В.Н. Салий

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Саратов – 2017

Содержание

Раздел I. ОСНОВНЫЕ КЛАССЫ ШИФРОВ

Тема 1. *ОБЩИЕ И ИСТОРИЧЕСКИЕ СВЕДЕНИЯ.*

Криптография (от греческого *тайнопись*) – это совокупность идей и методов, связанных с преобразованием информации с целью ее защиты от непредусмотренных пользователей. Информация считается представленной в виде некоторого текста (сообщения). Это – *открытый текст*. Способ его преобразования в защищенную форму называется *шифром*, процесс применения шифра – *шифрованием*, полученный в результате шифрования измененный текст – *криптограммой.* Перевод криптограммы в исходный открытый текст производится в ходе *дешифрования*.

Взаимно обратные действия шифрования и дешифрования осуществляются с помощью некоторой дополнительной информации, называемой *ключом.* Именно в ключе спрятан секрет шифра. Без знания ключа чтение криптограммы должно быть значительно затруднено или практически невозможно в пределах разумного интервала времени.

Одним из самых давних и до сих пор широко используемых методов криптографической защиты информации является применение так называемых кодовых книг. *Кодовая книга* – это своего рода словарь, в котором содержится список часто применяемых в секретной переписке слов, целых фраз, цифровых групп и т.п. с указанием для каждого фрагмента того набора символов, которым он будет заменен при шифровании. Кодовая книга и является ключом шифра.

Чтобы читать зашифрованные сообщения, их получатель должен знать соответствующие секретные ключи. Как правило, источник сообщения заранее передает их по защищенному каналу. Передача ключей и их хранение – самое уязвимое место в практической криптографии. Известны многочисленные случаи похищения, копирования, покупки кодовых книг, использовавшихся в дипломатической переписке, драматические истории,

связанные с обнаружением секретных ключей при обысках у подозреваемых в шпионаже.

Криптография является одной из трех составных частей *криптологии* – науки о передаче информации в виде, защищенном от несанкционированного доступа. Криптография, как было сказано, занимается шифрованием и дешифрованием сообщений с помощью секретных ключей. Другая часть криптологии – *криптоанализ* – представляет собой теорию и практику извлечения информации из криптограммы без использования ключа. Основной принцип криптоанализа сформулировал один из его основоположников бельгийский криптолог Огюст Керкхофс (1835-1903) в 1883 году в книге «Военная криптография»: «При оценке надежности шифра следует допустить, что противнику известно о нем все, кроме ключа». Третья часть криптологии – *аутентификация* – объединяет в себе совокупность приемов, позволяющих проверять подлинность источника информации и полученных сообщений.

В истории криптологии отчетливо выделяются три периода. Первый – интуитивная криптология, представлявшая собой занятие, доступное узкому кругу изобретательных умов. В их число входили, в частности, многие выдающиеся математики своего времени.

Второй период открывается публикацией в 1949 году статьи американского инженера и математика Клода Шеннона (1916-2001) «Теория связи в секретных системах». Под влиянием высказанных в ней идей криптология стала в последующие годы фактически разделом прикладной математики.

Третий период начинается с появления в 1978 году новой системы шифрования RSA, в которой американские криптографы Ривест, Шамир и Адлмен впервые реализовали на практике идею организации защищенной связи без передачи секретных ключей.

Криптология вплоть до недавнего времени была глубоко засекречена во всех странах, так как сферой ее применений была в основном защита

государственных и военных секретов. Лишь начиная с 1970-х годов, методы и средства криптологии официально стали использоваться для обеспечения информационной безопасности не только государства, но и частных лиц и организаций.

Отметим некоторые ключевые даты в развитии отечественной криптологии в XX веке.

5 мая 1921 года была образована криптографическая служба при ВЧК (Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем). 5 мая в нашей стране ежегодно отмечается День шифровальщика.

19 октября 1949 года было принято решение Центрального комитета ВКП(б) (Всесоюзная коммунистическая партия (большевиков)) о создании Главного управления специальной службы (ГУСС) – координатора единой криптографической службы СССР. 19 октября в нашей стране ежегодно отмечается День криптографа. (Заметим для полноты, что криптографическая служба США - Агентство Национальной безопасности – существует с 1952 года).

Месяцем ранее, 23 сентября 1949 года, был осуществлен первый набор студентов на закрытое отделение механико-математического факультета МГУ для подготовки кадров в области криптографии. Оно просуществовало до 1957 года.

Тогда же, в 1949 году, открылась Высшая школа криптографов (ВШК) с двухлетним обучением, обеспечивавшая получение второго высшего специального образования. В 1960 году ВШК была преобразована в технический факультет Высшей школы КГБ (Комитет государственной безопасности).

В 1992 году был создан Институт криптографии, связи и информатики (ИКСИ) в составе Академии ФСБ России.

В Доктрине информационной безопасности Российской Федерации, принятой в 2000 году, отмечается, что «подготовка специалистов с высшим

образованием в области информационной безопасности относится к важнейшим организационно-техническим методам обеспечения информационной безопасности РФ».

С середины 1990-х годов в ряде вузов страны начала развертываться система подготовки кадров в естественнонаучном и техническом направлениях в области информационной безопасности, в том числе и по разделам криптологии. В 2001 году в Саратовском государственном университете была лицензирована специальность 075200 (ныне 090102) «Компьютерная безопасность» со специализацией «Математические методы защиты информации». В 2002 г. был проведен первый набор студентов. В том же году в СГУ был создан Центр переподготовки и повышения квалификации специалистов по информационной безопасности, в программе которого реализуется настоящий курс.

Тема 2. *ПЕРЕСТАНОВОЧНЫЕ ШИФРЫ.*

За всю историю человечества было изобретено огромное количество шифров. Однако внимательное изучение показало, что подавляющее их число укладывается во вполне обозримое множество теоретических схем, важнейшие из которых будут представлены далее.

Шифр называется *перестановочным*, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Как запомнить (и передать другому лицу) выбранный способ перестановки? Рассмотрим два широко распространенных метода.

а) Маршрутное шифрование.

Этот способ шифрования изобрел выдающийся французский математик и криптограф Франсуа Виет (1540-1603). Пусть m и n – некоторые натуральные (т.е. целые положительные) числа, каждое больше 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной

произведению mn (если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор). Блок вписывается построчно в таблицу размерности $m \times n$ (т.е. m строк и n столбцов). Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра. Чаще всего буквы выписывают по столбцам, которые упорядочиваются в соответствии с *паролем*: под таблицей подписывается слово, состоящее из n неповторяющихся букв, и столбцы таблицы нумеруются по алфавитному порядку букв пароля. Например, для шифрования открытого текста, выражающего один из главных принципов криптологии: *нельзя недооценивать противника*, добавим к его 29 буквам еще одну, скажем *а,* возьмем m=5, n=6, впишем текст в таблицу 5×6 и выберем в качестве пароля слово п а р о л ь:

н	е	л	ь	з	я
н	е	д	о	о	ц
е	н	и	в	а	т
ь	п	р	о	т	и
в	н	и	к	а	а
п	*а*	*р*	*о*	*л*	*ь*

Выписывая теперь буквы по столбцам в соответствии с алфавитным порядком букв в пароле, получаем следующую криптограмму: ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦТИА (истинные пробелы в криптографии не выставляются).

Выберите другой пароль и посмотрите, как изменится криптограмма.

Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

б) Шифрование с помощью решеток.

Этот способ шифрования предложил в 1881 году австрийский криптограф Эдуард Флейснер.

Выбирается натуральное число $k > 1$, и квадрат размерности $k \times k$ построчно заполняется числами 1, 2, …, k^2. Для примера возьмем $k = 2$.

Квадрат поворачивается по часовой стрелке на 90° и размещается вплотную к предыдущему квадрату. Аналогичные действия совершаются еще два раза, так чтобы в результате из четырех малых квадратов образовался один большой с длиной стороны 2*k*.

1	2	3	**1**
3	4	4	2
2	**4**	4	**3**
1	3	**2**	1

Далее из большого квадрата вырезаются клетки с числами от 1 до k^2, для каждого числа одна клетка. Процесс шифрования происходит следующим образом. Сделанная решетка (квадрат с прорезями) накладывается на чистый квадрат $2k \times 2k$ и в прорези по строчкам (т.е. слева направо и сверху вниз) вписываются первые буквы открытого текста. Затем решетка поворачивается на 90° по часовой стрелке и накладывается на частично заполненный квадрат, вписывание продолжается. После третьего поворота, наложения и вписывания все клетки квадрата будут заполнены. Правило выбора прорезей гарантирует, что при заполнении квадрата буква на букву никогда не попадет. Из заполненного квадрата буквы можно выписать по столбцам, выбрав подходящий пароль. Например, с использованием изображенной выше решетки и пароля ш и ф р открытый текст *договор подписали* переводится в криптограмму за пять шагов:

–	–	–	д
–	–	–	–
–	о	–	г
–	–	о	–

–	–	–	д
–	в	–	–
о	о	–	г
–	р	о	п

–	о	–	д
а	в	п	–
о	о	–	г
и	р	о	п

с	о	а	д
д	в	п	л
о	о	и	г
и	р	о	п
ш	*и*	*ф*	*р*

Итоговая криптограмма: ОВОРДЛГПАПИОСДОИ.

Сконструируйте решетку с $k = 3$ и зашифруйте с ее помощью одно из практических указаний для криптографов: *не шифруй один и тот же текст разными ключам(и).* Последнюю, легко восстановимую, букву *и* для удобства отбросим.

Шифрование с помощью решеток в первой половине 1917 года германская армия использовала на Восточном (против России) фронте. В

1982 году его применяли британские войска в вооруженном конфликте с Аргентиной за Фолклендские острова.

Тема 3. *ПОДСТАНОВОЧНЫЕ ШИФРЫ (ШИФРЫ ЗАМЕНЫ).*

Класс *шифров замены* выделяется тем свойством, что для получения криптограммы отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита. В *шифре простой замены* происходит замена буквы на букву, т.е. устанавливается попарное соответствие символов исходного алфавита с символами шифроалфавита. Например, в рассказе Эдгара По «Золотой жук» пиратский капитан Кидд в своей шифровке вместо букв *a, b, c, d, e, f, g, h, i* писал соответственно 5, 2, -, +, 8, 1, 3, 4, 6, 0, 9. В «Пляшущих человечках» Артура Конан-Дойла бандит Слени использовал шифр, где буквы заменялись схематическими человеческими фигурками в разных позах.

В практической криптографии при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит с измененным порядком букв (*алфавитная перестановка*). Чтобы запомнить новый порядок букв, перемешивание алфавита осуществляют с помощью *пароля* – слова или нескольких слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк. В первой записывается стандартный алфавит открытого текста, во второй же строке, начиная с некоторой позиции, размещается пароль (без пробелов, если они есть), а после его окончания перечисляются в обычном алфавитном порядке буквы, в пароль не вошедшие. Если начало пароля не совпадает с началом строки, процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим место начальной буквы пароля. Например, таблица шифрования на ключе 7 п о л я р н и к имеет вид

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

При шифровании каждая буква открытого текста заменяется на стоящую под ней букву. В рассматриваемом примере указание *никогда не рассекречивай открытый текст в его истинной формулировке* можно представить в виде криптограммы КЛРАЬ ЭЩКЮВ ЩГГЮР ВЮМЛЫ ЩЯАДР ВФДФЯ ДЮРГД ЫЮЬАЛ ГДЛКК АЯЖАВ ИЕНЛВ АЫРЮУ. Здесь, как это часто делается, текст разбит на пятибуквенные блоки, в конце, для завершенности, добавлена незначащая буква.

Криптоанализ шифров простой замены осуществляется с помощью частотных характеристик языка открытых текстов. Известно, что в русском тексте длиной 10 000 знаков буква О встречается в среднем 1047 раз, Е – 836, А – 808, Н – 723, И – 700, Т – 625, Р – 584, В – 569, С – 466. Поэтому, если в достаточно длинной криптограмме какая-то буква оказывается безусловным лидером по числу вхождений, есть основание предполагать, что она заменяет О. Блестящим примером частотного криптоанализа являются рассуждения Леграна, героя рассказа «Золотой жук», прочитавшего шифрованное указание о месте сокрытия пиратского клада, и выводы (в подлиннике) Шерлока Холмса в Деле Пляшущих Человечков. Заметим, что в английских текстах самыми частыми являются (в порядке убывания) буквы *e*, *t*, *a*, *o*, *i*, *n*, *s*, *r*.

Для увеличения стойкости подстановочных шифров используют различные методы, скрывающие частотные соотношения языка. Рассмотрим несколько известных приемов. Шифры названы историческими именами использовавших их агентов.

а) Шифр «Дора».

	1	2	3	4	5	6	7	8	9
4, 5, 6, 7, 8, 9	*a*	*s*	*i*	*n*	*t*	*o*	*e*	*r*	
2, 3	b	c	d	f	g	h	j	k	l
1	m	p	q	u	v	w	x	y	z

Во второй строке таблицы записаны самые частые английские буквы (65% всех букв в текстах) в виде мнемонической (для запоминания) фразы *a sin to er(r)* – «грех ошибаться». Далее оставшиеся буквы перечисляются в

алфавитном порядке с пропуском букв из второй строки. Заметим, что, за счет только изменения порядка букв во второй строке, можно получить 40320 различных таблиц. Шифрование производится заменой каждой буквы на двузначное число, составленное из номера строки и номера столбца, где находится эта буква. При этом буква может выступать в криптограмме в нескольких вариантах. Например, 41, 51, 61, 71, 81, 91 – образы одной и той же буквы *а*. Понятно, что, глядя на криптограмму, невозможно установить, как же в ней «спрятана» та или иная из самых частых букв.

Расшифруйте послание 52707 94231 01468 44718 45562 26629 96685 12376 (фантомная цифра 0 вставлена для усложнения работы криптоаналитика).

б) Шифр «Марк».

	1	2	3	4	5	6	7	8	9	0
	с	*е*	*н*	*о*	*в*	*а*	*л*			
8	б	г	д	ж	з	и	й	к	м	п
9	р	т	у	ф	х	ц	ч	ш	щ	ъ
0	ы	ь	э	ю	я	·	/			

Буквы, стоящие во второй строке таблицы (они дают 45% букв в русских текстах), при шифровании заменяются стоящими над ними цифрами, остальные буквы – двузначными числами «строка-столбец». Косая черта – знак начала и окончания числового массива в открытом тексте (цифры при шифровании сохраняются).

Прочтите криптограмму 07607 89605 19380 91938 28650 12956 78689 28818 68893.

Зашифруйте текст *к встрече готовы*.

в) Шифр «Рамзай».

Проанализируйте метод, по которому составлена следующая шифровальная таблица с паролем *subway* –«метро».

s	*u*	*b*	*w*	*a*	*y*
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	·	/		
81	86	90	94		

На бланке расшифрованной радиограммы 9154873951708482739422 94 красным карандашом Сталин подчеркнул указанную в ней дату.

г) Шифр «Жанна».

Английский алфавит записан в таблицу 5×5 с паролем в данном примере *eighty four* – «84» (буква *j* в открытых текстах всюду заменялась на *i*). Открытый текст разбивается на блоки длины 4.

e	*i*	*g*	*h*	*t*
y	*f*	*o*	*u*	*r*
a	b	c	d	k
l	m	n	p	q
s	v	w	x	z

Первая буква каждого блока заменяется на своего верхнего соседа в таблице («север»), вторая – на правого («восток»), третья – на нижнего («юг»), четвертая – на левого («запад»).

Догадайтесь, как быть, если указанного соседа у буквы нет. Прочтите следующее сообщение о невыходе на связь: FIWVVM SASVFQ SPRMSZ RLGPRG.

Зашифруйте запрос *restate your questions*.

Тема 4. *БЛОЧНЫЕ ШИФРЫ.*

В самом общем виде идеология блочного шифрования выглядит так: открытый текст разбивается на блоки различной длины, каждый блок шифруется по особому методу, полученные блоки криптограммы после некоторой перестановки «сшиваются» в единый массив. На практике же все блоки открытого текста имеют одинаковую длину, все шифруются по одному и тому же способу и преобразуются в той же длины блоки криптограммы, которые последовательно выстраиваются в порядке соответствующих исходных блоков.

а) Шифр Уитстона-Плейфера.

Исторически первым блочным шифром был шифр, разработанный английским физиком и криптографом Чарлзом Уитстоном (1802-1875) и представленный лордом Плейфером министру иностранных дел

Великобритании Палмерстону в 1854 году. Английский алфавит (с $j=i$) обычным приемом парольного перемешивания вписывается в таблицу 5×5.

p	*a*	*l*	*m*	*e*
r	*s*	*t*	*o*	*n*
b	c	d	f	g
h	i	k	q	u
v	w	x	y	z

Открытый текст разбивается на блоки длины 2. Если обе буквы блока стоят в одной строке (в одном столбце) таблицы, они заменяются их правыми (нижними) соседями. Если же буквы блока стоят в разных строчках и разных столбцах, то каждая из них заменяется на букву, стоящую в той же строке, но в столбце другой буквы блока. Примеры соответствий: cf→DG, wz→XV, oq→FY, ez→NE, su→NI. Если в тексте рядом стоят две одинаковые буквы, между ними вставляется x, так что *lesson for miss Dolly* предстанет в виде *lesxson for misxs Dolxly*.

Шифр Уитстона-Плейфера использовался в ходе Первой мировой войны британской дипломатией, а во Второй мировой войне – в соединениях германской армии на Западном фронте (и его читали союзники).

б) Шифр Виженера.

Французский криптограф Блез Виженер (1523-1596) опубликовал свой метод в «Трактате о шифрах» в 1585 году. С тех пор на протяжении трех столетий шифр Виженера считался нераскрываемым, пока с ним не справился австриец Фридрих Казиски (в 1863 году). При этом способе шифрования открытый текст разбивается на блоки некоторой длины n. Задается ключ – последовательность из n натуральных чисел: $a_1, a_2,\ldots,a_n$. Затем в каждом блоке первая буква циклически сдвигается вправо по алфавиту на a_1 позиций, вторая буква – на a_2 позиций, …, последняя – на a_n шагов.

Зная ключ (25, 9, 21, 17), расшифруйте криптограмму ЭОАЯКНЪЬЩЦГ.

На ключе (13, 5, 9) зашифруйте донесение *приезжает завтра.*

Для лучшего запоминания, в качестве ключа обычно берут осмысленное слово, и алфавитные номера составляющих его букв используют для вычислений, связанных со сдвигами. Так, указанный в приведенном примере ключ имеет буквенную форму ш и ф р (в русском алфавите ш –двадцать пятая буква, и – девятая, ф – двадцать первая, р – семнадцатая). Для дальнейшего нам понадобится знать номера всех букв русского алфавита:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

и латинского:

1	2	3	4	5	6	7	8	9	10	11	12	13
a	b	c	d	e	f	g	h	i	j	k	l	m
14	15	16	17	18	19	20	21	22	23	24	25	26
n	o	p	q	r	s	t	u	v	w	x	y	z

Из-за нехватки опытных шифровальщиков шифр Виженера с длиной блока, равной всего лишь 3, применялся в низовых звеньях русской армии в 1916 году, во время наступления Юго-Западного фронта против австро-венгерской армии – знаменитого брусиловского прорыва. Противник легко читал русские оперативные шифровки, что, в конце концов, и не позволило генералу Брусилову добиться стратегического успеха в блестяще задуманной операции.

в) Шифр Цезаря.

Очень частный случай конструкции Виженера использовал римский полководец Юлий Цезарь: он каждую букву открытого текста циклически сдвигал на три позиции вправо. Знаменитая фраза «Пришел, увидел, победил», подводившая итог битвы при Зеле в августе 47 года до н.э., в шифрованном письме Цезаря выглядела как ZHQM ZMGM ZMFM.

Восстановите исходный текст (учтите, что во времена Цезаря в латинском алфавите еще не было букв *j, u, w*).

Тема 5. *МОДУЛЬНАЯ АРИФМЕТИКА.*

Пусть m – некоторое натуральное число. Не все натуральные числа делятся на m. Возможными остатками от деления являются 1, 2, …, m – 1, 0 (последний при делении нацело). По модулю m каждое натуральное число воспринимается как остаток от деления этого числа на m: $25_{\text{mod } 3}=1$, $9_{\text{mod } 7}=2$, $100_{\text{mod } 26}=22$, $100_{\text{mod } 32}=4$ и т.п. Два числа a и b называются *сравнимыми по модулю m*, если при делении на m они дают одинаковые остатки, т.е. если $a_{\text{mod } m}=b_{\text{mod } m}$. В этом случае пишут $a \equiv b \pmod m$ («a сравнимо с b по модулю m»). Так, например, $5 \equiv 11 \pmod 3$, $25 \equiv 0 \pmod 5$, $48 \equiv 6 \pmod 7$.

На множестве чисел 1, 2, …, m – 1, 0 вводится *сложение по модулю m*: в качестве результата берется остаток от деления обычной суммы слагаемых на модуль m, т.е. $a +_m b = (a+b)_{\text{mod } m}$. Например, при сложении по модулю 2 получаем $0 +_2 0 = 1 +_2 1 = 0$ и $0 +_2 1 = 1 +_2 0 = 1$. Составим таблицу сложения по модулю 3:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Как видим, $2 +_3 2 = (2+2)_{\text{mod } 3} = 4_{\text{mod } 3} = 1$.

При вычитании по модулю m для соответствующих чисел осуществляют обычное вычитание и, если в результате получится отрицательное число, к нему прибавляют m. Например, по модулю 5 имеем: $1 -_5 4 = -3_{\text{mod } 5} = 2$.

По модулю 32 вычислите разности 10-23, 3-31, 26-31. По модулю 26 найдите 2-17, 20-25, 15-19.

Если некоторый алфавит имеет мощность m (т.е. в нем m букв), то сложение и вычитание по модулю m можно истолковывать как сложение и вычитание букв с соответствующими номерами. Так, при m=32 (русский алфавит) имеем: Й-Ц=$10 -_{32} 23 = -13_{\text{mod}32}=19$=Т, Т+Т=$19 +_{32} 19 = 38_{\text{mod}32}=6$=Е и т.п.

При таком истолковании модульных операций сложения и вычитания, шифрование по Виженеру – это сложение блока открытого текста с ключом

по модулю мощности алфавита. Например, зашифруем открытый текст *шифр Виженера* на ключе з а д а ч а. Длина блоков (и ключа) равна 6. Текст разбивается на два блока: (шифрви)(женера), каждый из которых побуквенно складывается с ключом: (шифрви)+(задача)=(25,9,21,17,3,9)$+_{32}$(8,1,5,1,24,1) = = (33,10,26,18,27,10)$_{mod32}$=(1,10,26,18,27,10) = АЙЩСЪЙ, (женера)+(задача)=(7,6,14,6,17,1)$+_{32}$(8,1,5,1,24,1)=(15,7,19,7,9,2)=ОЖТЖИБ. Итоговая криптограмма: АЙЩСЪЙОЖТЖИБ.

При дешифровании из блока криптограммы побуквенно вычитается ключ. Так, зная, что криптограмма LAGZJEUUXRTJE получена на ключе Виженера p r o b l e m («задача»), легко восстанавливаем открытый текст. Сначала из первого блока криптограммы побуквенно вычитаем ключ: LAVGZJE – PROBLEM = (12,1,22,7,26,10,5) $-_{26}$ (16,18,15,2,12,5,13) = (-4, -17,7,5,14,5,-8)$_{mod26}$ = (22,9,7,5,14,5,18) = vigener, затем ключ побуквенно вычитается из второго блока криптограммы:

UUXRTJE-PROBLEM=(21,21,24,18,20,10,5)-$_{26}$(16,18,15,2,12,5,13) = =(5,3,9,16,8,5,-8)$_{mod26}$=(5,3,9,16,8,5,18)=ecipher. Открытый текст: Vigenere cipher (шифр Виженера).

В дальнейшем понадобится и *умножение по модулю m*: оно выполняется аналогично сложению – в качестве результата берется остаток от деления на *m* обычного произведения сомножителей. Например, для умножения по модулю 4 получаем следующую таблицу:

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Отметим необычное равенство $2\times_4 2=0$, оба сомножителя отличны от нуля, а их произведение равно нулю.

Составьте таблицы сложения и умножения по модулям 5 и 6. По модулю 6 для каждого из чисел 1, 2, 3, 4, 5, 0 укажите противоположное. Например, $-2_{mod\ 6}=4$.

Тема 6. *ПОТОЧНЫЕ ШИФРЫ.*

В шифре Виженера длина ключа может оказаться равной длине открытого текста. Шифры, обладающие этим свойством, называют *поточными*. Можно представить себе, что имеются два синхронизированных потока: буква за буквой поступающий открытый текст и параллельный с ним ключевой поток над тем же алфавитом. Шифрование осуществляется методом Виженера – путем побуквенного сложения этих двух потоков по модулю алфавитной мощности. Рассмотрим наиболее известные поточные шифры.

а) Книжный шифр.

В качестве ключа выбирается какая-либо книга с идентификатором некоторого стартового места в тексте (например, «третья буква в пятом абзаце второй главы»). Под открытым текстом подписывается текст книги, начиная с ключевого места. В следующем примере для удобства выставлены номера участвующих букв.

18	13	6	14	9	19	6	25	9	21	17	14	1	18	24	9	19	1	31	19
с	*м*	*е*	*н*	*и*	*т*	*е*	*щ*	*и*	*ф*	*р*	*н*	*а*	*с*	*ч*	*и*	*т*	*а*	*ю*	*т*
у	л	у	к	о	м	о	р	ь	я	д	у	б	з	е	л	е	н	ы	й
20	12	20	11	15	13	15	17	29	0	5	20	2	8	6	12	6	14	28	10
6	25	26	25	24	0	21	10	6	21	22	2	3	26	30	21	25	15	27	29
Е	Ш	Щ	Ш	Ч	Я	Ф	Й	Е	Ф	Х	Б	В	Щ	Э	Ф	Ш	О	Ъ	Ь

Во второй строке таблицы записан открытый текст, в третьей – ключ (А.С. Пушкин «Руслан и Людмила», Песнь Первая, с первой буквы), в шестой – криптограмма. В первой строке стоят номера букв открытого текста, в четвертой – номера букв ключа, в пятой – сумма по модулю 32 соответствующих букв открытого текста и ключа, т.е. номер получившейся буквы криптограммы.

б) Шифры с автоключами.

Первая буква ключа выбирается случайно, а далее он состоит из открытого текста:

Открытый текст:	*с*	*м*	*е*	*н*	*и*	*т*	*е*	*ш*	*и*	*ф*	*р*
Ключ:	к	с	м	е	н	и	т	е	ш	и	ф
Криптограмма:	Ь	Ю	Т	У	Ц	Ы	Ш	Ю	Б	Э	Е

или из получающейся буква за буквой криптограммы:

Открытый текст:	*с*	*м*	*е*	*н*	*и*	*т*	*е*	*ш*	*и*	*ф*	*р*
Ключ:	к	ь	й	п	э	ж	щ	я	ш	б	ц
Криптограмма:	Ь	Й	П	Э	Ж	Щ	Я	Ш	Б	Ц	З

Эти способы генерации ключевого потока предложил в своем упоминавшемся трактате Виженер.

в) Шифр Вернама.

В 1917 году американский инженер Гилберт Вернам (1890-1960) осуществил казалось бы несбыточную мечту криптографов: он предложил шифр, в принципе не раскрываемый. Это поточный шифр над двоичным алфавитом с буквами 0 и 1. Открытый текст представляется в двоичном виде (например, согласно телеграфному коду Бодо, где каждая буква заменяется двоичной последовательностью длины 5), ключом является случайная двоичная последовательность той же длины, которая используется только один раз – для шифрования данного текста. Криптограмма получается посимвольным сложением открытого текста и ключа по модулю 2. Заметим, что поскольку по модулю 2 вычитание совпадает со сложением, для дешифрования криптограмма посимвольно складывается с ключом.

Пусть, например, открытым текстом является *w h i t e* (белый). В кодовой таблице Бодо находим: *e* – 00001, *h* – 10100, *i* – 00110, *t* – 10000, *w* – 10011, так что шифроваться будет двоичная последовательность (длины 25) 1001110100001101000000001. В качестве ключа возьмем двоичную запись цифр после запятой в числе π=3,1415926536… .Для двоичного представления любого числа от 0 до 15 достаточно четырех цифр: 0 – 0000, 1 – 0001, 2 – 0010, 3 – 0011, 4 – 0100, 5 – 0101, 6 – 0110, 7 – 0111, 8 – 1000, 9 – 1001, …, 15 – 1111. Выбирая первые 25 двоичных знаков, кодирующих последовательность 1415926, находим ключ: 0001010000010101100100100.

Для получения криптограммы посимвольно складываем по модулю 2 двоичные коды открытого текста и ключа:

	1	0	0	1	1	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1
$+_2$																								
	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	1	1	0	0	1	0	0	1	0	0
=	1	0	0	0	1	0	0	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	1	0	1

(Обратим внимание на то, что при суммировании (снизу вверх) криптограммы и ключа в самом деле получается открытый текст).

Почему же шифр Вернама не раскрываем? Дело в том, что, если известна криптограмма, и ее длина равна *n* двоичных разрядов (битов), то, перебирая все возможные ключи (т.е. все возможные двоичные последовательности длины *n* битов) и складывая их посимвольно по модулю 2 с криптограммой, можно получить все возможные двоичные тексты длины *n* битов. Какой из них был подлинным сообщением, установить невозможно. Так, в рассмотренном примере, зная криптограмму 1000100100011000100100101 и не зная ключа, взломщик шифра попробует испытать все 2^{25}=33 554 432 возможных ключей, т.е. двоичных последовательностей длины 25 битов. На каком-то шаге он наткнется на истинный ключ и получит, складывая с ним криптограмму, *w h i t e*. Не зная, в самом ли деле это подлинный открытый текст, он в процессе дальнейшего перебора дойдет до ключа 0100010110011110011101010 и, сложив его по Виженеру с криптограммой, получит 1100110010000110111001111, что по таблице Бодо дает *b l a c k* (черный). Далее ему попадется в качестве возможного ключа последовательность 0101101110011010100001001 и в качестве возможного открытого текста он увидит 1101001010000010000101100 – *g r e e n* (зеленый).

Найдите ключ, при дешифровании на котором рассматриваемая криптограмма даст открытый текст *b r o w n* (коричневый) (у Бодо буква *O* кодируется как 11000).

32 буквы русского алфавита (без ё) закодированы пятибитовыми векторами: *а* – 00001, *б* – 00010, *в* - 00011, …, *ю* – 11111, *я* – 00000. Проверьте, что при подходящем подборе ключа любая буква может быть зашифрована как *Я*.

Абсолютно стойкий шифр Вернама, к сожалению, мало пригоден для повседневной практики: ведь с каждым открытым текстом нужно связать индивидуальную случайную двоичную последовательность той же длины. Где взять столько случайных двоичных последовательностей? Современные компьютеры генерировать их не способны. Поэтому шифр Вернама применяется только в особо важных случаях. Например, он служит для обмена секретной информацией между руководителями Российской Федерации и США.

Заметим, что тому, кто не имеет возможности использовать шифр Вернама, вполне доступны другие приемы надежной криптографической защиты информации. Последовательное применение трех разных шифров – один из них.

Раздел II. СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ КРИПТОГРАФИЯ

Тема 7. *ШИФРЫ DES И ГОСТ 28147-89.*

Рассматриваемые в этом разделе шифры заслуживают особого внимания. Алгоритм DES с 1977 года был стандартом шифрования в США. И хотя в 2001 году он утратил свой государственный статус, его значение для теоретической и прикладной криптографии невозможно переоценить и потому этот метод шифрования во всех деталях изучается профессионалами. Похожий на него шифр ГОСТ 28147-89 интересен в первую очередь тем, что на протяжении многих лет является действующим стандартом шифрования в Российской Федерации.

а) DES.

В начале 1970-х годов правительство США под давлением промышленных и финансовых кругов согласилось официально допустить использование криптографических методов для защиты конфиденциальных данных от несанкционированного доступа. Национальное бюро стандартов объявило открытый конкурс на создание общедоступного алгоритма шифрования с гарантированной надежностью. Оценку представленных кандидатов осуществляло Агентство национальной безопасности США. В январе 1977 года предложенный фирмой IBM и оказавшийся победителем конкурса, «Алгоритм шифрования для защиты данных ЭВМ» был зарегистрирован в качестве государственного стандарта США: Data Encryption Standard (Стандарт шифрования данных, DES).

Создание шифра DES (главным идеологом проекта был Хорст Фейстель) явилось выдающимся научно-техническим достижением, оказавшим глубокое влияние на дальнейшее развитие криптографии и на ее использование в интересах широких деловых кругов.

Алгоритм DES является блочным шифрованием. Открытый текст, представленный в двоичном виде, разбивается на блоки длины 64 бита,

которые переводятся в такой же длины блоки криптограммы с помощью чередования перестановочных и подстановочных шифров.

Входной блок подвергается начальной перестановке, и ее результат разбивается на два 32-разрядных блока L_0 и R_0. После этого следуют 16 раундов шифрования с использованием секретного ключа *K*. Над финальным блоком $L_{16}R_{16}$ осуществляется перестановка, обратная по отношению к начальной, и результат выдается в качестве блока криптограммы.

При дешифровании все действия производятся в обратном порядке.

Центральной операцией алгоритма DES, обеспечивающей стойкость шифра, является подстановка с использованием шифраторов, так называемых *S-боксов* (*substitution boxes*). *S*-бокс представляет собой таблицу размерности 4×6 с нумерацией строк 0, 1, 2, 3 и столбцов от 0 до 15. В каждой строке стоит своя перестановка столбцовых номеров. На вход *S*-бокса подается 6-разрядный двоичный блок $a_0a_1a_2a_3a_4a_5$. Первый и последний его символы a_0a_5 определяют строку *S*-бокса, средние $a_1a_2a_3a_4$ – его столбец. Стоящее на пересечении строки и столбца число дает в двоичной записи 4-разрядный выходной блок. Переработка 6-буквенных двоичных блоков в 4-буквенные и является функцией *S*-бокса. В качестве примера покажем, как это делает *S*-бокс 5:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Пусть на вход подается двоичное слово 111010. Оно выделяет в таблице строку с номером 2 (т.е. 10) и столбец с номером 13 (т.е. 1101). На их пересечении стоит число 3. Его двоичная запись 0011 и появляется на выходе.

В какое четырехбитовое двоичное слово бокс S_5 переведет шестибитовое слово 100100? слово 100101?

Найдите все 6-битовые двоичные слова, которые S_5 заменит на 0000, на 1111.

Все используемые в DES перестановки и подстановки известны. Неизвестен только секретный 56-разрядный ключ *K*, принадлежащий

пользователю. Таким образом, в DES реализован идеал Керкхофса: о шифре известно все, кроме ключа. Для прямого взлома DES нужно перебрать 2^{56}=72 057 594 037 927 936 (72 квадриллиона 57 триллионов 594 миллиарда 37 миллионов 927 тысяч 936) возможных ключей.

DES стал наиболее широко признанным механизмом криптографической защиты данных, не составляющих государственной тайны.

При регистрации DES в качестве государственного стандарта США рекомендовалось пересматривать его на предмет стойкости каждые пять лет. Последние испытания были проведены в 1997 году, и шифр в очередной раз был признан надежным. В июле 1998 года, затратив более 250 000 долларов, компания EFF (Electronic Frontier Foundation, Фонд электронного рубежа) предъявила суперкомпьютер «DES-взломщик», изготовленный с использованием 1536 чипов, обеспечивавших проверку 28 миллиардов ключей в секунду. С его помощью контрольная DES-криптограмма была дешифрована за 56 часов. В январе 1999 года, присоединив еще 100 000 объединенных в сеть персональных компьютеров, EFF справилась с этой задачей уже за 22 часа, – DES был окончательно скомпрометирован.

В январе 2000 года правительство США признало алгоритм DES ненадежным. Но еще в 1997 году оно объявило открытый международный конкурс на AES (Advanced Encryption Standard, Усовершенствованный стандарт шифрования). Причиной было не столько сомнение в надежности DES (применявшееся в практике трехкратное шифрование 3DES с количеством возможных ключей 2^{112} неприступно для взлома), сколько выявившиеся в процессе эксплуатации его неудобства и не полная приспособленность к новым запросам. В октябре 1999 года победителем конкурса был объявлен шифр Рейндал (Rijndael), который предложили бельгийские криптографы Йон Дамен и Винцент Реймен, использовавшие в своей разработке высшие разделы модульной алгебры. С апреля 2001 года Рейндал стал новым стандартом шифрования в США.

AES – блочный шифр, который работает с блоками длиной 128 битов и использует ключи длиной 128, 192 и 256 битов (один и тот же ключ применяется и при шифровании и при дешифровании). Алгоритм производит операции над двумерными массивами байтов. Количество раундов для ключей длиной 128, 192 и 256 битов соответственно равно 10, 12 и 14. Программная реализация алгоритма на компьютере с частотой 2 ГГц шифрует данные со скоростью 700 Мбит/с. При использовании 128-битового ключа для прямого взлома шифра потребуется примерно 149 триллионов лет. Ключ длиной 128 битов рекомендован для закрытия секретной информации, ключи большей длины защищают информацию с грифом «совершенно секретно» («top secret»).

б) ГОСТ 28147-89.

Алгоритм, о котором пойдет речь, был разработан в конце 1970-х годов группой советских криптографов во главе с И.А.Заботиным и первоначально предназначался для защиты совершенно секретной информации. В последующие годы гриф секретности снижался и, вскоре после регистрации в качестве государственного стандарта в 1989 году (ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»), шифр, будем называть его для краткости ГОСТ, стал общедоступным.

ГОСТ является блочным шифром. Исходный двоичный текст разбивается на блоки длиной 64 бита. Первые 32 бита (младшие) шифруемого блока заносятся в регистр N_1, оставшиеся 32 бита (старшие) – в регистр N_2. После этого осуществляются 32 *основных шага* шифрования с помощью секретного ключа K. Ключ K имеет длину 256. Он разбивается на 8 последовательно идущих 32-разрядных подключей K_0, K_1,…, K_7. Эти *шаговые ключи* размещаются в ключевом запоминающем устройстве (КЗУ). Для обслуживания 32 основных шифрошагов ключи (по одному на каждый шаг) три раза подаются в прямой последовательности K_0 K_1, …, K_7 и один раз – в обратной K_7, K_6, …, K_0.

Основной шаг шифрования состоит в следующем:

1) производится сложение по модулю 2^{32} содержимого регистра N_1 с очередным шаговым ключом из КЗУ;

2) 32-разрядный результат сложения X разбивается на 8 последовательно идущих 4-разрядных блоков X_0, X_1, … , X_7, каждый из которых преобразуется в новый 4-разрядный блок по таблице замены S, после чего выходные блоки последовательно объединяются в один 32-разрядный блок;

3) полученный блок циклически сдвигается на 11 позиций в сторону старших разрядов (влево);

4) результат сдвига поразрядно складывается по модулю 2 с содержимым регистра N_2;

5) полученная сумма заносится в регистр N_1, содержимое которого одновременно перемещается в регистр N_2. На последнем, 32-м, шаге сумма заносится в регистр N_2, а содержимое регистра N_1 сохраняется.

После 32 шагов работы алгоритма содержимое регистров N_1 и N_2 объединяется в единый 64-разрядный блок криптограммы, соответствующий исходному блоку открытого текста.

Одним из основных моментов, обеспечивающих стойкость шифра, наряду с длиной ключа K, является подстановочный шифратор – *таблица замены* S, состоящая из 8 строк и 16 столбцов. Строки S_0, S_1, … , S_7 таблицы называются *узлами замены* и каждая из них представляет собой некоторую перестановку чисел от 0 до 15. Упомянутые 4-разрядные блоки X_0, X_1, …, , X_7 поступают каждый на вход своего узла замены, соответственно S_0, S_1,…, S_7. Блок X_i рассматривается как двоичная запись некоторого целого числа от 0 до 15. Это число определяет конкретное место в узле замены (строке) S_i соответствующем X_i. Стоящее на этом месте число, в 4-разрядной двоичной записи, подается на выход шифратора S.

Например, пусть блок X_5=1001 поступает на вход таблицы замены S.

Она отправит его в узел замены S_5:

4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14

В двоичной записи 1001 – это число 9. На девятом месте (счет начинается с 0) в строке S_5 стоит число 6. Его двоичная 4-разрядная запись 0110 идет на выход таблицы замены.

Определите, какой входной блок будет заменен узлом S_5 на 1001, на 1111.

Заметим, что, в отличие от DES, где все *S*-боксы представлены в явном виде, узлы замены в документации алгоритма ГОСТ не описаны, и приводимые в разных публикациях их примеры восходят к неофициальным данным.

После введения в США стандарта шифрования AES естественно возник вопрос о дальнейшей судьбе шифра ГОСТ. Предпринятые с этой целью исследования показали, что удобства в эксплуатации, криптостойкость и эффективность алгоритмов ГОСТ и AES вполне сопоставимы.

19 июня 2015 года приказом Росстандарта (Федеральное агентство по техническому регулированию и метрологии) № 749-ст был утвержден новый стандарт шифрования ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» с датой вступления в действие 1 января 2016 года. В нем представлены два блочных шифра. Один из них – это ГОСТ 28147-89 с модификацией, которая состоит в том, что узлы замены задаются в фиксированном виде, позволяя исключить случайный или намеренный их выбор, приводящий к снижению стойкости алгоритма. Улучшенный таким образом ГОСТ в составе нового стандарта именуется – *Магма*. Второй шифр, называемый *Кузнечик*, имеет длину входного блока 128 битов и длину ключа 256 битов. Этот шифр разработан Центром защиты информации и специальной связи ФСБ России при участии ОАО «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Необходимость разработки нового алгоритма шифрования объясняется потребностью в использовании блочных шифров с входными блоками

различной длины для обеспечения современных требований к криптографической стойкости и эксплуатационным качествам. Шифры стандарта не накладывают ограничений на степень секретности защищаемой информации.

Тема 8. *КРИПТОСИСТЕМА RSA.*

В июне 2003 года в Сан-Диего, Калифорния, состоялось очередное вручение Тьюринговской премии, учрежденной Ассоциацией вычислительной техники (Association for Computing Machinery). Эта премия названа именем Алана Тьюринга (1912-1954), английского математика, заложившего основы компьютерных наук и внесшего решающий вклад в раскрытие германского шифра «Энигма» в годы Второй мировой войны. Она присуждается с 1966 года специалистам в области компьютерных наук, создавшим теоретические и технические предпосылки для новых, этапных, достижений в области информационных технологий. Лауреатами 2002 года стали Рональд Ривест, Ади Шамир и Леонард Адлмен. В 1977-78 годах, работая в Массачусетском технологическом институте, они создали шифр, названный RSA (по первым буквам фамилий), который произвел переворот в криптографии и открыл новый период в сфере защиты информации. В настоящее время RSA – самый распространенный метод шифрования, используемый в компьютерных сетях. В этом шифре осуществлена другая казавшаяся несбыточной мечта криптографов: возможность защищенной связи без передачи секретного ключа.

После некоторых необходимых предварительных сведений дадим краткое описание шифра RSA.

Напомним, что натуральное число, большее 1, называется простым, если оно делится только на 1 и на себя. Первые десять простых чисел:2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Простых чисел бесконечно много, они распределены по натуральному ряду вне какой-либо известной закономерности. Числа, не являющиеся простыми, называются составными.

Всякое составное число единственным образом можно представить в виде произведения степеней простых чисел. Например, $12=2^2\cdot3$, $45=3^2\cdot5$, $105=3\cdot5\cdot7$ и т.д. Существующие алгоритмы позволяют персональному компьютеру за несколько секунд проверить, является ли простым предъявленное число, имеющее порядка 180 цифр (уровень современной практической криптографии). В то же время задача разложения на множители столь же больших составных чисел лежит далеко за пределами современных технологических возможностей.

Два натуральных числа a и b называются взаимно простыми, если у них нет общих делителей, т.е. таких натуральных чисел, на которые делились бы и a, и b. Так, $50=2\cdot5^2$ и $63=3^2\cdot7$ являются взаимно простыми числами, а $36=2^2\cdot3^2$ и $105=3\cdot5\cdot7$ – нет: у них имеется общий делитель 3.

Теперь о шифре. Пусть имеется компьютерная сеть, абоненты которой хотят обмениваться информацией, не предназначенной для непредусмотренных пользователей. Абонент А выбирает два больших (примерно по 100 цифр) простых числа p и q, находит их произведение $n=pq$ и подбирает целое число e в интервале от 2 до $(p-1)(q-1)$, взаимно простое с $p-1$ и с $q-1$. Затем он опубликовывает пару (n,e), это его *открытый ключ*, он применяется для шифрования сообщений.

Предположим, что другой абонент В желает отправить для А секретное сообщение. Он переводит открытый текст в числовую форму m (например, заменяя a на 01, b – на 02, … , z – на 26, а пробел между словами – на 00). Если полученное число m превышает n, его можно разбить на последовательные части, каждая меньше n, так что для простоты пусть $m < n$. Далее В вычисляет $c=(m^e)_{\mathrm{mod}\ n}$. Это криптограмма, которую он и посылает абоненту А. Для того чтобы ее прочитать, А уже заготовил свой *закрытый ключ* – число d, удовлетворяющее двум требованиям: $1< d < n$ и $ed\equiv1\ (\mathrm{mod}\ (p-1)(q-1))$. Из теории известно, что такое число существует и притом только одно. Теперь А вычисляет $(c^d)_{\mathrm{mod}\ n}$ и (математическая теорема) получает m.

Возьмем для примера p=3, q=11. Тогда $n=pq=3\cdot11=33$, $(p-1)(q-1)=2\cdot10=20$. Выберем e=7. Открытым ключом является пара чисел (33,7). Теперь нужно «изготовить» закрытый ключ (ключ расшифрования), т.е. найти число d такое, что $ed\equiv1 \pmod{20}$. Очевидно, что d=3, так как $7\cdot3=21_{\text{mod }20}=1$. Предположим, что m=2. Тогда $c=(m^e)_{\text{mod }n}=2^7{}_{\text{mod}33}=128_{\text{mod}33}=29$. Итак, криптограммой сообщения m=2 является c=29. Дешифрование:
$(c^d)_{\text{mod }n}=(29^3)_{\text{mod }33}=(-4)^3{}_{\text{mod }33}=(-64)_{\text{mod }33}=(-31)_{\text{mod }33}=2=m$.

При p=3, q=11, e=7 зашифруйте сообщение m=3, сообщение m=4.

В условиях предыдущей задачи расшифруйте криптограмму c=5.

Стойкость шифра RSA обосновывается следующими соображениями. Для того чтобы прочитать криптограмму c, нужно знать закрытый ключ d. Поскольку числа e и $n=pq$ известны, для нахождения d достаточно найти произведение $(p-1)(q-1)$, так как $ed\equiv1 \pmod{(p-1)(q-1)}$, Таким образом, все сводится к определению множителей p и q числа n. Как уже было отмечено выше, задача разложения на множители для больших составных чисел в настоящее время вычислительно не разрешима.

Все шифры, которые рассматривались до настоящего раздела, обладают тем свойством, что для шифрования и дешифрования в них применяется один и тот же секретный ключ. Поэтому такие шифры называют *симметричными*. Шифр RSA этим свойством не обладает, процедуры шифрование и дешифрование в нем осуществляются на разных ключах. Подобные шифры называются *асимметричными*.

Для коротких сообщений шифр RSA почти идеален, но при передаче информации большого объема он сильно уступает по скорости симметричным алгоритмам шифрования. Так, самые быстрые микросхемы для RSA имеют пропускную способность около 65 Кбит/с, в то время, как скорость реализации, например AES, достигает 70 Мбит/с. Поэтому в коммуникационных сетях с большой нагрузкой рекомендуется применять RSA вместе с AES (по протоколу «цифровой конверт»): абонент А, желая установить защищенную связь с абонентом В, посылает ему по открытому

каналу секретный AES-ключ K, зашифрованный по методу RSA; абонент B расшифровывает полученную криптограмму, используя свой закрытый RSA-ключ, и теперь может приступить к скоростному обмену информацией с A, применяя шифрование по методу AES на ключе K.

Тема 9. *АУТЕНТИФИКАЦИЯ. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ.*

Идентификация – это назначение объекту системы уникальной условной метки, которая позволяет однозначно определить этот объект. Под *аутентификацией* понимается проверка подлинности объекта, предъявившего данный идентификатор. Аутентификация основана на информации, которая может быть известна только истинному пользователю системы.

Пусть в коммуникационной сети, снабженной системой шифрования RSA, абонент A желает распространить открытое сообщение m и подтвердить свое авторство. Всем пользователям сети доступен открытый ключ абонента A – пара чисел (n,e). Кроме того, A держит в секрете свой закрытый ключ d – единственное число, вместе с e и $n=pq$ удовлетворяющее сравнению $ed \equiv 1 (\mathrm{mod}\ (p-1)(q-1))$. Для осуществления своей задачи A представляет m в числовом виде, пусть окажется $m < n$, и вычисляет $s=(m^d)_{\mathrm{mod}\ n}$ – это его *цифровая подпись*. Затем он рассылает по сети пару чисел (m, s). Абонент B, прочитав m и желая убедиться в том, что приславший сообщение на самом деле тот, за кого он себя выдает, извлекает из RSA-справочника сети принадлежащий A открытый ключ (n, e) и находит с его помощью число $(s^e)_{\mathrm{mod}\ n}$. Если полученное число совпадает с m, проверяющий убеждается в том, что *целостность* исходного сообщения не нарушена, т.е. в процессе передачи оно не было изменено, и что приславший это сообщение знает закрытый ключ, связанный с открытым ключом абонента A, т.е. это и есть A.

Например, если криптографическими параметрами абонента А в системе являются p=3, q=11, n=33, e=7, d=3 и рассылаемое сообщение это m=2, то подписью А будет $s=(m^d)_{\text{mod } 33}=(2^3)_{\text{mod } 33}=8$. Абоненты сети получат пару чисел (2, 8). Желая проверить авторство А и подлинность сообщения 2, В вычисляет: $(s^e)_{\text{mod } n}=$

$=(8^7)_{\text{mod } 33}=((2^3)^7)_{\text{mod } 33}=(2^{21})_{\text{mod } 33}= ((2^5)^4\cdot 2)_{\text{mod } 33}=((32)^4\cdot 2)_{\text{mod } 33}=((-1)^4\cdot 2)_{\text{mod } 33}=2$

и приходит по результатам проведенных одновременно аутентификации и проверки целостности к положительному заключению.

Какой была бы подпись абонента А под сообщением m=2, если бы он выбрал e=3 и тогда получил бы d=7?

Какой была бы подпись абонента А под сообщением m=3, если бы он выбрал p=3, q=11, e=7. Проверьте подлинность подписи абонента А.

Использованная в описанной процедуре аутентификации идея цифровой подписи приобрела фундаментальное значение для современного электронного документооборота. Поскольку реализация этой идеи невозможна без средств современной вычислительной техники, принято говорить об *электронной цифровой подписи* (*ЭЦП*).

Деловой обмен информацией между пользователями информационной сети предполагает, в частности, передачу данных, направленных на осуществление тех или иных действий. При этом должна быть обеспечена защита от различных злонамеренных поступков, таких как отказ отправителя от переданного сообщения, приписывание им авторства другому лицу, изменение текста получателем или кем-либо другим и т.п. На протяжении столетий надежным препятствием на пути подобных нежелательных возможностей являлась собственноручная подпись отправителя на передаваемом документе. Привлечение сети Интернет для финансовой и торговой деятельности побудило заинтересованные структуры к поиску столь же надежного электронного средства обеспечения безопасности соответствующего документооборота. В результате появилась следующая общая схема электронной цифровой подписи, основанная на практике

асимметричной криптографии. Пользователь А имеет в своем распоряжении два ключа: закрытый, который он держит в секрете, и открытый, который может быть доступен любому другому пользователю. С помощью своего закрытого ключа А изготавливает из оригинального текста некоторое другое сообщение – это его ЭЦП. Затем А передает исходный текст вместе со своей ЭЦП абоненту В, снабжая его при необходимости своим открытым ключом (или В сам может найти этот ключ в справочнике сети). Далее В осуществляет второй этап процедуры ЭЦП: он проверяет подпись абонента А с помощью его открытого ключа. При этом происходит и проверка целостности полученного сообщения.

Существенным моментом является то, что подпись зависит от текста передаваемого сообщения: малейшее изменение в нем обязательно влечет за собой изменение подписи, в частности подпись, сопровождающую один документ, невозможно перенести на другой. Если подпись успешно прошла проверку, подписавший не может отказаться от нее, поскольку открытый ключ, используемый при проверке, однозначно определяется хранящимся у него закрытым ключом.

ЭЦП признается аналогом собственноручной подписи во многих странах мира. В числе первых, принявших соответствующий закон, были США, где с лета 2000 года документы с ЭЦП получили такую же юридическую силу, как и подписанные от руки. Через год, в июле 2001 года, директиву, юридически признающую ЭЦП в государствах-членах европейского Союза, приняла Европейская комиссия. В январе 2002 года вступил в силу закон Российской Федерации №1–ФЗ «Об электронной цифровой подписи». В том же году для обеспечения большей криптостойкости первый отечественный стандарт ЭЦП ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» был заменен на новый стандарт ГОСТ Р 34.10-2001 «Информационная технология.

Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», разработанный коллективом ведущих российских криптографов во главе с А.С. Кузьминым и Н.Н. Мурашовым и основанный на математическом аппарате эллиптических кривых. Модификация этого алгоритма ГОСТ Р 34.10-2012 (под тем же названием) была осуществлена Главным управлением безопасности связи Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации при участии Всероссийского НИИ стандартизации. Согласно приказу Росстандарта от 7 августа 2012 года этот алгоритм электронной подписи введен в действие с 1 января 2013 года. Полный переход к новому стандарту должен завершиться к 31 декабря 2017 года.

8 апреля 2011 года вступил в силу новый Федеральный закон Российской Федерации: № 63-ФЗ «Об электронной подписи». В нем в качестве основного принимается термин *электронная подпись* (сокращенно *ЭП*), формулируются основные понятия, устанавливается правовое регулирование отношений в области использования электронных подписей, описываются средства электронной подписи и поддерживающая ее инфраструктура. Федеральный закон от 10 января 2002 года №1–ФЗ «Об электронной цифровой подписи» признается утратившим силу с 1 июля 2012 года.

Тема 10. *ХЕШ-ФУНКЦИИ.*

Медлительность алгоритмов асимметричного шифрования сильно затягивает процессы изготовления и проверки ЭЦП в случае подписываемых текстов большой длины. Поэтому необходимым элементом всех практических процедур ЭЦП является использование так называемых функций хеширования, или хеш-функций.

Хеш-функция предназначается для компактного представления длинных последовательностей (слов). Она преобразует сообщение

произвольной длины над данным алфавитом в блок фиксированной длины над тем же алфавитом, т.е. производит свертку всех сообщений (слов) в сообщения (слова) одной и той же заданной длины. Так, например, отечественная функция хеширования ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования», базирующаяся на алгоритме шифрования ГОСТ 28147-89, переводит двоичные последовательности произвольной длины в двоичные 256-битовые слова, а разработанная в 1992 году Ривестом MD-5 дает 128-битовое хеш-значение (называемое дайджестом сообщения, Message Digest).

Нетрудно придумать примеры хеш-функций: пусть, скажем, сверткой сообщения является его начальный пятибуквенный отрезок или просто первая буква. Однако криптографическая хеш-функция h должна для любого слова p не только достаточно просто вычислять его свертку $h(p)$, но и обладать следующими защитными свойствами:

1) (*противодействие определению прообраза*) если известно, что q является сверткой некоторого слова, то практически невозможно найти слово p, для которого $h(p)=q$;

2) (*противодействие обнаружению второго прообраза*) для данного слова p невозможно найти другое слово p' с такой же сверткой: $h(p')=h(p)$;

3) (*противодействие коллизии*) невозможно найти два разных слова p и p' с одинаковой сверткой: $h(p)=h(p')$.

Какое из свойств противодействия 2) или 3) хеш-функции, по вашему мнению важнее для ее практического использования?

В алгоритмах ЭЦП перед изготовлением подписи исходное сообщение m заменяется его сверткой $h(m)$, где h - выбранная для данной процедуры ЭЦП хеш-функция. В отечественном стандарте ЭЦП ГОСТ Р 34.10-2001, как и в его предшественнике ГОСТ Р 34.10-94, используется упомянутая хеш-функция ГОСТ Р 34.11-94. Хеш-функция SHA (Secure Hash Algorithm), применяемая в американском стандарте ЭЦП 1994 года, выдает 160-битовые значения и имеет большое сходство с MD-5, которая не была

стандартизирована из-за обнаруженной слабости в противодействии коллизии. Сравнительная скорость хеширования (Кбайт/с): ГОСТ – 11, MD-5 – 174, SHA – 75.

В 2012 году российский стандарт хеш-функции был модифицирован Центром защиты информации и специальной связи ФСБ России при участии ОАО «ИнфоТеКС» («Информационные технологии и коммуникационные системы») и приказом Росстандарта от 7 августа 2012 года новый стандарт ГОСТ Р 34.11-2012 был введен в действие с 1 января 2013 года. Необходимость замены вызвана возросшими требованиями к криптографической стойкости и предписаниями стандарта ГОСТ Р 34.10-2012 на электронную подпись, где используется новая хеш-функция «Стрибог». Неофициальное название хеш-функции ГОСТ Р 34.11-2012 отсылает нас к славянской мифологии и к ее божеству воздушных стихий. В самом стандарте оно не упоминается. Хеш-функция «Стрибог» по своей структуре очень похожа на ГОСТ Р 34.11-94. Она состоит из двух хеш-функций «Стрибог-256» и «Стрибог-512» с длинами результирующих значений 256 и 512 битов соответственно.

Кроме выполнения задачи компактного представления информации, криптографические хеш-функции, обладая вышеуказанными свойствами противодействия, могут служить и для аутентификации сообщений. Код проверки подлинности сообщения, или MAC (Message Authentication Code) – это зависящая от секретного ключа криптографическая хеш-функция. Если абоненты сети A и B используют общий секретный ключ k, то A, посылая для B сообщение m, прикрепляет к нему MAC – хеш-значение $h(k||m)$ (к сообщению впереди приписывается ключ, создавая единый массив). Так как B знает ключ k, то, получив сообщение, скажем m', он вычислит $h(k||m')$ и, сравнив это значение с присланным MAC $h(k||m)$, увидит, изменилось или нет исходное сообщение в ходе передачи.

Коды MAC используются не только для аутентификации файлов, которыми обмениваются пользователи, но и для проверки сохранности

личных файлов при возможном вредоносном воздействии: владелец составляет таблицу MAC своих файлов и при обращении к какому-либо из них сверяет его вновь вычисленный MAC со значением, записанным в таблице.

Тема 11. *ЗАКОН ОБ ЭП: ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ.*

Согласно Закону «Об электронной подписи» сертификации соответствующим федеральным органом подлежат как средства, используемые при создании ключей ЭП, так и сами подписи. Сертификация подписи означает, что специальная организация – *удостоверяющий центр* – подтверждает, что данный открытый ключ (*ключ проверки ЭП*) принадлежит именно данному лицу.

Достоверность ЭП означает соответствие открытого ключа закрытому ключу. Однако сама подпись не содержит никаких данных о ее владельце, поэтому в случае судебного разбирательства при отказе абонента от его подписи, признанной достоверной, необходимо подтвердить, что подпись действительно принадлежит этому лицу. В случае традиционной подписи на бумажном носителе для этого назначается графологическая экспертиза, а когда речь идет об ЭП, этой цели служит сертификат ключа проверки ЭП. В этом документе, в частности содержатся: регистрационный номер ключа проверки ЭП, сам этот ключ, дата его формирования и срок действия, ФИО или псевдоним владельца ключа, его собственноручная подпись. Сертификат изготовляется в двух экземплярах на бумажных носителях. Один экземпляр выдается владельцу ключа, второй остается в удостоверяющем центре.

Кроме выдачи сертификатов ключей подписей, в функции удостоверяющего центра входит создание ключей ЭП по заявкам абонентов системы с гарантией сохранения в тайне закрытого ключа подписи; ведение реестра сертификатов ключей подписей с обеспечением свободного доступа к нему абонентов; подтверждение подлинности сертифицированных в этом

удостоверяющем центре подписей, проставленных в электронных документах.

В качестве удостоверяющего центра ЭП должно выступать юридическое лицо, обладающее необходимыми материальными и финансовыми возможностями, позволяющими ему нести ответственность перед пользователями сертификатов ключей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Единый государственный реестр сертификатов ключей подписей должен вести уполномоченный федеральный орган – Головной удостоверяющий центр ЭП.

В терминологии ФЗ РФ «Об электронной подписи» укажите в примере из темы 9 ключ подписи и ключ проверки подписи.

Уясните классификацию видов электронной подписи на основе статьи 5 Закона «Об электронной подписи».

Некоторый электронный документ подписан электронной цифровой подписью в мае 2009 года. Каков его настоящий статус в соответствии с Федеральным Законом РФ «Об электронной подписи» № 63-ФЗ 2011 года?

Сейчас в стране действует значительное число удостоверяющих центров, ассоциированных с различными ведомствами и негосударственными структурами. Так, целый ряд удостоверяющих центров был организован на базе сертифицированного программно-аппаратного комплекса «КриптоПро УЦ», разработанного ведущей компанией РФ в сфере защиты информации ООО «КриптоПро».

Однако, несмотря на развитую сеть локальных удостоверяющих центров, они, обслуживая свою клиентуру, все же не могут обеспечить ей правовую защиту при внешнем обмене документами. Полностью проблема применения электронной цифровой подписи в нашей стране будет решена лишь после начала функционирования Головного удостоверяющего центра ЭП.

Тема 12. *СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ), РЕАЛИЗУЮЩИЕ ОСНОВНЫЕ ФУНКЦИИ ЭП.*

Основными криптографическими действиями, осуществляемыми процедурой цифровой подписи, являются шифрование подлежащего подписанию текста (иногда этот этап опускается), изготовление хеш-образа подписываемого сообщения, формирование подписи и ее проверка. Существует множество программных и программно-аппаратных комплексов, предназначенных специально для реализации этих функций. Рассмотрим наиболее известные из них.

а) Общедоступный пакет PGP.

В 1991 году американский программист Филипп Циммерман на основе известных криптографических алгоритмов создал пакет программ PGP (Pretty Good Privacy, Очень хорошая конфиденциальность) для защиты электронной корреспонденции от несанкционированного доступа и передал его для размещения в Интернете. Эффективная реализация самых стойких шифров, бесплатный доступ, удобный интерфейс способствовали быстрому распространению пакета по всему миру. Вследствие этого автору пришлось энергично отбиваться от обвинений со стороны ФБР в запрещенном экспорте военного снаряжения (по законодательству США шифры относились к такому снаряжению наряду, например с танками и ракетами). Трехлетнее расследование так и не дошло до суда, а только принесло Циммерману, без преувеличения, мировую известность. Вскоре он уладил и другое неприятное дело – с большим трудом все же получил лицензию от компании RSA Data Security Inc., считавшей, что он нарушил ее патентные права, самовольно включив в свою разработку шифр RSA. В 1996 году была образована компания Pretty Good Privacy Inc., которая затем подверглась многочисленным коммерческим преобразованиям. В 2010 году калифорнийская компания Symantec, разработчик программного обеспечения в области защиты информации, выкупила PGP за 300 миллионов долларов.

Пакет PGP позволяет выполнять операции шифрования и цифровой подписи сообщений. Для шифрования пользователь может выбрать, например, 3DES или AES. Для создания ключей ЭЦП он должен указать свое имя и свой адрес электронной почты, тип ключа (закрытый, открытый), его длину (от 1024 до 2048 битов) и предполагаемый срок действия.

При выработке ЭЦП сообщение по умолчанию шифруется, но этот этап можно опустить. Свертку текста осуществляет по выбору одна из хеш-функций, например, MD5. Затем подпись для хеш-значения создается при помощи закрытого ключа. Проверку подписи осуществляет получатель, которому передается открытый ключ отправителя. При этом получатель возможно захочет убедиться в том, что открытый ключ действительно принадлежит отправителю. PGP включает в себя внутреннюю схему сертификации открытых ключей, называемую «сетью доверия». Пара «имя пользователя – открытый ключ» может быть подписана третьим лицом, пользующимся доверием получателя, которое удостоверяет соответствие ключа и его владельца. При широких сетевых контактах найти такое лицо несложно. Впрочем, есть и сертификация через базовые серверы.

Пакет PGP является самым распространенным программным продуктом для защиты информации в персональных компьютерах. Он легко доступен в Интернете.

б) Семейство СКЗИ «Верба».

Пакет программ «Верба» был разработан в МО ПНИЭИ (Московское отделение Пензенского научно-исследовательского электротехнического института) для обеспечения конфиденциальности и целостности информации в электронных коммуникационных системах. Различные модификации первоначального продукта в настоящее время применяются в системах защиты многих информационных сетей.

В СКЗИ «Верба-OW» (для операционной сети Windows) реализованы следующие процедуры: шифрование и дешифрование (в соответствии с алгоритмом ГОСТ 28147-89), генерация ключей шифрования и ключей ЭП,

формирование и проверка ЭП (в последней версии 6.1 наряду со стандартом ГОСТ Р 34.10-94 применяется и алгоритм ГОСТ Р 34.10-2001), выработка значения хеш-функции (по ГОСТ Р 34.11-94). Динамическая библиотека СКЗИ «Верба-OW» встраивается в прикладное программное обеспечение пользователя. Разрешена эксплуатация до 31 декабря 2018 года (СКЗИ «Верба-OW» версии 6.1.2).

При работе на персональном компьютере (Intel Celeron 266 МГц) СКЗИ «Верба-OW» обеспечивает следующие показатели: шифрование – 2,0 Мбайт/с, дешифрование – 2,0 Мбайт/с, формирование ЭП – 0,01 с, проверка ЭП – 0,04 с, выработка значения хеш-функции – 1,9 Мбайт/с.

СКЗИ семейства «Верба» заслужили высокую деловую репутацию и используются в практике многих коммерческих, банковских и финансовых структур, а также в целом ряде государственных учреждений.

Подробнее о СКЗИ «Верба» можно узнать на официальном сайте www.security.ru компании ЗАО МО ПНИЭИ.

в) Криптопровайдер «КриптоПро CSP».

Рассматриваемое СКЗИ было разработано ООО «КриптоПро» в соответствии с криптографическим интерфейсом фирмы Microsoft – Cryptographic Service Provider (CSP), что позволяет использовать российские криптографические алгоритмы в продуктах Microsoft Windows.

Система имеет сертификат соответствия и предназначена для обеспечения конфиденциальности и контроля целостности информации посредством шифрования, для гарантии юридической значимости документооборота в информационной сети посредством использования процедур формирования и проверки электронной подписи, для защиты системного и прикладного программного обеспечения от несанкционированного изменения. В ней реализуются отечественные криптографические стандарты: для шифрования и дешифрования – ГОСТ 28147-89, для электронной подписи – ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, для хеширования – ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012. Размеры

ключей ЭП: ключ ЭП – 512 битов при использовании алгоритма ГОСТ Р 34.10-2001 и 512 или 1024 битов при использовании алгоритма ГОСТ Р 34.10-2012, ключ проверки ЭП – 512 битов при использовании алгоритма ГОСТ Р 34.10-2001 и 512 или 1024 битов при использовании алгоритма ГОСТ Р 34.10-2012.

«КриптоПро CSP» может применяться в составе стандартного программного обеспечения Microsoft и других компаний, реализующих криптографический интерфейс в соответствии с архитектурой Microsoft, и может встраиваться во вновь разрабатываемое или существующее прикладное программное обеспечение.

Производительность системы в КриптоПро CSP 4.0 (для платформы Intel Core i5 3.3 GHz, Windows 7 x64): шифрование и дешифрование – 370 Мбайт/с, вычисление ЭП на коротких и на длинных ключах (по ГОСТ Р 34.10-2012) соответственно 0,06 мсек и 0,3 мсек, проверка ЭП на коротких и на длинных ключах (по ГОСТ Р 34.10-2012) соответственно 0,1 мсек и 0,5 мсек, выработка хеш-значения – 106 Мбайт/с.

На базе СКЗИ «КриптоПро CSP» был разработан программно-аппаратный комплекс «Удостоверяющий центр «КриптоПро УЦ» (сокращенно: ПАК «КриптоПро УЦ»). Его назначением является обеспечение деятельности удостоверяющих центров ЭЦП при реализации их целевых функций в соответствии с действующим законодательством. Число организаций, эксплуатирующих ПАК «КриптоПро УЦ», неуклонно растет и включает в себя некоторые важнейшие структуры государственного управления.

Подробнее о СКЗИ «КриптоПро CSP» можно узнать на официальном сайте www.cryptopro.ru компании ООО «КриптоПро».

КОНТРОЛЬНЫЕ ВОПРОСЫ К КУРСУ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

1. Какой шифр называется перестановочным?
2. Как осуществляется маршрутное шифрование?
3. Как осуществляется шифрование с помощью решеток?
4. Какой шифр называется шифром простой замены?
5. Как осуществляется шифрование с помощью алфавитной перестановки?
6. На чем основан криптоанализ шифров простой замены?
7. Какой шифр называется блочным?
8. Опишите шифр Уитстона-Плейфера.
9. Опишите шифр Виженера.
10. Как осуществляются сложение и умножение в модульной арифметике?
11. Какой шифр называется поточным?
12. Дайте общее описание книжного шифра.
13. Опишите процесс шифрования с автоключами.
14. Опишите шифр Вернама.
15. Почему шифр Вернама не раскрываем?
16. В чем недостаток шифра Вернама?
17. Какова длина секретного ключа в шифре DES? Сколько раундов шифрования выполняется в DES?
18. Какова длина секретного ключа в шифре ГОСТ 28147-89? Сколько основных шагов шифрования выполняется в ГОСТ 28147-89?
19. Какова функция таблицы замены в шифре ГОСТ 28147-89?
20. Какие шифры являются государственными стандартами шифрования в США и России в настоящее время?
21. Почему шифр RSA называется асимметричным?

22. На чем основана стойкость шифра RSA?

23. Что такое цифровой конверт?

24. Опишите общую схему ЭЦП.

25. Каково назначение хеш-функции?

26. Какими свойствами противодействия должна обладать криптографическая хеш-функция?

27. Что такое MAC и как он формируется?

28. Каковы функции удостоверяющего центра ЭП?

29. Какие сведения заносятся в сертификат открытого ключа ЭП?

30. Для каких целей используется СКЗИ «Верба-OW»?

31. Какие отечественные криптоалгоритмы реализуются в «КриптоПро CSP»?

32. Каково назначение ПАК «КриптоПро УЦ»?

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии : учебное пособие, 3-е изд., испр. и доп. М. : Гелиос АРВ, 2005. 480 с.
2. Баричев С.Г., Серов Р.Е. Основы современной криптографии [Электронный ресурс] : Учебный курс. Ver. 1.3. URL: http://www.ict.edu.ru/ft/002447/crypto1-3.pdf (дата обращения: 31.08.2017). Загл. с экрана. Яз. рус.
3. Гашков С.Б., Применко М.А., Черепнев М.А. Криптографические методы защиты информации. М. : Изд. Центр «Академия», 2010.
4. Государственный стандарт РФ ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (принят и введен в действие постановлением Госстандарта РФ от 12 сентября 2001 г. № 380-ст).
5. Государственный стандарт РФ ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» (принят и введен в действие постановлением Госстандарта от 23 мая 1994 г. № 154) : [Электронный ресурс]. URL: http://www.certisfera.ru/uploads/GOST-R-34.11-94.pdf (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.
6. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М. : КУДИЦ-ОБРАЗ, 2001.
7. Национальный стандарт РФ ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (утвержден и введен в действие приказом Росстандарта от 7 августа 2012 г. № 215-ст) : [Электронный ресурс]. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.
8. Национальный стандарт РФ ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (утвержден и введен в действие приказом Росстандарта от 7 августа 2012 г. № 216-ст) : [Электронный ресурс]. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.
9. Национальный стандарт РФ ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» (утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст) : [Электронный ресурс]. URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.

10. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М. : Науч. Мир, 2004.
11. Сингх С. Книга шифров: тайная история шифров и их расшифровки. М. : АСТ: Астрель, 2007.
12. Федеральный закон Российской Федерации от 10 января 2002 г. №1-ФЗ «Об электронной цифровой подписи» : [Электронный ресурс]. URL: http://www.rg.ru/2002/01/10/podpis-dok.html (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.
13. Федеральный закон Российской Федерации от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» : [Электронный ресурс]. URL: http://www.rg.ru/2011/04/08/podpis-dok.html (дата обращения: 31.08.2017). Загл. с экрана. Яз. Рус.
14. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптографии. Минск : Новое Знание, 2004.
15. Черчхаус Р.Ф. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. М. : Весь мир, 2005.