки в классической "докомпьютерной" криптографии получались в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.

Простейшим примером перестановки является *перестановка с фиксированным периодом d*. В этом методе сообщение делится на блоки по *d* символов и в каждом блоке производится одна и та же перестановка. Правило, по которому производится перестановка, является ключом и может быть задано некоторой перестановкой первых *d* натуральных чисел. В результате сами буквы сообщения не изменяются, но передаются в другом порядке.

Например, для d=6 в качестве ключа перестановки можно взять 436215. Это означает, что в каждом блоке из 6 символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д. Пусть необходимо зашифровать такой текст:

ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ

Количество символов в исходном сообщении равно 24, следовательно, сообщение необходимо разбить на 4 блока. Результатом шифрования с помощью перестановки 436215 будет сообщение

_ОЕТЭТ_ТЛСКДИШР_ЯФНАЯВОИ

Теоретически, если блок состоит из *d* символов, то число возможных перестановок d!=1*2*...*(d-1)*d. В последнем примере d=6, следовательно, число перестановок равно 6!=1*2*3*4*5*6=720. Таким образом, если противник перехватил зашифрованное сообщение из рассмотренного примера, ему понадобится не более 720 попыток для раскрытия исходного сообщения (при условии, что размер блока известен противнику).

Для повышения криптостойкости можно последовательно применить к шифруемому сообщению две или более перестановки с разными периодами.

Другим примером методов перестановки является *перестановка по таблице*. В этом методе производится запись исходного текста по строкам некоторой таблицы и чтение его по столбцам этой же таблицы. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом.

Рассмотрим пример. Пусть в таблице кодирования будет 4 столбца и 3 строки (размер блока равен 3*4=12 символов). Зашифруем такой текст:

ЭТО ТЕКСТ ДЛЯ ШИФРОВАНИЯ

Количество символов в исходном сообщении равно 24, следовательно, сообщение необходимо разбить на 2 блока. Запишем каждый блок в свою таблицу по строчкам (таблица 2.9).

Таблица 2.9. Шифрование методом перестановки по таблице

1 блок			
Э	Т	О	
Т	Е	К	С
Т		Д	Л
2 блок			
Я		Ш	И
Ф	Р	О	В
А	Н	И	Я

Затем будем считывать из таблицы каждый блок последовательно по столбцам:

ЭТТТЕ ОКД СЛЯФА РНШОИИВЯ

Можно считывать столбцы не последовательно, а, например, так: третий, второй, первый, четвертый:

ОКДТЕ ЭТТ СЛШОИ РНЯФАИВЯ

В этом случае порядок считывания столбцов и будет ключом.

В случае, если размер сообщения не кратен размеру блока, можно дополнить сообщение какими-либо символами, не влияющими на смысл, например, пробелами. Однако это делать не рекомендуется, так как это дает противнику в случае перехвата криптограммы информацию о размере используемой таблицы перестановок (длине блока). После определения длины блока противник может найти длину ключа (количество столбцов таблицы) среди делителей длины блока.

Посмотрим, как зашифровать и расшифровать сообщение, имеющее длину, не кратной размеру таблицы перестановки. Зашифруем слово

ПЕРЕМЕНКА

Количество символов в исходном сообщении равно 9. Запишем сообщение в таблицу по строкам (таблица 2.10), а последние три ячейки оставим пустыми.

Таблица 2.10. Шифрование неполного блока методом перестановки по таблице			
П	Е	Р	Е
М	Е	Н	К
А			

Затем будем считывать из таблицы последовательно по столбцам:
ПМАЕЕРНЕК

Для расшифрования вначале определяют число полных столбцов, то есть количество символов в последней строке. Для этого делят размер сообщения (в нашем примере – 9) на количество столбцов или размер ключа (в примере – 4). Остаток от деления будет числом полных столбцов: 9 mod 4 = 1. Следовательно, в нашем примере был 1 полный столбец и три коротких. Теперь можно поставить буквы сообщения на свои места и расшифровать сообщение. Так как ключом при шифровании было число 1234 (столбцы считывались последовательно), то при расшифровании первые три символа (ПМА) записываются в первый столбец таблицы перестановки, следующие два (ЕЕ) – во второй столбец, следующие два (РН) – в третий, и последние два (ЕК) – в четвертый. После заполнения таблицы считываем строки и получаем исходное сообщение ПЕРЕМЕНКА.

Существуют и другие способы перестановки, которые можно реализовать программным и аппаратным путем. Например, при передаче данных, записанных в двоичном виде, удобно использовать аппаратный блок, который перемешивает определенным образом с помощью соответствующего электрического монтажа биты исходного n-разрядного сообщения. Так, если принять размер блока равным восьми битам, можно, к примеру, использовать такой блок перестановки, как на рис. 2.7.

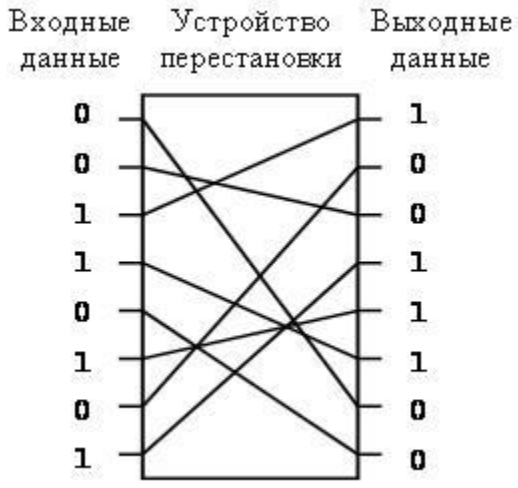

Рис. 2.7. Аппаратный блок перестановки

Для расшифрования на приемной стороне устанавливается другой блок, восстанавливающий порядок цепей.

Аппаратно реализуемая перестановка широко используется на практике как составная часть некоторых современных шифров.

При перестановке любого вида в зашифрованное сообщение будут входить те же символы, что и в открытый текст, но в другом порядке. Следовательно, статистические закономерности языка останутся без изменения. Это дает криптоаналитику возможность использовать различные методы для восстановления правильного порядка символов.

Если у противника есть возможность пропускать через систему шифрования методом перестановки специально подобранные сообщения, то он сможет организовать атаку по выбранному тексту. Так, если длина блока в исходном тексте равна N символам, то для раскрытия ключа достаточно пропустить через шифровальную систему N-1 блоков исходного текста, в которых все символы, кроме одного, одинаковы. Другой вариант атаки по выбранному тексту возможен в случае, если длина блока N меньше количества символов в алфавите. В этом случае можно сформировать одно специальное сообщение из разных букв алфавита, расположив их, например, по порядку следования в алфавите. Пропустив подготовленное таким образом сообщение через шифровальную систему, специалисту по криптоанализу останется только посмотреть, на каких позициях очутились символы алфавита после шифрования, и составить схему перестановки.

Мы рассмотрели общую схему симметричного шифрования и классификацию простейших методов шифрования с закрытым ключом. В следующей лекции мы познакомимся с принципами построения современных блочных алгоритмов

Практическая часть

Задание 1

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №1

- И.РЮУ.ЪФОБГНО
- СЛХГ.ЪЛХО.ФОО.ЩВ

2. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	∑
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №2:

- $\nabla * !(\infty \blacklozenge № > \sharp \oplus$
- $@\spadesuit - \heartsuit \infty \nabla * !(-) \sharp * \Delta$

3. Пусть исходный алфавит содержит следующие символы:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:

- КРИПТОСТОЙКОСТЬ
- ГАММИРОВАНИЕ

4. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):

5. АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_

Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:

- ШВМБУЖНЯ
- ЯБХЪШЮМХ

Задание 2

6. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?

7. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?

Задание 3

8. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:

- ЖЕЛТЫЙ_ОГОНЬ
- МЫ_НАСТУПАЕМ

9. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:

- СЛПИЬНАЕ
- РОИАГДВН

10. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:

- МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
- СИГНАЛ БОЯ – НИСАГО ЛЯБ

11. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании.

- ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)
- ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)

12. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.

- ЕАУПД_КЕАЗАРЧВ (ключ: 4123)
- А_НСЫИЛБСАЛЙГ (ключ: 3142)

Задание 4

13. Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:

Таблица замен для пропорционального шифра												
Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	035…

14. Расшифруйте указанные сообщения.

- 353214764134136759136762849754128212350354035767106216753211
- 351 761756130532128759353134758105757213101752352763211762

Вопросы для самопроверки

1. Поясните общую схему симметричного шифрования.
2. Что общего имеют все методы шифрования с закрытым ключом?
3. Назовите основные группы методов шифрования с закрытым ключом.
4. Приведите примеры шифров перестановки.
5. Сформулируйте общие принципы для методов шифрования подстановкой.
6. В чем заключаются многоалфавитные подстановки?
7. Приведите пример шифра одноалфавитной замены.
8. Опишите алгоритм любого метода шифрования перестановкой. Приведите пример шифрования некоторого сообщения этим методом. Каков алгоритм расшифрования в этом методе?
9. К какой группе методов шифрования с закрытым ключом относится метод с использованием таблицы Вижинера? Каковы алгоритмы шифрования и расшифрования в этом методе? Приведите пример шифрования некоторого сообщения этим методом.
10. Каким образом можно зашифровать и расшифровать сообщение методом табличной перестановки, если размер шифруемого сообщения не кратен размеру блока?
11. Что такое монофонические шифры?