ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»

Болелов Э.А., Петров В.И.

АВИАИНЖЕНЕР БУДУЩЕГО: ИНФОРМАЦИОННЫЙ МИР XXI ВЕКА

Криптография – основа информационной безопасности

Методическое пособие для учителей инженерных классов московских школ

Москва 2016 г.

Рецензенты: д.т.н., проф. Прохоров А.В. (МГТУ ГА)
к.т.н., доц. Полосин С.А. (ГосНИИ АС)

Болелов Э.А., Петров В.И.
Авиаинженер будущего: информационный мир XXI века. Криптография – основа информационной безопасности.
Методическое пособие для учителей инженерных классов московских школ

В методическом пособии излагаются вопросы зарождения и развития криптографии, как науки, приводятся примеры самых известных систем шифрования, рассматриваются математические основы современной криптографии, приводятся примеры современных симметричных и асимметричных систем шифрования и их применение в области защиты информации. В методическом пособии рассмотрены задачи по криптографии для учащихся инженерных классов с примерами их решения.

Данное учебное пособие написано в рамках Соглашения Департамента образования г. Москвы с МГТУ ГА. Методическое пособие рассмотрено на заседании кафедры «Технической эксплуатации радиоэлектронного оборудования воздушного транспорта» 18.11.2016 г. протокол №4.

Содержание

Введение

Дорогие учителя инженерных классов! Вашему вниманию представляется методическое пособие серии «Информационный мир XXI века», которая посвящена криптографическим методам защиты информации.

Информационная революция, начавшаяся в семидесятых годах двадцатого века и связанная с появлением микропроцессорных технологий и персонального компьютера изменила мир до неузнаваемости практически за время жизни одного поколения. Невозможно представить сегодня жизнь современного общества без компьютера, смартфона, интернета. Звонок знакомому, находящемуся на другом континенте, не выходя из дома, перестал восприниматься как «чудеса техники», а «виртуальные» финансовые операции (оплата счетов за услуги, покупка билетов на транспорт, бронирование мест и т.д.) стали обыденными. Современный самолет уже называют "летающим компьютером". Так, вычислительная система пассажирского самолета включает порядка восьмидесяти бортовых компьютеров, получающих данные о параметрах полета и управляющих по специальному полетному плану режимами взлета, следования по маршруту и посадки. Данные с органов управления самолета поступают непосредственно в вычислительную систему самолета. То есть, штурвал самолета, на самом деле, является джойстиком бортового компьютера воздушного судна и вычислительная система самолета, контролируя пилотов, принимает решение на окончательное управление рулевыми поверхностями самолета.

Информационный мир сегодня огромен и многогранен, он затрагивает практически все стороны нашей жизни. Поэтому проблема защиты информации в этом информационном мире на сегодняшний день стоит особенно остро. Средства массовой информации то и дело сообщают нам об успешных или безуспешных попытках «взлома» серверов банков, государственных и частных компаний, прослушиваниях телефонов государственных деятелей, крупных коммерческих фирм и так далее. Так, на профильной конференции в Амстердаме, бывший пилот, а ныне консультант по вопросам безопасности Хьюго Тесо наглядно продемонстрировал возможность взлома бортовой системы самолета с помощью смартфона Samsung на платформе Android (об этом 11 апреля 2013 года писала The Daily Mail).

Целью пособия является знакомство вас с криптографией и ее решающей ролью в обеспечении информационной безопасности современного информационного мира, а также предоставления вам необходимых для понимания криптографии задач для учащихся с примерами их решения. Задачи разделены на два типа сложности. Усложненный тип задач может стать основой для формирования тем различных проектов, выполняемых учащимися инженерных классов.

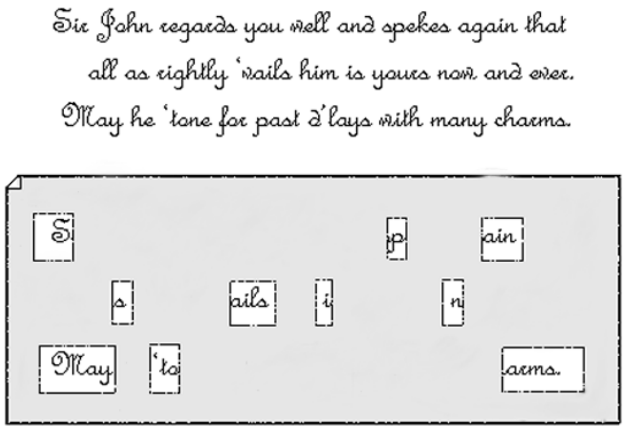
1. Как защитить свое послание?

С тех пор как люди изобрели письменность, потребовалось защищать свои послания от посторонних. В документах древних цивилизаций (Индии, Египта, Месопотамии, Греции) встречаются сведения о способах защиты посланий. Уже в те времена человек выработал три основных способа защиты информации.

Первый способ защиты информации – физическая защита от противника материального носителя информации (пергамента, бумаги), например, передача информации специальным курьером с охраной, сундук с надежным замком для тайного послания и так далее.

Второй способ защиты информации – сокрытие от противника самого факта передачи информации. Интересен способ, описанный в трудах Геродота. На голове раба, которая брилась наголо, записывалось послание. Когда волосы раба достаточно отрастали, его отправляли к адресату, который снова брил голову раба и читал послание.

Для защиты посланий были широко распространены, и сейчас используются, симпатические или «невидимые» чернила. Между строк ничем не примечательного послания записывалось передаваемое сообщение. Адресат проводил термическую, химическую или другую обработку и читал передаваемое скрытое сообщение. В XVI-XVIII веках пользовались популярностью различные «решетки», предназначенные для кодирования сообщений. Наиболее известна «решетка», которую называют «шифром Ришелье». Эта «решетка» вырезалась из листа картона или пергамента, или же из любого тонкого металла.



«Решетка» помещается на лист бумаги и затем записывается сообщение в ее прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделенным на большое число маленьких фрагментов. Затем «решетка» убирается, и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью другого текста. Такое заполнение требует известного литературного таланта. Для расшифровки у получателя сообщения должна быть такая же «решетка». Подобной «решеткой» пользовался известный русский дипломат и писатель А.С. Грибоедов будучи послом в Персии.

В настоящее время разработкой средств и методов сокрытия факта передачи сообщений занимается специальная наука – **стеганография.**

Третий способ защиты информации – преобразование информации, маскирующее ее содержание от посторонних лиц. Такое преобразование информации называется **криптографическим**, а наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей называется **криптографией.**

Далее мы будем рассматривать только криптографические способы защиты информации, потому что криптография является основой современных систем защиты информации и наиболее широко используется.

В целях понимания материала, изложенного в книге, дадим некоторые основные определения и понятия криптографии.

Криптография – наука, изучающая методы, алгоритмы и средства преобразования информации (шифрования) в целях сокрытия ее содержания. **Криптоанализ** - наука, изучающая методы, алгоритмы и средства анализа криптосистем извлечения конфиденциальной информации. Таким образом, криптография и криптоанализ составляют единое целое и образуют науку - **криптологию.**

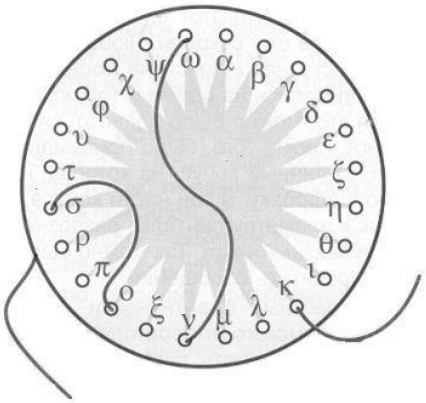
Исторически центральным понятием криптографии является понятие шифра. **Шифром** называется совокупность обратимых криптографических преобразований множества открытых текстов на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид криптографического преобразования открытого текста определяется с помощью **ключа** шифрования. **Открытым текстом** называют исходное сообщение, которое подлежит зашифрованию. Под **зашифрованием** понимается процесс применения обратимого криптографического преобразования к открытому тексту, а результат этого преобразования называется **шифртекстом** или **криптограммой**. Соответственно, процесс обратного криптографического преобразования криптограммы в открытый текст называется **расшифрованием**. Расшифрование нельзя путать с дешифрованием. **Дешифрование (дешифровка, взлом)** - процесс извлечения открытого текста без знания криптографического ключа на основе перехваченных криптограмм.

2. Из истории криптографии

Вероятно, первые в истории человечества шифровальные устройства (шифраторы) появились в Древней Греции. Первое шифровальное устройство - скиталу создали в Спарте примерно в V-IX вв. до н. э.. **Скитала** (в переводе - «жезл» или «посох») представляет собой цилиндр заданного диаметра. На цилиндр наматывался ремень из пергамента, на который наносился текст сообщения вдоль оси цилиндра. Затем ремень сматывался и отправлялся получателю сообщения. Последний, имея аналогичный цилиндр, расшифровывал сообщение. Ключом шифра является диаметр скитала. Изобретение

дешифровального устройства приписывается Аристотелю. Он предложил использовать для дешифрования конусообразное «копье», на которое наматывался перехваченный ремень, до тех пор, пока не появлялся осмысленный текст. Скитала упоминается в трудах Аполлония Родосского (III в. до н.э.), а также Плутарха (около 45-127 гг. н. э.), у которого описывается сам способ шифрования.

В античные времена в IV в. до н.э. древнегреческий полководец Эней Тактик предложил устройство, названное впоследствии **диском Энея**. Принцип был прост. На диске размером 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска закреплена катушка с нитью. При зашифровании нитка последовательно протягивалась через отверстия соответствующие буквам послания. Диск отсылался получателю, который вытягивал нитку из отверстий и получал сообщение в обратном порядке.



Другим устройством шифрования, предложенным Энеем Тактиком является **линейка Энея**. Здесь вместо диска использовалась линейка с числом отверстий, равным числу букв в алфавите. Буквы по отверстиям располагались в произвольном порядке. К линейке прикреплялась катушка с нитью. При шифровании нить протягивалась через отверстие, соответствующее букве шифруемого послания, при этом на нити в месте прохождения отверстия завязывался узелок. Таким образом, зашифрованное послание представляло собой нить с узелками, в которой каждой букве ставилось в соответствие расстояние между узелками нити. Ключом шифра являлся порядок следования букв по отверстиям линейки.

Еще оно изобретение древних греков - **квадрат Полибия**. Полибий – греческий государственный деятель, полководец III века до н.э. Применительно к современному английскому алфавиту шифрование по этому квадрату заключалось в следующем. Шифруемая буква заменялась на координаты квадрата, в котором она записана. Так буква R заменяется на DB. При расшифровании каждая пара букв определяет соответствующую букву сообщения. Например, TABLE – DDAAABCAAE. Ключом этого шифра является сам квадрат.

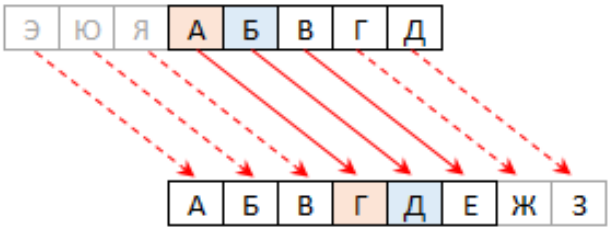
	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I,J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

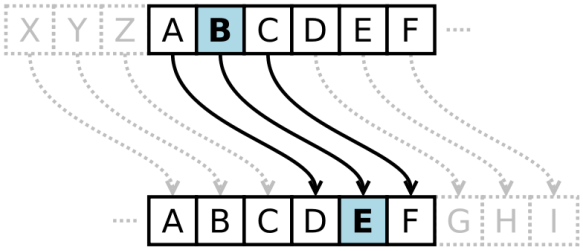
Интересно отметить, что в несколько измененном виде квадрат Полибия дошел до наших дней и получил название «тюремный шифр». Для его использования достаточно знать только естественный порядок букв в алфавите. Стороны квадрата обозначаются не буквами, а цифрами. Каждая цифра кодируется определенным количеством стуков. При передаче сообщения сначала «отстукивается» номер строки, а затем номер столбца. «Тюремный шифр» строго говоря, не является

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

шифром, это способ кодировки сообщения с целью его приведения к виду удобному для передачи по каналу связи (тюремная стена).

Значительный вклад в развитие криптографии внес Гай Юлий Цезарь - древнеримский государственный и политический деятель, диктатор. Суть метода шифрования заключается в следующем. Выписывается алфавит, а затем под ним выписывается тот же алфавит, но с циклическим сдвигом на три буквы влево.





Шифрование заключается в выборе буквы из первой строки и замену ее на букву второй строки, расшифрование представляет собой обратную операцию. Например, APPLE – DSSOH. Ключом шифра Цезаря является величина циклического сдвига. Гай Юлий Цезарь всю жизнь использовал один и тот же ключ – сдвиг на 3 буквы. Приемник Юлия Цезаря – Цезарь Август использовал тот же шифр, но со сдвигом на одну букву.

В эпоху раннего средневековья мощная созидательная энергия арабской культуры, которую ислам лишил портретной живописи и скульптуры, дала плоды на ниве литературы, музыки и наук. Распространились различные ремесла, развивалась система государственного управления, которая потребовалаосоздания различных методов защиты информации. Разумеется, не обошли своим вниманием арабы и криптографию. Получило широкое распространение составление словесных загадок, ребусов и каламбуров. Грамматика стала главным учебным предметом и включала в себя тайнопись. Тайнопись и ее значение упоминаются в сказках Шехерезады «Тысяча и одна ночь». Да и само слово «шифр» имеет корни в арабском слове صِفْر («сифр», т.е. «ноль»). Кстати, цифры которыми сейчас пользуются в мире, называются «арабскими», хотя на самом деле они пришли в Европу через Ближний Восток из Индии. Сейчас арабы, как и все в мире, пользуются десятичной системой счисления, однако написание цифр серьезно отличается от принятого на Западе.

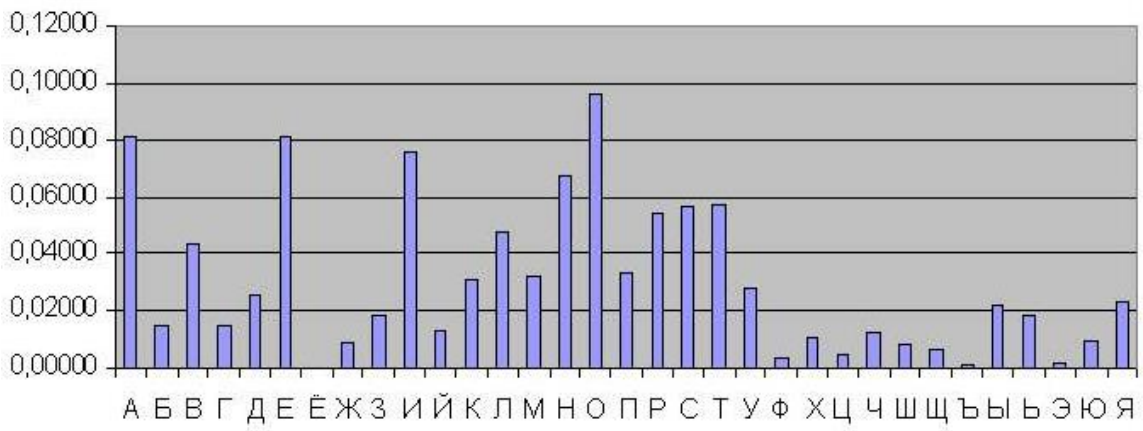
0 1 2 3 4 5 6 7 8 9

٠ ١ ٢ ٣ ٤ ٥ ٦ ٧ ٨ ٩

На Арабском Востоке появились книги не только с описаниями известных на тот момент систем шифрования, но и впервые в истории было рассказано о криптоанализе (дешифровании). Именно в этих книгах (примерно в VIII-IX веках) впервые были описаны содержательные методы криптоанализа.

Арабский филолог, создатель методики традиционного арабского языкознанияХалиль ибн Ахмад аль-Фарахиди (VIII век) первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования. Он предположил, что первыми словами в письме на греческом языке византийскому императору будут «Во имя Аллаха», что позволило ему прочитать оставшуюся часть сообщения. Позже он написал книгу с описанием изобретенного им метода - «Китаб аль-Муамма» («Книга тайного языка»). Сейчас этот метод криптоанализа носит название - «протяжка вероятного слова».

Арабский философ, математик, астроном, теоретик музыки Абу Юсуф Якуб ибн Исхак аль-Кинди (IX век) работал в «Доме мудрости» в Багдаде. Аль-Кинди является автором около 250 трактатов по метафизике, логике, этике, математике, медицине, метеорологии, оптике, музыке, а также криптографии. Аль-Кинди можно по праву назвать «отцом» криптоанализа. Наиболее значимый его труд по криптографии и криптоанализу «Трактат по дешифрованию криптографических сообщений». Аль-Кинди проанализировал отдельные буквы арабского алфавита и обнаружил, что некоторые буквы встречаются чаще, чем другие. На основании анализа Корана он вычислил частоты встречаемости букв арабского алфавита (на диаграмме представлены частоты встречаемости букв русского алфавита). Это, казалось бы, незначительное открытие привело к огромному прорыву в криптоанализе. Аль-Кинди впервые описал метод криптоанализа, известный сейчас как **частотный криптоанализ.**



Суть метода частотно криптоанализа заключается в следующем. Частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае простой замены, если в криптограмме будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Анализируя открытый им метод аль-Кинди выдвинул идею сложной замены, более устойчивой к частотному криптоанализу.

В 855 годувыходит «Книга о большом стремлении человека разгадать загадки древней письменности» арабского ученого АбуБакр Ахмед ибн Али Ибн Вахшия ан-Набати. В книге описываются несколько шифров, в том числе с

применением нескольких алфавитов. Также книге ан-Набати была посвящена дешифрованию древних письменностей, в том числе египетских иероглифов.

В книге X века «Адаб аль-Куттаб» («Руководство для секретарей») арабского ученого Абу Вакре Мухаммеде Бен Яхьяас-Сули есть инструкции по шифрованию записей о налогах, что подтверждает распространение криптографии в обычной, гражданской жизни.

В1412 году выходит 14-томная энциклопедия «Шауба ал-Аша» арабского ученого Шихаб аль-Дин Абу ал-Аббас Ахмед бен Али бен Ахмад Абд Аллах аль-Кашканди, один из разделов которой назывался «Относительно сокрытия в буквах тайных сообщений» и содержал описание семи шифров замены и перестановки, частотного метода криптоанализа, а также таблицы частотности букв в арабском языке на основе текста Корана. Основные криптографические идеи, описанные в книге аль-Кашканди, состоят в следующем: одна буква может заменять другую; можно записывать слово в обратном порядке; можно переставлять в обратном порядке чередующиеся буквы слов; можно заменять буквы на цифры; можно заменять каждую букву открытого текста на две арабские буквы, которые используются в качестве чисел, и сумма которых равна цифровой величине шифруемой буквы; можно заменять букву на имя человека; при шифровании можно использовать словарь замены, описывающий положения луны, названия стран, названия фруктов, деревьев и т.д.

Последующие 200 лет привели к последовательному упадку всей арабской науки, в том числе и криптографии. Во всяком случае, при описании дипломатической переписки арабских государств XV-XVI веков встречаются только простейшие системы шифрования и полное отсутствие малейших попыток вскрытия чужих шифров.

В эпоху раннего средневековья Западная Европа утратила большинство античных знаний. Уровень грамотности среди населения был чрезвычайно низкий, что приводило к тому, что необходимость шифрования информации практически отсутствовала. Значительно лучше положение дел обстояло в Византийской империи, но и здесь в основном использовались шифры простой замены и перестановки.

Во времена позднего средневековья европейская криптография приобрела сомнительную славу, отголоски которой слышаться и в наши дни. Дело в том, что криптографию стали отождествлять с черной магией, астрологией, алхимией, к шифрованию призывались мистические силы, европейские ученые того времени пытались получить знания у потусторонних сил.

Центром образованности в эти времена были монастыри. Здесь изучение тайнописи поощрялось, так как считалось, что в Священном писании скрыт тайный смысл. Криптография использовалась европейскими учеными для сокрытия своих научных результатов. Например, Галилей опубликовал ряд своих результатов в зашифрованном виде – очевидно, с целью, в случае если они будут признаны церковью, подтвердить

свой приоритет на научное открытие. Расшифровка ряда других средневековых текстов так же позволяет говорить о том, что этот прием широко использовался многими учеными. Некоторые из текстов остаются нерасшифрованными по сей день, например манускрипт Войнича (фрагмент манускрипта Войнича представлен на рисунке).

Одним из наиболее известных средневековых шифров перестановки является шифр **«магический квадрат».** «Магическим квадратам» приписывалась мистическая сила, поэтому шифры на их основе считались абсолютно стойкими. Магия этих квадратов заключалась в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному числу. Шифрование по «магическому квадрату» проводилось следующим образом. Буквы сообщения вписывались в квадрат согласно записанным в них числам, а в пустые клетки вставлялись произвольные буквы. Шифртекст выписывался в оговоренном заранее порядке. Например, сообщение ПРИЕЗЖАЮ СЕГОДНЯ зашифрованное с помощь «магического квадрата» имеет вид УИРДЗЕГЮСЖАОЕЯНП.

16 У	**3** И	**2** Р	**13** Д
5 З	**10** Е	**11** Г	**8** Ю
9 С	**6** Ж	**7** А	**12** О
4 Е	**15** Я	**14** Н	**1** П

Известным в эпоху средневековья шифром был еврейский шифр **атбаш.** Евреями были разработаны множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования. Знания этих шифров, и, в частности, шифра атбаш, позже перешло к рыцарям Ордена Тамплиеров. Шифр атбаш использовался тамплиерами на протяжении многих лет вплоть до 1300 г., когда Орден Тамплиеров был распущен. Алгоритм шифрования заключается в замене буквы открытого текста на букву шифртекста в соответствии с таблицей. В шифре атбаш просматривается идея шифра Цезаря.

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

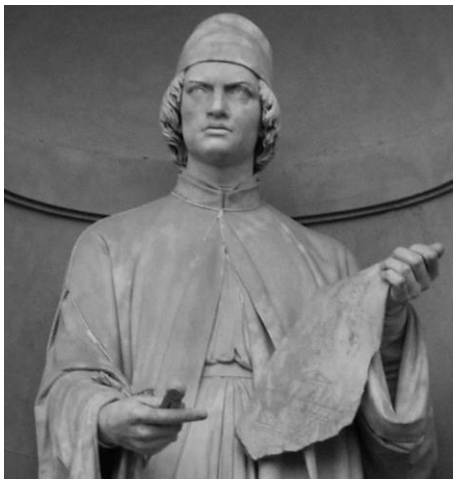
Первой европейской книгой, описывающей использование криптографии, считается труд английского монаха-францисканца, математика, оптика и астронома профессора Оксфордского и Парижского университетов Роджера Бэкона (1214 - 1292 гг.) «Послание монаха Роджера Бэкона о тайных действиях искусства и природы и ничтожестве магии», описывающий, в числе прочего, применение методов криптографии. Роджер Бэкон описывает методы криптографии, основанные на:

- пропуске гласных букв;
- использование метафор;
- использование букв из иностранных языков;
- использование способов передачи тайных посланий под видом обычных текстов.

Роджер Бэкон был обвинен в черной магии (изготовлении бронзовой головы, говорящей с помощью призванных Бэконом и его учеником Бунгеем потусторонних темных сил), провел 14 лет в заточении, а после освобождения стал отшельником.

Пришедшая на смену Средневековью и имеющая мировое значение эпоха Возрождения (Ренессанс) имеет свое начало в Италии примерно в XIV веке и затем распространившаяся повсеместно в Европе. Развитие культуры, наук, торговли, международных отношений послужило толчком к развитию криптографии. Основным потребителем криптографических знаний становится дипломатия. Появление посольств и дипломатических представительств потребовало создания надежных систем шифрования переписки дипломатов.

ВXIV веке сотрудник тайной канцелярии папской курии Чикко Симонети пишет книгу о системах тайнописи, а вXV веке секретарь папы Климентия XII Габриэль де Левинда, родом из города Пармы, заканчивает работу над «Трактатом о шифрах». Первая организация, посвятившая себя целиком криптографии, была создана в Венеции в1452 году. Три секретаря этой организации занимались взломом и созданием шифров по заданиям правительства.



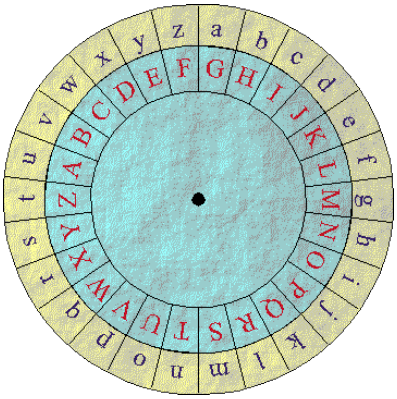
В XV веке итальянский ученый, философ, писатель, криптограф, ведущий теоретик искусства эпохи Возрождения, прослуживший более 30 лет прослужил в папской канцелярии, Леон Батиста Альберти разработал системы шифрования, ставшие основой шифровальных систем на несколько столетий. Изучив методы вскрытия использовавшихся в Европе простых шифров замены, он попытался создать шифр, который был бы устойчив к частотному криптоанализу.

Основной труд Альберти по криптографии - «Трактат о шифрах» (1466). Книга написана по заказу папы Римского. В книге Альберти:

- провел анализ шифров замены и перестановки;
- затронул вопросы стойкости шифров;
- провел анализ частот букв;
- выдвинул идею «двойного» шифрования;

- описал шифр собственного изобретения, названный им «шифром, достойным королей».

По сути, в своей системе шифрования Альберти предложил вместо единственного шифралфавита, как в простых шифрах, использовать два или более шифралфавита, которые переключаются по какому-либо правилу. Реализация шифра Альберти осуществлялась с помощью изобретенного им шифровального устройства. Устройство представляло собой шифровальный диск. На внешний неподвижный диск наносились буквы (могли наносится и цифры), под которыми располагались буквы внутреннего подвижного диска. Процесс шифрования прост – буквам и цифрам открытого текста ставились в соответствие буквы и цифры внутреннего диска. Пока диски не двигаются, они позволяют шифровать с использованием шифра Цезаря.После зашифровывания слова послания внутренний диск сдвигался на один шаг. Начальное положение дисков заранее оговаривалось. Диск Альберти с незначительными изменениями использовался вплоть до начала XX века.Леона Батиста Альберти историки часто называют «отцом» европейской криптографии.



Новаторские предложения в области криптографии в XV веке были сделаны немецким историком и криптографом аббатом Тритемием (Иоганном Хайденбергом). Он предложил шифр «Аве Мария» и шифр, основанный на периодически сдвигаемом ключе.

Наиболее серьезное предложение Тритемия, дошедшее до наших дней, заключается в придуманной им таблице.

Первая буква текста шифруется по первой строке, вторая буква по второй строке и так далее. Первая строка одновременно является строкой букв открытого текста. Например, FIGHT – FJIKX. В первоначальном варианте в шифре Тритемия отсутствовал ключ. Секретом являлся сам способ шифрования. Дальнейшее усложнение шифра шло двумя путями: введением произвольного порядка расположения букв в таблице и усложнением порядка выбора строк таблицы при шифровании. Следует сказать, что шифр Цезаря является частным случаем шифра Тритемия.

Шифр «Аве Мария» основан на принципе замены букв шифруемого текста на целые слова, из которых составлялись внешне невинные сообщения. Например, **Н** – «Я», «ЗДЕСЬ»; **Е** – «ЖДУ», «БУДУ»; **Т** – «ДОМА», «ВЕЧЕРОМ». Тогда открытомупосланию**НЕТ** могут соответствовать послания «Я ЖДУ ДОМА», «ЗДЕСЬ БУДУ ВЕЧЕРОМ».

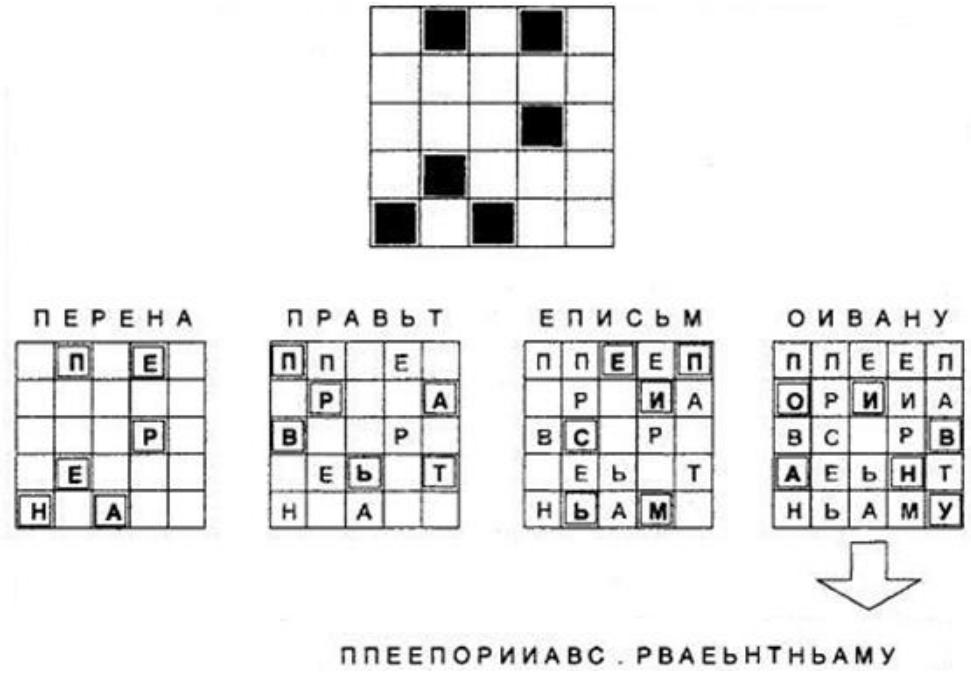
Кроме этого, Тритемий первым заметил, что шифровать можно и биграммами (биграмма представляет собой две рядом стоящие буквы слова или предложения), хотя первые шифры биграммной замены появились только XIXвеке.

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

Криптографические идеи Тритемия были улучшены Жовани Батиста Белазо, который в своей работе «Шифр сеньора Белазо» предложил выбирать некоторое ключевое слово и записывать его над каждым словом открытого текста. Каждая буква ключевого слова используется для выбора конкретного шифра сдвига из полного набора шифров для шифрования конкретной буквы, тогда как в работе Тритемия шифры выбираются просто по циклу. Для следующего слова открытого текста ключ начинал использоваться снова, так, что одинаковые слова оказывались зашифрованы одинаково. Данный способ в настоящий момент известен как шифр Виженера.

Существенный вклад в развитие криптографии внес математик, врач и философ ДжероламоКордано. Предложенный им в 1550 году шифр вошел в историю под названием «решетка Кордано». **«Решетка Кордано»** - это шифр перестановки, суть которого заключается в следующем. Брался лист плотного материала (картон, пергамент), представляющий собой квадрат в котором вырезаны «окна». При шифровании квадрат накладывался на лист бумаги и сообщение вписывалось в «окна», затем квадрат поворачивался на 90 градусов и сообщение продолжали записывать в «окна» повернутого квадрата. Такая процедура продолжалась до полного поворота квадрата на 360 градусов. Главное требование «решетки Кордано» - при всех поворотах «окна» не должны попадать на дно и тоже место, а при полном повороте квадрата все места в

шифртексте оказываются занятыми. Шифртекст считывался по строкам из полученной таблицы.

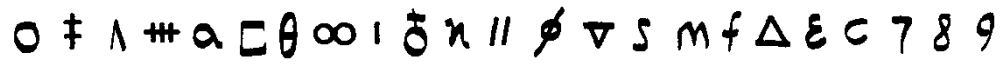


Кордано выдвинул, но не успел целиком реализовать идею «самоключа». Суть ее заключается в использовании в качестве ключа части открытого сообщения.

В XVI веке заметный вклад в развитие криптографии внесли Матео Ардженти, Джовани Батиста Порта и др.

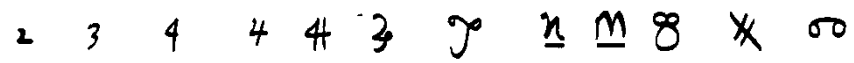
Матео Ардженти был криптографом папы Римского, именно ему принадлежит идея использования слова-лозунга для придания алфавиту легко запоминаемого смешанного вида. Ардженти также предложил вставлять в шифртекст большое количество букв «пустышек», устранять пунктуацию, не вставлять в шифртекст открытые слова («клер»), заменять буквы шифртекста на цифры. Ардженти занимался также усложнением кодов (номенклаторов). Им разработан новый номенклатор в котором 1200 букв, слогов и целых фраз заменялись на группы букв. Шифры **номенклаторы** известны с XII века. Номенклатор был разработан как система шифрования, наилучшим образом приспособленная к наиболее употребительным в то время методам криптоанализа. Он основывался на шифре замены с добавлением записи отдельных слов специальными кодами. Первоначально шифр был ограничен именами важных людей того времени, отсюда и последовало название шифра; в более поздних изданиях этот шифр дополнился большим количеством распространённых слов и географических названий. Обычным путем усиления стойкости номенклаторов было увеличение объёмов таблиц. К концу восемнадцатого столетия, когда система начала выходить из употребления, некоторые номенклаторы имели до 50 000 символов. Однако не все номенклаторы были сломаны. Некоторые номенклаторы были весьма внушительными по объему и занимали порой несколько книг.На рисунке приведен пример простого номенклатора Марии Стюарт.

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

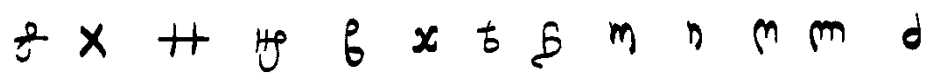


«Пустые» символы  Дублет 

and for with that if but where as of the from by



so not when there this in wich is what say me my wyrt



send ſre receave bearer I pray you Mte your name myne

Джовани Батиста делла Порта - итальянский ученый-энциклопедист, драматург, криптограф. Делла Порта постоянно приходилось опасаться интриг своих недоброжелателей, что заставляло его окружать свою жизнь атмосферой загадочности. Интерес делла Порта к магии и алхимии привел к тому, что против ученого было начато следствие Святейшей Инквизицией, завершившееся, впрочем, для него без последствий. Однако после этого делла Порта постепенно отошёл от научных изысканий и посвятил себя литературно-драматургической деятельности. Однако, он постоянно находились под пристальным наблюдением агентов инквизиции.

В 1563 делла Порта опубликовал фундаментальный труд по криптологии - «Про скрытую значимость отдельных букв», сделавший его известным. В книге делла Порта предложил шифр сложной замены собственного изобретения. Делла Порта использовал систему ключевых слов для реализации шифра, который может рассматриваться как усовершенствование шифра Альберти. Одно ключевое слово используется для формирования перестановки алфавита, другое ключевое слово используется, чтобы определить последовательность для нескольких алфавитов. Это техника, была названа им «двойной шифр».

Самым известным криптографом XVI века можно назвать французского дипломата и криптографа Блеза де Виженера. В своём «Трактате о цифрах и тайнописи»1586 года он описал шифр, подобный шифру Тритемия, но с применением ключевого слова, а также предложил и описал шифр с автоключом. По сути в своем труде Виженер объединил подходы Тритемия, Белазо, Альберти и делла Порта не внеся ничего оригинального. Идея

шифрования, заложенная в шифре Виженера, была приписана ему ошибочно в XIX веке. В последующем этот шифр был несколько упрощен для практического использования начальником первого в Германии государственного дешифровального отдела графом Гронсфельдом. Шифр Виженера и шифр Гронсфельда являются по сути дела родоначальниками широко используемого в настоящее время шифра гаммирования применяемого в поточных криптосистемах. Шифр Виженера использовался в различных вариантах вплоть до XIX века. Одним из наиболее известных модификаций шифра Виженера является шифр английского адмирала Бофора. Достоинство шифра Бофора заключается в том, что правило зашифрования сообщений и их расшифрования совпадают. Астрологические увлечения Виженера привели его к идее шифра, в котором шифрзнаки представляют собой положения планет в момент шифрования. Идея такого шифра не получила дальнейшего распространения.

В XVII веке английский философ и ученый, лорд-канцлер Френсис Бэкон выдвинул главные требования к шифрам: «*Они не должны поддаваться дешифрованию, не должны требовать много времени для написания и чтения, не должны возбуждать никаких подозрений*». Эти требования актуальны и сегодня.Френсис Бэкон предложил оригинальную систему шифрования, основу которой составляет двоичное кодирование. Однако, шифр изобретенный Френсисом Бэконом был сложным и не получил распространения. Френсис Бэкон одним из первых понял всю глубину негативных последствий ошибок при шифровании – «*в результате неловкости и не искусности тех рук, через которые проходят величайшие секреты, эти секреты во многих случаях оказываются облеченными слабейшими шифрами*».

Письма зашифровывали не только короли и высшие сановники, но и представители католических орденов и отдельные личности. Свой шифр имел завоеватель Мексики Эрнан Кортес, он использовал комбинированный шифр с подстановкой омофонови кодированием, а также шифр номенклатор. **Омофоны** - фонетическаядвусмысленность, слова, которыезвучатодинаково, нопишутсяпо-разному и имеют разное значение. Например, плод - плот, бал - балл, кот - код и т.д.Уникальный слоговой шифр иезуитов использован в«Тетради Бласа Валера»(Перу, г.Куско,1616). Одновременно в документе содержится дешифровка инкских кипу, юпаны (счетные устройства инков), знаков токапу (одеяние инков)и секес (воображаемые векторы, исходившие из храма Кориканча в Кусково все стороны Империи Инков), во многом послуживших основой для создания шифра.

Эпоха Нового времени или Просвещения - одна из ключевых эпох в истории европейской культуры, связанная с развитием научной,философскойи общественной мысли. Особенно влиятельными были французские просветители, ставшие «властителями дум».Широкое развитие криптографии в

эпоху Просвещения было связано в развитие естественных наук, математики. В это же время в Европе появляются первые специальные органы дипломатической службы, которые занимались вопросами шифрования собственной корреспонденции и дешифрования перехваченной корреспонденции.

XVII-XVIII века вошли в историю криптографии как эра «черных кабинетов». **«Черные кабинеты»** - специальный государственный орган по перехвату, перлюстрации и дешифрованию переписки, в первую очередь дипломатической. В штат «черных кабинетов» (обычно тайная комната в почтовом отделении) входили дешифровальщики, агенты по перехвату почты, писцы-копировальщики, переводчики, специалисты по подделке печатей, химики, специалисты по подделке почерков и т.д. Эти специалисты ценились весьма высоко и находились под особым покровительством властей, предательство очень сурово наказывалось.

Первая организация под наименованием «чёрный кабинет» появилась во Франции XVII века, а система действительно массовой перлюстрации корреспонденции была организована во Франции во время правления Людовика XV. В XVIII веке «чёрные кабинеты» стали распространенным явлением в Европе.

Начальником «Счетной части», т.е. дешифровального отделения во Франции был вдающийся криптограф Антуан Россиньоль. Во время осады Ла-Рошели в 1628 году Россиньоль успешно взломал шифр переписки гугенотов. Талантливый дешифровщик привлёк к себе внимание первого министраЛюдовика XIII,кардинала Ришелье, который активно использовал шифры для своей дипломатической и разведывательной переписки. Россиньоль являлся первым профессиональным криптоаналитиком Франции. На смертном одреЛюдовик XIIIназвал его «*человеком, от которого зависит благополучие моих подданных*».

Во время правления Людовика XIV Антуан Россиньоль и его сын, Бонавентур Россиньоль, работали в своем имении в Жюсви-сюр-Орж, расположенном неподалеку от королевской резиденции в Версале. Они разработали для короля так называемый **Великий шифр**, который был настолько стойким, что в течение двух столетий никто не мог взломать его, пока это не сделал Этьен Базери в 1893 году, после трёх лет работы. Великий шифр, использовал 587 различных чисел. Этьен Базери понял, что каждое число

замещало французский слог, а не одну букву, как до этого считали. Этьен Базери предположил, что специфическая последовательность повторных чисел 124-22-125-46-345 кодирует слово «lesennemis» (враги), и, отталкиваясь от этой информации, смог распутать весь шифр. После того как этот шифр перестал использоваться, французские архивы были закрытыми еще в течение нескольких сотен лет.

После назначения маркиза Лувуа военным министром в 1668 году, во Франции был создан первый «чёрный кабинет», где Россиньоль работал вместе с сыном. Французский «черный кабинет» пользовался известностью во всём мире. Авторитет Россиньоля во Франции был чрезвычайно высок, аббат де Буаробер написал в его честь поэму «EpistresenVers», а Шарль Перро включил его биографию в книгу «Знаменитые люди Франции».

Антуану Россиньолю принадлежит доктрина, согласно которой стойкость шифра должна определяться видом зашифрованной информации. Для военного времени достаточной будет являться стойкость, если сообщение с приказом армейскому подразделению не будет расшифровано противником хотя бы до момента исполнения получателем, а для дипломатической почты шифр должен обеспечивать сохранность на десятки лет.

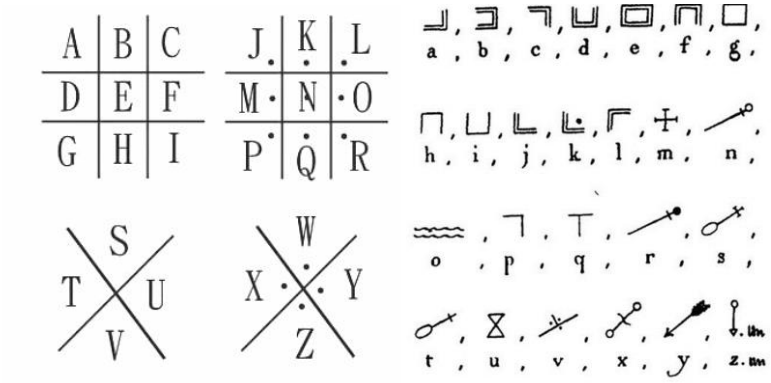
Бурные политические события середины XIX века и развитие гражданского общества привели к ограничению власти европейских правительств и секретных органов надзора. В июне 1844 года английское правительство объявило о прекращении перехвата переписки, в 1848 году закрылись австрийский и французский «чёрные кабинеты». Однако фактически, в той или иной форме, службы перлюстрации и дешифровки переписки существовали и позже, существуют и поныне, несмотря на принятые законы о тайне переписки.

Не только государственные деятели, но и различные тайные общества использовали секретные шифры. Широко использовали шифры братства «вольных каменщиков» (масонов) и другие тайные общества, которые стали появляться в Западной Европе в XVII веке. **Шифр «вольных каменщиков»** является шифром замены и вопреки распространенному мнению не является стойким, но представляет определенный интерес. Внешне в своем большинстве шифры «вольных каменщиков» выглядели как шифры простой замены, где буквы алфавита заменялись особыми геометрическими фигурами, графемами - «гиероглифами» по терминологии того времени. Шифрование заключается в замене букв открытого текста символами по таблице:

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

Например, APPLE соответствует криптограмме:

Существовали и другие способы формирования таблиц замены.



При походе на Россию Наполеон использовал шифр «вольных каменщиков» в низших звеньях своей связи, однако шифр достаточно быстро был раскрыт русскими дешифровальщиками.

Масоны предложили классифицировать шифры. Их вариант классификации заключается в следующем.

Буквенный шифр – шифры простой замены, перестановки, реализующие побуквенное преобразование открытого сообщения.

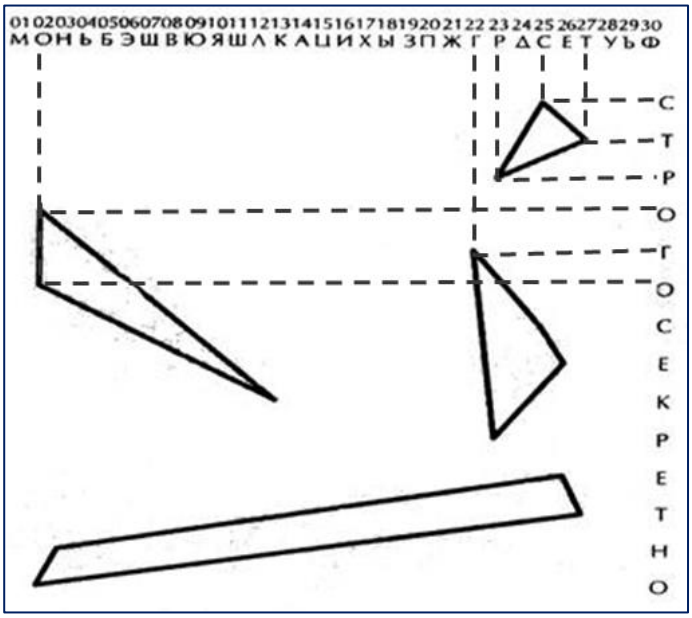
Картинный шифр – сокрытие информации в картинах или рисунках.

Акроматический шифр – сокрытие информации в притчах, аллегориях и т.д.

Нумерический шифр – шифры, осуществляющие замену букв, слов или целых фраз цифрами. К этим шифрам относятся и книжные шифры.

Музыкальный шифр – сообщение представляется в виде музыкальной мелодии.

Кодовый шифр – сообщение кодируется, например терминами из биологии или химии. Криптограмма часто представляет собой осмысленный текст.



Геометрический шифр - сокрытие информации в геометрических фигурах.

Британский философ и лингвист, один из основателей Лондонского Королевского общества Джон Уилкинс (1614-1672) увлекался криптографией и разработал ряд шифров, в том числе геометрический и музыкальный шифры.

Музыкальный шифр не нашел широкого применения, т.к. предполагал определенную музыкальную подготовку шифровальщика.

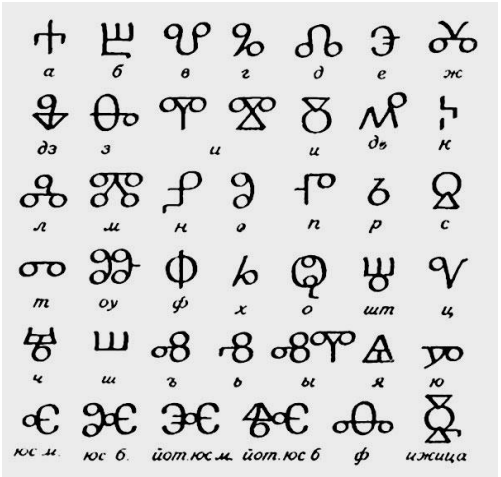
Геометрический шифр Уилкинсона носит элементы, как криптографии, так и стеганографии.

Традиции русской криптографии (тайнописи) уходят своими корнями в раннее средневековье. Подобно другим древним и всем славянским

письменностям, уже древнерусская письменность обладала этим особым применением. Термин «тайнопись» получил распространение в славянской научной литературе в XIX веке. В более раннее время одного общего названия для тайнописи, по-видимому, не существовало, отдельные ее виды имели свои особые названия. Тайнопись становится довольно распространенным явлением в древнерусских рукописных памятниках в XIV веке. Обычное место тайных надписей или записей в рукописях - в виде послесловий или приписок на особых местах - в основном, в начале или конце рукописи, часто на внутренней стороне переплета.

Уже в середине XIX века многие отечественные ученые-филологи начали проявлять в той или иной степени интерес к вопросам тайнописания в южнославянских и русских рукописях. Наиболее глубоко исследовал эту проблему академик М.Н. Сперанский. В своем фундаментальном труде «Тайнопись в югославянских и русских памятниках письма», созданном на базе скрупулезного изучения многочисленных рукописных памятников, находившихся не только в России, но и в многочисленных европейских книгохранилищах, автор детально описал ряд систем славянской и русской тайнописи.

На Руси всякое тайное послание называлось **тарабарской грамотой**, или **тарабарщиной**. Существовал и особый язык для устной передачи сообщения, тоже называемый **тарабарским языком**. Доподлинно не известно, какая из первых систем тайнописи стала носить название тарабарской грамоты. Одна из таких первых систем шифрования заключается в следующем. Например, пусть открытое сообщение представляет собой слово ТАЙНОПИСЬ. Слово делили на биграммы (или слоги) и искажали при написании добавлением ТАРА и БАРА. В этом случае получается – ТАРАТАБАРАЙНТАРАОПБАРАИСЬ. Достаточно вычеркнуть из послания ТАРА и БАРА и получиться открытое сообщение.



Наиболее ранней из известных по древнерусским памятникам письменности систем тайнописи является **система «иных письмен»**. В этом виде тайнописи буквы кирилловского алфавита заменяются буквами других алфавитов: глаголицы, греческого, латинского, пермской азбуки. В употреблении глаголицы в качестве тайнописи хронологически следует различать два периода: древнейший (XI-XIII века), когда глаголицей в кириллическом тексте пишут только отдельные буквы и слова, и позднейший (XV-XVI века), когда глаголицей пишутся целые фразы. Глаголицу древнерусские писцы хорошо знали, они ее умели читать и копировали в своих текстах, чему есть множество примеров. Поэтому в древнейший период глаголица не была на Руси чем-то особенным, и употребление ее в кириллических текстах, вероятно, лишь отражает стремление писца обратить особое внимание на какое-то место в

тексте. Но к концу XV в. глаголица была уже на Руси основательно забыта и в рукописях использовалась исключительно как тайнопись.

Употребление греческой тайнописи связывают с определенной модой, которая прошла к концу XVI в. Появление же этого способа тайнописи было обусловлено оживлением начавшихся с конца XIV в сношений Московской Руси с греками.

Употребление латинской азбуки в качестве тайнописи относится к более позднему времени и обусловлено усилившимся западноевропейским влиянием. В распространении этого вида тайнописи, встречающегося в рукописях начала XVI века и вплоть до конца XVII века, вероятно, известную роль играла школа с ее латинским языком преподавания.

Несколько обособленное место среди других алфавитов в применении к тайнописи занимает пермская азбука (**абур**). Изобретенная, по преданию, просветителем зырян епископом пермским Стефаном, создавшим ее на основах современного кирилловского, греческого алфавитов и пермских рун, азбука эта не прижилась на практике и уже в XV в., как малоизвестная, получила значение тайнописи. Но и в этом качестве она не была широко распространена.

Второй после системы «иных письмен» системой тайнописи, известной по русским рукописным памятникам, является **система «измененных знаков»,** зафиксированная уже в XIV веке. Выделяют две ее разновидности:

а) систему знаков, измененных «путем прибавок» к обычным начертаниям;

б) построенную на принципе, сходном с греческой тахиграфией, когда вместо буквы пишется лишь часть ее.

Первую разновидность такой тайнописи М. Н. Сперанский открыл в Смоленской Псалтыри 1395 г. По свидетельству ученого, эта Псалтырь Онежского Крестного монастыря хранилась в свое время в Архангельском местном отделении Церковно-Археологического комитета. Ее писец, смолянин инок Лука, прекрасно владевший искусством письма, владел и тайнописью.

Присматриваясь к манере изменения обычных письменных знаков, можно выделить такие характерные приемы, как:

- перевороты букв;
- деформация букв;
- урезка части букв;
- использование особых начертаний.

Распространение на Руси получила **полусловица** - система тайнописи, основу которой составляет система упрощенного, более сокращенного и более быстрого письма. Характерные построения знаков полусловицы:

- вместо целой буквы пишется ее характерная часть, т.о. чтобы разные буквы не совпадали своими знаками;

- знаки переворачиваются в обратную сторону;

- используются знаки, полученные деформацией исходных букв.

Вариантом полусловицы являлась **гласная полусловица** - разновидность тайнописи, в которой сокращению подлежат только гласные буквы, а согласные остаются на своих местах без изменения.

Цифровая система тайнописи или, как ее еще называют, «счетная» или «цифирная», основанная на употреблении букв в качестве цифр и на различных действиях с ними, является весьма распространенной на Руси и притом с довольно раннего времени. **Простая цифровая тайнопись** состоит в том, что для каждой цифры-буквы, соответствующей желательной в обычном письме букве, дается два или несколько большей частью одинаковых слагаемых. Таким образом, чтобы получить нужную букву, надо произвести сложение, а полученная сумма, изображенная соответствующей цифрой-буквой, и будет искомой буквой. Реже сумма слагается из различных цифр-букв, причем каждая группа цифр-слагаемых отделяется каким-либо знаком или пробелом от соседних. Буквы, не имеющие цифрового значения, остаются неизменными. Старейший образец тайнописи находится в псковском Апостоле 1307 г. Такая система тайнописи была популярна на Руси долгое время, вплоть доXVII века. Именно отсюда она проникла на славянский юг. Однако само появление цифровой системы тайнописи у славян следует поставить в зависимость от Византии, где она была известна уже в VII-VIII вв.

Греческим по происхождению является и **описательный вид цифровой тайнописи**. Примером ее может служить тайнописный текст из рукописного собрания Кирилло-Белозерского монастыря XV в.: «*Аще хощеши увъдати имя писавшаго книгу сию, и то ти написую: «Десятерица сугубая (10+10=20) и пятерица четверицею (5×4 = 20, сумма 40) и единъ (1); десятерица дващи (10×2 = 20) и един (1); десятья четыре сугубо и четырежди по пяти (10×2×4 + 4×5 = 100); дващи два съединемъ (2×2 + 1 = 5); единица четверицею сугубо (1×4×2 = 8); в семъ имени словъ седмерица, три столпы и три души, царь. И всего же числа в семъ имени РОЕ (175)*». В результате расшифрования получим имя - Макарей (сумма букв-цифр действительно 175 и семь букв, из которых три гласные и три согласные и одна (й) полугласная).

Арабские числа стали использоваться в качестве тайнописи лишь с того времени, как они начали входить в употребление в русской письменности, т.е. со второй половины XVI в. на русском юго-западе и с начала XVII в. на северо-востоке.

Следующая система тайнописи, которая использовалась писцами в русских рукописях - это **«система замен»**. Выделяют два вида для такой тайнописи: «простую литорею» (т. е. простое риторское письмо) и «мудрую литорею», а также как вариант этой последней - тайнопись «в квадратах».

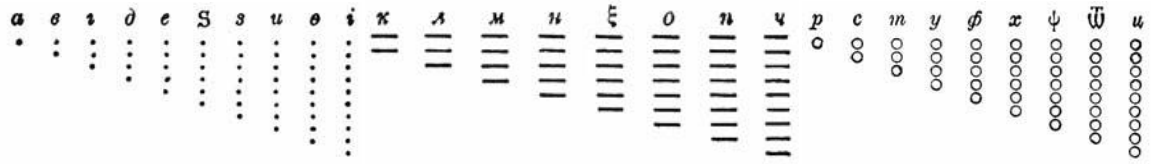
«Простая литорея», особенно часто встречаемая, весьма не сложна. Она состоит в том, что каждая из десяти по порядку азбуки согласных, поставленных в одном ряду, при письме литореей заменяется соответствующей

ей буквой во втором таком же ряду, состоящем из остальных десяти согласных, идущих в обратном (справа налево) порядке и обратно; гласные и бывшие редуцированные **ъ, ь** остаются на своих местах, греческие буквы, как известно, также входившие в состав кириллицы, исключены и заменяются созвучными. Ключ к «простой литорее» представлял собой таблицу:

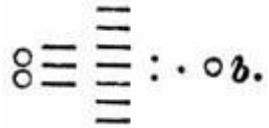
Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Слово ЯБЛОКО будет зашифровано как ЯЩСОТО. Шифр относится к шифрам простой замены.Старейший образец этого вида тайнописи представлен в Шенкурском Прологе 1229 г., принадлежавшем в свое время профессору Московского университета Баузе и сгоревшем в Москве во время пожара 1812г. По-настоящему распространен этот вид тайнописи был в XIV-XV веках и поэтому весьма вероятно, что приписка тайнописью была сделана в древней рукописи позднее. Мода же на этот вид тайнописи не прекращалась до XVIII века включительно.

«Мудрая литорея» представляет собой шифр простой замены. «Мудрая литорея» просуществовала на Руси вплоть до XIX века. 30 букв алфавита делили на три равные части, по 10 букв в каждой. В пределах первого десятка буквы последовательно обозначали точками, второго десятка - черточками, а третьего – кружочками или крестиками.



Тогда слово СЛОВАРЬ будет представлено криптограммой:



К этому же виду тайнописи относится использовавшаяся в XVI-XVII веках **тайнопись «в квадратах»**, где таблицы замены букв выписывались в виде квадратов.

Еще одной системой тайнописи на Руси была **система нарочито придуманных знаков**. В этой системе осуществлялась замена букв открытого текста на специально придуманные обозначения.

Подобные тайнописи создавались боярами и государственными деятелями для шифрования своей переписки.

Практиковалось также видоизменение знаков письма,которое получило название **«вязь».** Надо отметить,что подобные системы шифрования нередко сочетали в себе криптографию и

стеганографию.Причудливые завитушки,вязь,различные выдуманные знаки противник мог принять за бессмысленные каракули, рисунки и др.,а никак не за осмысленный текст.

На рисунке приведен пример записи вязью православной молитвы Пресвятой Богородице «*Достоино есть яко воистину блъжъти Тя, Богородицу, Присноблаженую и Пренепорочную и Матерь Бога нашего. Честнъишую Херувимъ и славнъишую без сравнения Серафимъ, без истлъния Бога Слова рождшую, сущую Богородицу Тявъличаемъ*».

Тайнопись использовалась для написания текстов на русских знаменах и на колоколах.

Появление в России первых профессиональных криптографов, находящихся на государственной службе, следует отнести к 1549 г., к моменту образования Посольского приказа, осуществлявшего общее руководство внешней политикой страны. Кроме того, Приказ ведал выкупом и обменом пленными, управлял рядом территорий на Юго-Востоке страны и некоторыми категориями служилых людей. Вся эта деятельность с необходимостью требовала осуществления довольно интенсивной шифрованной переписки. На службе в Посольском приказе и находились лица, создававшие шифры или, как их называли тогда, «цифири», «цифры» или «азбуки».

В XVII-XIX веках использовались в основном шифры сложной замены и перестановки, тексты, подлежащие зашифрованию, писались на разных языках. В различных шифрах шифрвеличинами выступали отдельные буквы, слова и стандартные выражения. В качестве шифробозначений использовались элементы, как правило, специально составлявшихся с этой целью алфавитов, которые могли представлять собой буквы кириллицы, латиницы, других азбук, цифры, особые значки. К этим последним относятся символы планет, одновременно являвшиеся и символами металлов. В шифрах рассматриваемого периода широко используются «пустышки» - шифробозначения, которым не соответствует никакого знака открытого текста. Введение «пустышек» в шифртекст разбивает структурные лингвистические связи открытого текста и, в определенной мере, изменяют статистические закономерности, то есть именно те особенности текста, которые используют, в первую очередь, при частотном криптоанализе.

Высокая активность государств в XVII-XIX веках во всех сферах деятельности - политической, военной, экономической, дипломатической и других породила появление отдельных криптографических служб в составе государственных органов. Криптографические службы постоянно разрабатывали новые шифры, эта работа не прекращалась не на минуту, к

работе в криптографических службах часто привлекали выдающихся ученых математиков, физиков, химиков.

В XIX веке появляются первые механические шифровальные устройства. Наиболее известными являются изобретения полковника американской армии Д. Уодсворта и английского инженера Ч. Уитстона. Устройство Уодсворта (1817 г.) представляло механический шифратор основными элементами которого были два шифровальных диска, на торце одного располагались буквы английского алфавита, а на торце второго буквы и цифры от 2 до 8.

Литеры на втором диске били съемные, что позволяло менять алфавит шифрованного текста. Диски помещались в футляр с прорезанными в нем окнами. При вращении первого диска в верхнем окне выставлялась буква открытого сообщения. Диски были соединены шестеренчатой передачей, поэтому в нижнем окне появлялась соответствующая буква шифртекста. Устройство было снабжено специальной кнопкой для разъединения дисков. Это требовалось для того, чтобы обеспечивать установку устройства в заданное начальное положение. В устройстве Уодсворта просматриваются идеи Альберти, Тритемия, Виженера. Несмотря на то, что устройство было достаточно громоздким, к тому же в это время господствовали «ручные» шифры, которые не требовали специальных приспособлений, оно послужило толчком к развитию механических устройств для шифрования сообщений.

Интересное предложение по созданию механического устройства шифрования сделал Ч. Уитстон во второй половине XIX века. В устройстве Уитстона просматриваются идеи Альберти, а также Уодсворта. Внешне устройство Уитстона напоминает диск Альберти, однако в нем реализована парадоксальная идея – алфавит открытого текста содержит большее количество знаков, чем шифрованного. Проблема неоднозначности в определении букв открытого сообщения решена Уитстоном блестяще.

Внешний диск, диск алфавита открытого текста, состоял из 27 знаков (26 букв английского алфавита и специального знака "+", означающего пробел). Внутренний алфавит определяет алфавит открытого текста и состоит из обычных 26 букв, расположенных в произвольном ключевом порядке. На той же оси, что и диски (алфавиты) устройства, соединенные шестернями размером 27×26 соответственно, расположены две стрелки, как в современных часах.

В начале шифрования большая (длинная) стрелка указывает на знак "+". Малая стрелка, связанная с большой резьбовой шестеренкой, ставилась в то же положение, т.е. "часы" показывали "12.00". Набор букв открытого текста производился поворотом большой стрелки по направлению движения часовой. После такого поворота малая стрелка указывает знак шифрованного текста. Таким образом, при полном повороте большого диска малый диск смещался на единицу по отношению к исходному взаимному состоянию двух дисков, что приводило к сдвиговому изменению алфавита шифрованного текста по отношению к алфавиту открытого текста. По окончании каждого слова большая стрелка становилась на знак "+", буква, на которую при этом указывала короткая стрелка, записывалась как знак шифрованного текста. Во избежание неоднозначности расшифрования, удвоение букв в открытом тексте не допускается. Повторную букву следует либо пропустить, либо ставить вместо нее какую-нибудь редкую букву, напримерQ. Например, словоTHE APPLE при шифровании записывается как +THE+APLE+ или +THE+APQLE+.

Изобретение Уитстона, также как и Уодсворта, не нашло широкого применения. Однако судьба другого его предложения в области криптографии - шифра биграммной замены - сложилась лучше, хотя шифр несправедливо был назван именем друга изобретателя барона Плейфера. Вместе с тем, сам Плейфер вел себя весьма корректно: популяризируя изобретение, он всегда указывал имя автора – Уитстона, но история распорядилась иначе: шифру было присвоено имя не изобретателя, а популяризатора.

В начале XX века значительный вклад в развитие криптографии внес американец Г. Вернам. В 1917 году он, будучи сотрудником телеграфной компании, предложил идею автоматического шифрования телеграфных сообщений, суть которой заключается в следующем. Открытый текст представляется в коде Бодо (в виде пятизначных "импульсных комбинаций"). В этом коде, например, буква "А" имела вид (+ + — — —). На бумаге знак "+" означал отверстие, а знак "-" - его отсутствие. При считывании с ленты пятерка металлических щупов "опознавала" отверстия (при

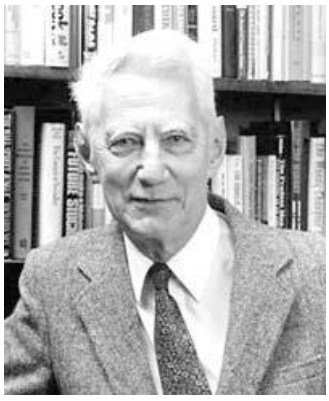
наличии отверстия щуп замыкал электрическую цепь). В линию связи посылались импульсы тока. Вернам предложил электромеханически покоординатно складировать импульсы знаков секретного текста с импульсами секретного ключа, представляющего из себя хаотический набор букв того же самого алфавита. Сложение, по современной терминологии, осуществлялось по модулю 2. Г. Вернам создал устройство, производящее операции шифрования автоматически, без участия шифровальщика, тем самым было положено начало так называемому "линейному шифрованию", когда процессы шифрования и передачи сообщения происходят одновременно. До той поры шифрование было предварительным, поэтому линейное шифрование существенно повышало оперативность связи. Шифр Вернама обладает исключительной криптографической стойкостью. В то же время очевиден и недостаток этой системы шифрования - ключ должна иметь ту же длину, что и открытый текст. Для расшифрования на приемном конце связи туда нужно передать (по тайным, защищенным каналам) ключ достаточной длины. При практической реализации это порождает проблемы, причем весьма существенные, что и предопределило скромное распространение шифров Вернама. Сам Вернам не был математиком-криптографом, тем не менее, он настаивал на том, что ключ шифра не должен повторяться при шифровании, и в этом, как показала история криптографии, он был прав. Его идеи породили новые подходы к надежной защите информации при передаче больших объемов сообщений.

Первая половина XX века стала «золотым веком» электромеханических шифровальных машин. Наибольшую известность получило семейство немецких электромеханических шифровальных машин Enigma. Различные модификации этой шифровальной машины использовались германскими войсками с конца 1923 года вплоть до 1945 года. В 1943 году союзникам по антигитлеровской коалиции удалось «взломать» машину Enigma, что сыграло большую роль в победе во Второй мировой войне. Для передачи наиболее секретных сообщений во время Второй мировой войне немцами использовалась шифровальная машина Lorenz. В американской армии с 1923 по 1943 год использовалась механическое устройство для шифрования М-94. В основу этого устройства положен диск Альберти. Для защиты дипломатической переписки в США использовалась машина ХебернаMarkII. Шведский криптограф Б. Хагелин разработал для французской секретной полиции шифровальное устройство CD-57, а для французских спецслужб – шифровальную машину М-209. Модификация этой машины использовалась также и американскими военными во Второй мировой войне. С 1939 года по 1952 год японцы использовали шифровальную машину для защиты дипломатической переписки под названием «Тип 97» и ее модификацию. В США эти машины получили красочное обозначение «Пурпурный код» и «Красный код». В СССР перед войной и в годы Великой Отечественной войны широко использовалась

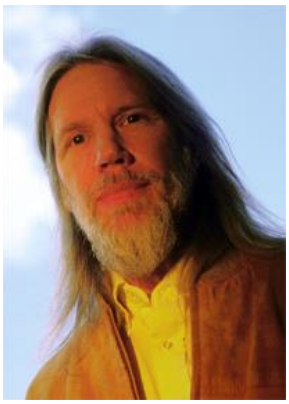
малогабаритная дисковая кодировочная машина К-37 «Кристалл». Только в 1940 году было выпущено 100 комплектов этой машины.

После войны были подведены итоги эксплуатации К-37 и проводилась работа по ее дальнейшему совершенствованию. Самой известной и распространенной советской криптографической машиной стала М-125 «Фиалка» (на фото).

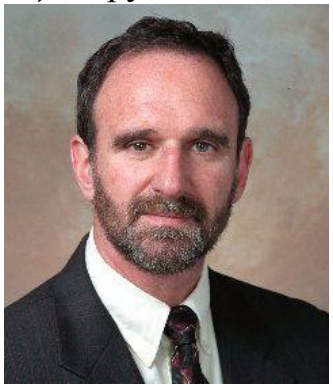
К началу 1930-х годов сформировались разделы математики (теория чисел, теория вероятностей и математическая статистика) являющиеся основой будущей науки – криптологии. Ключевой вехой в развитии криптографии является фундаментальный труд Клода Шеннона «Теория связи в секретных системах», написанный в форме секретного доклада в 1945 году и опубликованный в 1949 году. В этой работе впервые был показан подход к криптографии как к математической науке. В области секретных систем связи и теоретических основ криптографии работал выдающийся советский ученый Владимир Александрович Котельников. Научные труды К. Шеннона и В.А. Котельникова стали теоретической основой современной криптографии.



Развитие во второй половине XX века компьютерной техники и электроники сделало возможным использование более сложных шифров. В 1960-х годах появляются первые блочные шифры, обладающие большей стойкостью, чем электромеханические машины. В 1976 году в США принимается государственный стандарт шифрования – DES (DataEncryptionStandart), являющийся первым в мире открыто опубликованным стандартом шифрования. На основе используемой в системе DES сети Хорста Фейстеля разработаны множество других криптосистем: российский стандарт ГОСТ 28147-89, криптосистема TEA (TinyEncryptionAlgorithm), Twofish, IDEA (InternationalDataEncryptionAlgorithm) и другие.



В 1975 году публикуется работа Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии». Данная работа открыла новую область криптографии, теперь называемую криптографией с открытым ключом или асимметричную криптографию.



Хотя работа У. Диффи и М. Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают криптосистему RSA,

названную по имени авторов - Рона Ривеста, Ади Шамира и Леонарда Адлемана.

С конца 1990-х годов начинается процесс открытого формирования государственных криптографических стандартов. Пожалуй, самым известным является начатый в 1997 году конкурс AES, в результате которого в 2000 году государственным стандартом США для криптографии с секретным ключом был принят шифр Rijndael, сейчас уже более известный как AES.

Также развиваются принципиально новые направления. На стыке квантовой физики и математики развиваются квантовые вычисления и квантовая криптография. Хотя квантовые компьютеры лишь дело будущего, уже сейчас предложены алгоритмы для взлома существующих «надёжных» систем (например, алгоритм Шора).

В современном мире криптография находит множество различных применений. Кроме очевидных - собственно, для передачи секретной информации, она используется в сотовой связи, платном цифровом телевидении, беспроводной связи, на транспорте (например, для защиты билетов от подделок), в банковских операциях, и даже для защиты электронной почты от спама.В современной информационном мери уже трудно найти область, где криптография не использовалась бы.

3. Математические основы современной криптографии

В этом разделе познакомимся с математическими основами современной криптографии. Очевидно, что в рамках настоящей книги невозможно охватить все разделы математики, которые требуется знать криптографу, но попытаемся «приоткрыть дверь» в эту область.

Начнем, пожалуй, с **комбинаторики**, которая требуются для дальнейшего изучения как симметричной, так и асимметричной криптографии. Комбинаторика является самостоятельным разделом высшей математики и по ней написаны увесистые учебники. Однако, нам будет достаточно небольшой доли теоретических знаний из этого раздела математики.

В узком смысле комбинаторика – это подсчет различных комбинаций, которые можно составить из некоторого множествадискретныхобъектов. Под объектами понимаются какие-либо обособленные предметы или живые существа – люди, звери, грибы, растения, насекомые и т.д. В криптографии объектами являются буквы (биграммы, слова и т.д.) открытого текста и криптограммы. Для комбинаторики принципиально важно, что объекты поддаются перечислению и существенно то, что среди них нет одинаковых.

Самыми распространёнными видами комбинаций, которые используются в криптографии, являются перестановки объектов и их выборка из множества. Посмотрим, как это происходит.

Выборки. Если выбор объекта происходит в два этапа и на первом этапе существует n возможностей, а на втором - m возможностей, то итоговое количество вариантов выбора равно $n \cdot m$. Пусть имеется n объектов, и мы

выбираем из них m объектов. Это и есть выборки. Количество выборок зависит от следующих факторов:

- считаем ли мы различными выборки из одинаковых элементов, но идущих в разном порядке (например, «abc» и «cab»);

- возможно ли выбрать уже выбранный элемент повторно (например, в алфавите «abc»с возможностью повторного выбора элементов могут существовать варианты выборки: «aab»,«ccb», «cbb» и т.д.).

Рассмотрим сначала случай, когда элемент не может быть выбран повторно, т.е. случай **выборки без возвращения**.

На первом этапе есть возможность выбрать один элемент из n. Это можно сделать n различными способами. На втором этапе можно выбрать один элемент из оставшихся $n-1$ элементов. На $m-$м этапе можно выбрать из $n-m+1$ оставшихся элементов. Тогда количество всех возможных вариантов находится путем умножения количества вариантов полученных на этапах с 1 по m. Это можно записать формулой:

$$A_n^m = n(n-1)(n-2)...(n-m+1).$$

Например, из 20 символов нужно выбрать пять. Очевидно, что каждый символ может быть выбран не более одного раза. В данном примере $n=20$, $m=5$. Сначала выбираем один символ из 20, потом один символ из 19, далее один из 18 и т.д. Всего возможных вариантов выбора символов.

Теперь рассмотрим случай, когда выборка может содержать какой-либо элемент более одного раза. Это - **выборка с возвращением**. Пусть имеется n-й алфавит. Сколько m-буквенных слов можно получить в этом алфавите. Ответ очевиден - n^m. Например, из пяти первых букв русского алфавита необходимо составить все трехбуквенные слова. Первую букву слова можно выбрать 5-ю способами, вторую тоже 5-ю, третью – 5-ю способами, т.к. буква может быть выбрана повторно. Всего вариантов $5\cdot 5\cdot 5 = 5^3 = 125$.

Перестановки. Часто в алгоритмах шифрования требуется не выбирать какие-то элементы, а просто изменять порядок их следования, например, в шифрах простой перестановки. Перестановка – это выбор n элементов из n возможных, в которой элемент не может быть выбран повторно. Для вычисления возможного количества перестановок используется формула:

$$P_n = A_n^n = n(n-1)(n-2)...(n-n+1) = n!$$

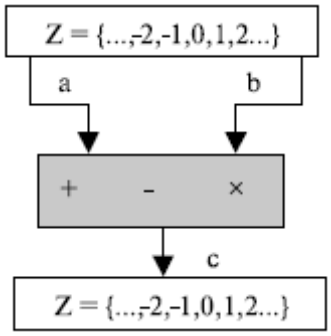
В формуле вводится понятие факториала. Факториал числа – это произведение всех натуральных чисел от 1 до этого числа. Факториал обозначается как $n!$ Факториал нуля равен 1.

Рассмотрим поясняющий пример. Сколько можно получить пятибуквенных слов в алфавите «*абвгд*»? Так как нужно построить пятибуквенное слово, то этапов выбора будет пять. Всего вариантов возможных будет $5\cdot 4\cdot 3\cdot 2\cdot 1 = 5! = 125$.

Помимо комбинаторики криптография опирается на арифметику целых чисел и модульную арифметику.

В арифметике целых чисел мы используем множество целых чисел и несколько операций. Читатель наверняка уже знаком с этим множеством и соответствующими операциями, но мы рассмотрим их, чтобы объяснить потом основы действий со сравнениями по модулю m.

Множество целых чисел, обозначают Z, оно содержит все числа (без дробей) отминус бесконечности до плюс бесконечности.Для криптографии представляет интерес трибинарные.**Бинарные операции**имеют два входа и один выход. Для целых чисел определены три бинарных операции - сложение, вычитаниеиумножение. Каждая из этих операций имеет два входа (**a**и**b**) и выход (**c**), как это показанорисунке. Два входа принимают числа из множества целых чисел; результат операции - число из множества целых чисел.



Обращаем внимание, чтоделениене относится к этой категории операций, потому что этой операции нужны два выхода вместо одного.

В арифметике целых чисел, если *a*делим на*n*, можем получить*q*и*r*. Отношения между этими четырьмя целыми числами можно выразить формулой:

$$a = q \cdot n + r.$$

В этом равенстве a называется делимое q - частное; n – делитель и r - остаток. Обратите внимание, что это – не бинарная операция, поскольку результат деления a на n - это два целых числа, q и r. Мы будем называть этоуравнением деления. Например, предположим, что $a = 225$, = 255, а $n = 23$. Мы можем найти $q = 11$ и $r = 2$, используя алгоритм деления.

Когда мы используем уравнение деления в криптографии, мы налагаем два ограничения. Первое требование: чтобы делитель был положительным целым числом ($n > 0$). Второе требование: чтобы остаток был неотрицательным целым числом ($r > 0$).

Теперь кратко рассмотрим **теорию делимости** - тема, с которой часто сталкиваются в криптографии. Если*a*не равно нулю, а*r*=0, в равенстве деления мы имеем:

$$a = q \cdot n.$$

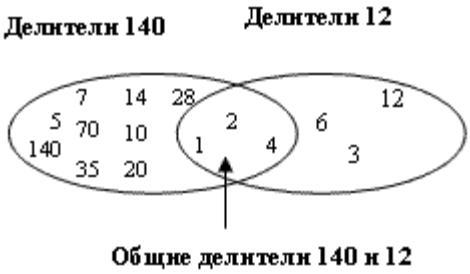
Тогда говорят, что*a*делится на*n*,или, что*a* делится без остатка на*n*. Например, целое число4делит целое число32, потому что $32 = 8 \cdot 4$. Число8не делит число42, потому что $42 = 5 \cdot 8 + 2$.

Положительное целое число может иметь больше чем один делитель. Следует упомянуть о двух интересных свойствах делителей положительных целых чисел.

Свойство 1: целое число1имеет только один делитель - само себя.

Свойство 2: любое положительное целое число имеет по крайней мере два делителя – 1и само себя (но может иметь больше).

Одно целое число, часто необходимое в криптографии, - **наибольший общий делитель**двух положительных целых чисел. Два положительных целых числа могут иметь много общих делителей, но только один наибольший общий делитель. Например, общие делители чисел12и140есть1,2и4. Однако наибольший общий делитель - 4.



Наибольший общий делитель двух положительных целых чисел - наибольшее целое число, которое делит оба целых числа.

Нахождение наибольшего общего делителя (НОД) двух положительных целых чисел путем составления списка всех общих делителей непригодно для достаточно больших чисел.К счастью, больше чем 2000 лет назад математик по имени Евклид разработал алгоритм, который может найти наибольший общий делитель двух положительных целых чисел.Алгоритмоснован на следующих двух фактах:

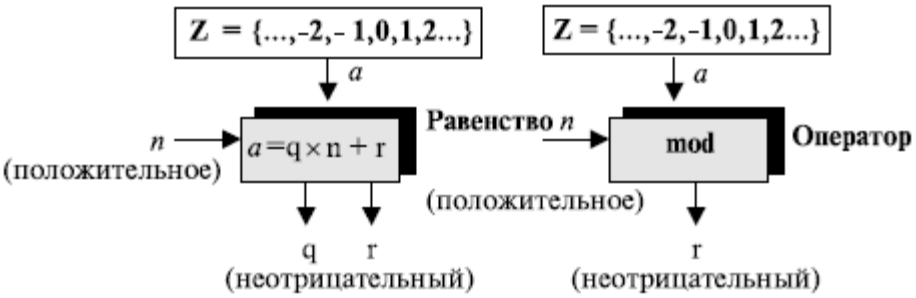
Факт 1:НОД (*a*, 0)=*a*.

Факт 2:НОД (*a*, *b*) = НОД (*b*, *r*), где*r* - остаток от деления*a*на*b*.

Первый факт говорит, что если второе целое число - 0, наибольший общий делитель равен первому числу. Второй факт позволяет нам изменять значение*a*на*b*, пока*b*не станет0. Например, вычисляяНОД (36, 10), мы можем использовать второй факт несколько раз и один раз первый факт, как показано ниже.

НОД(36,10)=НОД(10,6)=НОД(6,4)=НОД(4,2)=НОД(2,0)=2.

Уравнение деления ($a = q \cdot n + r$), рассмотренное ранее, имеет два входа (*a*и*n*) и два выхода (*q*и*r*). В **модульной арифметике** мы интересуемся только одним из выходов – остатком*r*. Другими словами, когда мы делим*a*на*n*, мы интересуемся только тем, чтозначение остатка равно*r*. Это подразумевает, что мы можем представить изображение вышеупомянутого уравнения как бинарный оператор с двумя входами ***a*** и ***n*** и одним выходом ***r***. Вышеупомянутый *бинарный оператор* назван **оператором по модулю** и обозначается как mod. Второй вход (*n*) назван**модулем**. Вывод *r* назван **вычетом**.



Как показано, оператор по модулю (mod) выбирает целое число (a) из множестваZи положительный модуль (n). Оператор определяет неотрицательный остаток (r).Мы можем сказать, что:

$$a \bmod n = r .$$

Например, разделим 27 на 5, результатом будем r=2. Это означает, что $27 \bmod 5 = 2$.

Результат операции по модулюn - всегда целое число между0иn-1. Другими словами, результат$a \bmod n$ - всегда неотрицательное целое число, меньшее, чемn. Мы можем сказать, что операция по модулю создает набор, который в модульной арифметике можно понимать как **систему наименьших вычетов по модулю n**, или Z_n. Однако мы должны помнить, что хотя существует только одно множество целых чисел (Z), мы имеем бесконечное число множеств вычетов (Z_n), но лишь одно для каждого значениян.

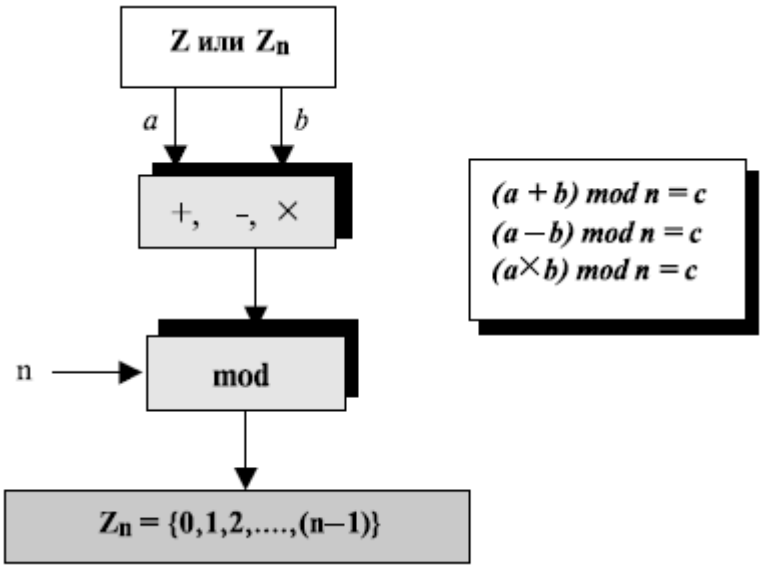
$$Z_n = \{0,1,2,3,\ldots..,(n-1)\}$$

$Z_2 = \{0,1\}$ $Z_6 = \{0,1,2,3,4,5\}$ $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$

В криптографии часто используется понятие**сравнения**вместо равенства. Отображение Z в Z_n не отображаются «один в один». Бесконечные элементы множестваZмогут быть отображены одним элементом Z_n. Например, результат 2mod10=2,12mod10=2,22mod10=2, и так далее. В модульной арифметике целые числа, подобные2,12, и22, называются сравнимыми по модулю10 (mod10). Для того чтобы указать, что два целых числа сравнимы, мы используемоператор сравнения:

$$2 \equiv 12 \bmod 10 \quad 13 \equiv 23 \bmod 10$$

Трибинарных операции(сложение, вычитаниеиумножение), которые мы обсуждали дляZ, могут также быть определены для набора Z_n. Результат, возможно, должен быть отображен в Z_n с использованием операции по модулю, как это показано на рисунке.



Фактически в криптографии применяются два набора операторов: первый набор - один избинарных операторов (сложение, вычитание и умножение); второй - операторы по модулю.

Когда мы работаем в модульной арифметике, нам часто нужно найти операцию, которая позволяет вычислить величину, обратную заданному числу. Мы обычно ищем**аддитивную инверсию**(оператор, обратный сложению) или**мультипликативную инверсию**(оператор, обратный умножению).

В Z_n два числа *a*и *b* **аддитивно инверсны** друг другу, если $b=n-a$. Например, аддитивная инверсия 4 в Z_{10} равна 10-4=6. В модульной арифметике каждое целое число имеет аддитивную инверсию. Сумма целого числа и его аддитивной инверсии сравнима с 0 по модулю *n*. Обратите внимание, что в модульной арифметике каждое число имеет аддитивную инверсию, и эта инверсия уникальна; каждое число имеет одну и только одну аддитивную инверсию. Однако инверсия числа может быть непосредственно тем же самым числом.

В Z_n два числа *a* и *b* мультипликативно инверсны друг другу, если $a \cdot b \equiv 1 \bmod n$ Например, если модуль равен10, то мультипликативная инверсия3есть7. В модульной арифметике целое число может или не может иметь мультипликативную инверсию. Целое число и его мультипликативная инверсия сравнимы с1по модулю *n*. Может быть доказано, что *a* имеет мультипликативную инверсию в Z_n, если только НОД(*n*, *a*) = 1. В этом случае говорят, что *a* и *n* **взаимно простые**.

В криптографии должны обрабатывать матрицы. Хотя эта тема принадлежит высшей математике, которая называется линейной алгеброй, необходим краткий обзор матриц для понимания ряда алгоритмов шифрования.

Матрица - прямоугольный массив, содержащий $l \times m$ элементов, в которых l - число строк, m - число столбцов. Матрица обычно обозначается заглавной буквой, такой, как **A**. Элемент a_{ij} расположен в i -той строке и j -том столбце. Хотя элементы матрицы могут быть любым множеством чисел, мы обсуждаем только матрицы с элементами в Z.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & & & \\ a_{l1} & a_{l2} & \dots & a_{lm} \end{pmatrix}$$

Если матрица имеет только одну строку (l=1), она называется **матрицей-строкой**; если она имеет только один столбец (m=1), то называется **матрицей-столбцом**. Матрица называется квадратной, если число строк равно числу столбцов ($l = m$) и содержит элементы a_{11}, a_{22}, ……, a_{mm}. Матрица обозначается **0**, если все строки и все столбцы содержат нули. **Единичная матрица**, обозначаемая как **I**, - квадратная и содержит все единицы на главной диагонали и все нули на других местах.

В линейной алгебре для матриц определены одно уравнение (равенство) и четыре операции (сложение, вычитание, умножение и скалярное умножение).

Равенство. Две матрицы равны, если они имеют одинаковое число строк и столбцов и соответствующие элементы равны. **Другими словами**, A = B, если мы имеем $a_{ij} = b_{ij}$ для всех i и j.

Сложение и вычитание. Операция сложения двух матриц может применяться, если матрицы имеют одинаковое число столбцов и строк. Сложение записывают как C =A + B. В этом случае полученная в результате матрица C имеет тот же самый номер строк и столбцов, как A или B. Каждый элемент C - это сумма двух соответствующих элементов A и B: $a_{ij} + b_{ij}$.

Операция вычитания производится аналогично сложению, за исключением того, что каждый элемент B вычитается из соответствующего элемента A: $d_{ij}= a_{ij} – b_{ij}$.Ниже показан пример сложения и вычитания.

$$\begin{pmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{pmatrix} = \begin{pmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{pmatrix} + \begin{pmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{pmatrix}$$

$$\begin{pmatrix} -2 & 0 & -2 \\ -5 & -8 & -10 \end{pmatrix} = \begin{pmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{pmatrix} - \begin{pmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{pmatrix}$$

Умножение. Две матрицы различного размера могут быть перемножены, если число столбцов первой матрицы совпадает с числом строк второй матрицы. ЕслиA - матрица размера 1×m, а матрица B размера m×p, то произведением будет матрицаCразмером 1×p. Если элемент матрицы A обозначить a_{ij}, а каждый элемент матрицы B обозначить b_{jk}, то элемент c_{ik} вычисляется следующим образом:

$$c_{ik} = \Sigma a_{ij} x b_{jk} = a_{i11j} + a_{i2} x b_{2j} + \ldots + a_{im} x b_{mj}$$

Пример умножения матрицы-строки на матрицу-столбец:

Пример умножения произвольных матриц:

$$\underset{\mathbf{C}}{\begin{pmatrix} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{pmatrix}} = \underset{\mathbf{A}}{\begin{pmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{pmatrix}} \times \underset{\mathbf{B}}{\begin{pmatrix} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{pmatrix}}$$

Скалярное умножение. Мы можем также умножить матрицу на число (называемое**скаляр**). Если A – матрицаn×m и *x* - скаляр, то C=*x*A – матрицаn×m:

$$\underset{\mathbf{B}}{\begin{pmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{pmatrix}} = 3 \times \underset{\mathbf{A}}{\begin{pmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{pmatrix}}$$

Матрицы имеют аддитивные и мультипликативные *инверсии*. Аддитивная *инверсия* матрицы - это другая матрица B, такая, чтоA+B=0. Обычно аддитивная *инверсия* A обозначается как (-A). Мультипликативная *инверсия* определена только для квадратных матриц. Мультипликативная *инверсия* квадратной матрицы A - квадратная матрица B, такая, что их произведение представляет собой единичную матрицу. Обычно мультипликативная *инверсия* обозначается как A^{-1}.

Матрицы вычетов. Криптография использует матрицы вычетов: матрицы могут содержать все элементы из Z_n. Все операции на матрицах вычетов выполняются так же, как и на матрицах целых чисел, за исключением того, что операции производятся в модульной арифметике.

Криптография с открытым ключом, предложенная в работах Диффи и Хеллмана основана на идеи использования для криптопреобразований односторонней функции.

Пусть дана функция $y = f(x)$, определенная на множестве $X, x \in X$, для которой существует обратная функция $x = f^{-1}(y)$. Функция называется **односторонней**, если вычисление значения функции является сравнительно простой задачей, требующей немного времени, а вычисление значения аргумента по известному значению функции – задача сложная, требующая привлечения массы вычислительных ресурсов, например 10^6-10^9 лет работы мощного компьютера. Данное определение, конечно, не является математически строгим, но достаточно для понимания сути. Собственно односторонняя функция в криптографии не используется. Применяется **односторонняя функция с секретом** (односторонняя функция с «лазейкой», односторонняя функция с «ловушкой»). Применение односторонней функции с секретом в криптографии позволяет:

1) организовать обмен шифрованными сообщениями с использованием только открытых каналов связи, то есть отказаться от секретных каналов связи для предварительного обмена ключами;

2) включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить стойкость шифра;

3) решать новые криптографические задачи (электронная подпись, аутентифицированное распределение ключей и др.).

В качестве односторонней функции в современных системах шифрования с открытым ключом используются следующие функции.

Дискретное экспоненцирование и логарифмирование. Пусть

$$y = a^x \bmod p,$$

где p - некоторое простое число, а $x \in \{1,2,..., p-1\}$. Обратная функция обозначается:

$$x = \log_a y \bmod p,$$

и называется **дискретным логарифмом.**

Операция дискретного экспоненцирования занимает у современного компьютера около $6 \cdot 10^{-12}$ секунд, а операция вычисления дискретного логарифма занимает 10^{31} секунд $\approx 10^{22}$ лет (количество операций $\approx 10^{45}$).

Умножение и факторизация. Другим примером односторонней функции является задача факторизации. Существо ее базируется на двух фактах из теории чисел:

1) задача проверки чисел на простоту является сравнительно легкой;

2) задача разложения чисел вида:

$$n = pq,$$

является очень трудновыполнимой, если известно только n, а p и q - большие простые числа.

Возведение в квадрат и извлечение квадратного корня по модулю. Пусть x и N два целых числа, причем $N = pq$, а p и q - простые числа. Тогда прямая функция вычисляется по формуле:

$$y = x^2 \bmod N.$$

Обратная функция представляет собой операцию вычисления квадратного корня по $\bmod N$. Эта операция вычислительно сложна, как и задача факторизации.

В заключении этого главы хочется сказать еще об одной очень важно задаче – **задаче построения ключей алгоритма шифрования**. Ключ, как было показано выше, представляет собой произвольный набор символов из конкретного алфавита, длина которого определяется алгоритмом шифрования. Построения стойкого ключа - дело трудоемкое. Время «жизни» ключа для современных систем шифрования определяется времени зашифрования и расшифрования. Другими словами ключ является одноразовым, иначе возникает опасность, что противник «взломает» шифр и получит доступ к защищаемой информации. Криптографы давно заметили, что безопасность передаваемой информации определяется в первую очередь ключом. Клод Шеннон в своих работах определил принцип в соответствии с которым алгоритм шифрования не должен быть секретным, секретным параметром должен быть только ключ. Поэтому главная задача криптоаналитика – определить ключ шифра.

Для оценки стойкости шифра в первую очередь необходимо определить, основываясь на длине ключа, сколько времени потребуется противнику для перебора возможных вариантов ключей для взлома шифра.

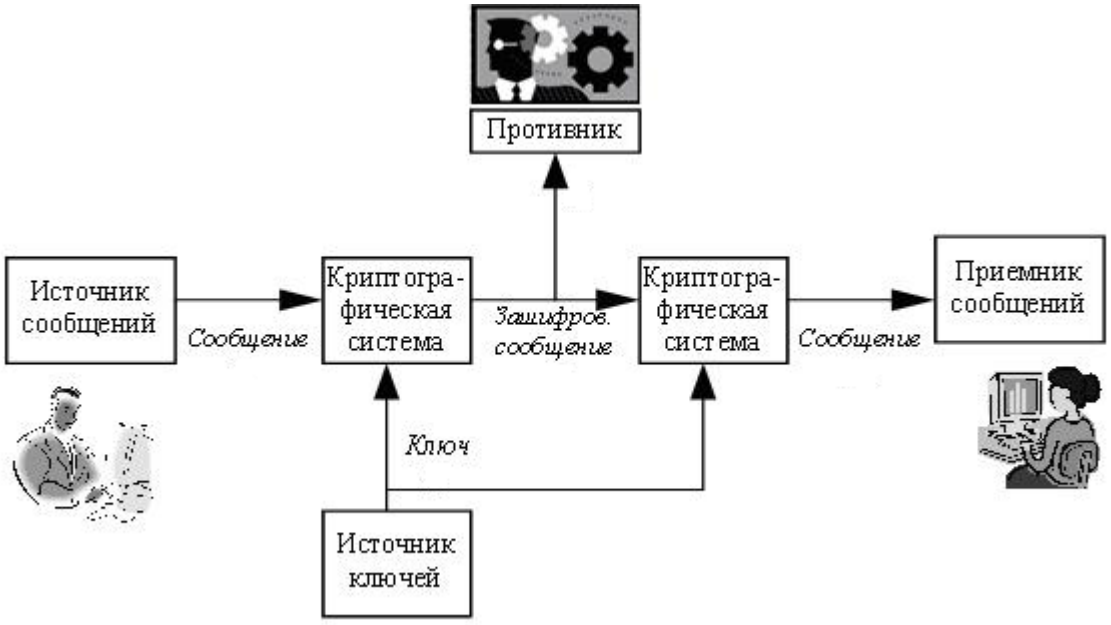
Например, пусть ключ содержит 5 символов, каждый из которых может встречаться в ключе только один раз. Ключ построен на латинском алфавите. Для составления и проверки ключа, т.е опробования его при расшифровании перехваченной криптограммы требуется 30 секунд. Можно подсчитать число возможных вариантов ключа – 7893600. Для проверки всех вариантов потребуется 7893600×30 сек.=236808000 сек = 2740 суток. Современные компьютеры на опробование ключа тратят доли секунды, поэтому полное время перебора, для данного примера, значительно сокращается и практически равно нескольким секундам.

Современные алгоритмы в качестве ключа используют последовательность двоичных кодов, что позволяет применять операции побитового сложения и вычитания. Для получения двоичного кода каждому элементу ключа нужно поставить в соответствие код из таблицы ASCII и затем перевести каждый полученный код в двоичную систему счисления.

Например, Пусть слово «текст» будет ключом. Тогда этому ключу соответствует последовательность ASCII кодов – 226, 165. 170, 225, 226. Перевод этого кода в двоичную систему счисления даст ключ – 11100010101001011010101010000110100010.

4. Современные симметричные криптосистемы

Симметричные криптосистемы (шифры) или **криптосистемы с секретным ключом** построены на принципе сохранения в тайне ключа шифрования..



Перед использованием симметричной криптосистемы пользователи должны получить общий секретный ключ и исключить доступ к нему злоумышленника. Открытое сообщение подвергается криптографическому преобразованию и полученная криптограмма (зашифрованное сообщение) по

открытому каналу связи передается получателю, где осуществляется обратное преобразование с целью выделения исходного открытого сообщения Симметричные криптосистемы различают: по виду криптографического преобразования; по конструктивным принципам; по виду защищаемой информации; по криптографической стойкости и т.д. Чаще всего используются первые два признака классификации.

По виду криптографического преобразования симметричные криптосистемы делятся на три группы: шифры перестановки, шифры замены и композиционные шифры.

Под шифром перестановки понимается переупорядочение букв исходного сообщения, в результате которого оно становится нечитаемым. На языке математики это может быть описано так.

Для открытого сообщения $X = x_0 x_1 ... x_{n-1}$ длины n в алфавите A_X может быть применено правило перестановки (криптографическое преобразование) $f_n = (f(0), f(1),.., f(n-1))$. Результатом такой перестановки будет криптограмма $Y = y_0 y_1 ... y_{n-1} = x_{f(0)}, x_{f(1)},..., x_{f(n-1)}$

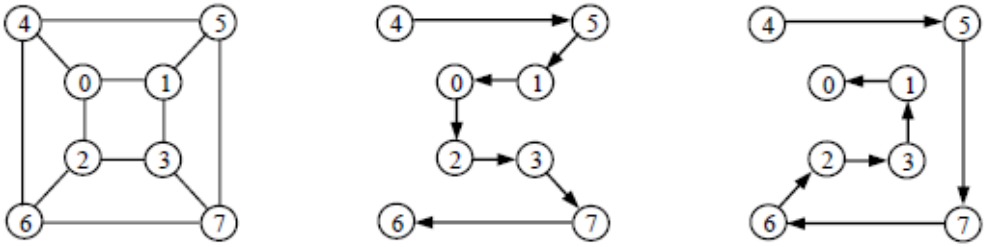
Семейство криптографических преобразований $f_n = (f(0), f(1),.., f(n-1))$ представляет собой **шифр перестановки**. Ключом шифра является правило перестановки. Ранее мы рассмотрели такие шифры перестановки как скитала, «магический квадрат» и «решетка Кордано».

На практике при применении шифров перестановки длины открытого текста и ключа не совпадают, так как, как правило, ключ имеет фиксированную длину l. В этом случае открытый текст разбивается на $n_l = \frac{N}{l}$ отрезков длины l к каждому из которых применяется перестановка. В случае, когда открытое сообщение не может быть разделено на n_l равных отрезков, т.е. $N = l \cdot n_l + r$, где r - остаток, необходимо дополнить открытый текст $l - r$ произвольными символами, то есть «пустышками».

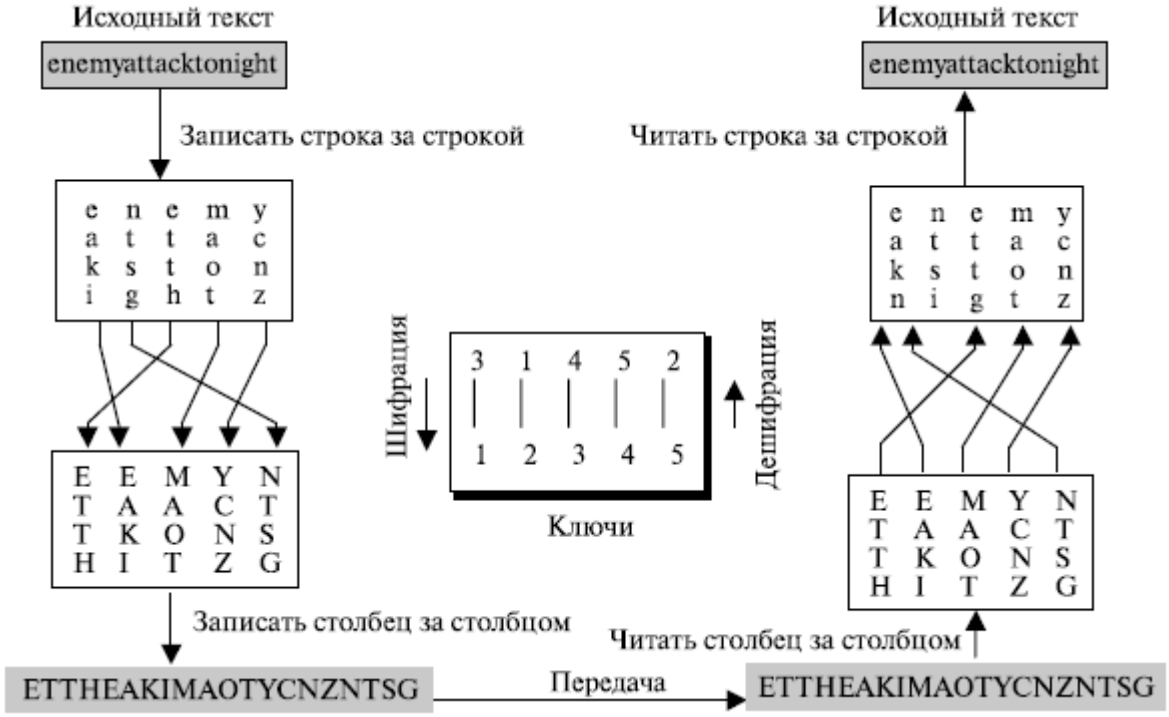
Наиболее известны следующие типы шифров перестановки. **Шифр простой перестановки**. В соответствии с заданным правилом осуществляется перестановка букв открытого текста. Правило перестановки является ключом шифра. Как правило, длина ключа соответствует длине открытого сообщения. **Шифр перестановки с фиксированным периодом** относиться к простым шифрам перестановки. Сообщение делится на блоки соответствующие заданному периоду. К каждому блоку применяется одна и та же перестановка.

Шифры маршрутной перестановки используют прямоугольную таблицу, в которую текст записывается, например, по строкам, а криптограмма считывается по определенному маршруту (по столбцам, по диагонали и т.п.). Расшифрование состоит в обратном действии, сначала по заданному маршруту заполняется таблица, а затем, например, по строкам, считывается исходный текст. Ключом таких шифров являются размеры таблицы и маршрут записи и

считывания символов. Наиболее сложные маршрутные перестановки реализуются с применением гамильтоновых путей на графе:



Шифр вертикальной перестановки является частным случаем шифра маршрутной перестановки. Шифрование заключается в записи по строкам открытого текста в таблицу, а считывание криптограммы осуществляется по столбцам. На рисунке иллюстрируется пример алгоритма этого шифрования.



Под шифром замены понимается преобразование, которое заключается в замене букв исходного сообщения на другие буквы по более или менее сложному правилу. Пусть имеется открытое сообщение $X = x_0 x_1 ... x_{n-1}$ длины n в алфавите A_X и правило замены $f_з = (f_0, f_1, .., f_{n-1})$, тогда применение этого криптографического преобразования к открытому сообщению дает криптограмму $Y = y_0 y_1 ... y_{n-1} = f_0(x_0), f_1(x_1), ..., f_{n-1}(x_{n-1})$. Семейство криптографических преобразований $f_з = (f_0, f_1, .., f_{n-1})$ называется **шифром замены**.

В зависимости от вида криптографической функции шифры замены делятся на шифры моноалфавитной замены и шифры многоалфавитной замены.

Моноалфавитные (одноалфавитные) замены – наиболее простой вид преобразований, заключающийся в замене по определенному правилу букв исходного сообщения на другие буквы из этого же алфавита, т.е. каждая буква исходного текста преобразуется в букву криптограммы по одному и тому же закону. К таким шифрам относятся шифр Цезаря, шифр атбаш, простая и мудрая литорея и другие, рассмотренные ранее шифры.

В случае **многоалфавитной замены** закон преобразования меняется от буквы к букве. Необходимо заметить, что один и тот же шифр может рассматриваться и как моно-, и как многоалфавитная замена в зависимости от определяемого алфавита. Например, замена биграмм с точки зрения обычного алфавита является моноалфавитной заменой, а с точки зрения алфавита биграмм - многоалфавитным. Рассмотрим наиболее известные шифры замены. Шифрами многоалфавитной замены можно отнести шифр Виженера, шифр Тритемия. Шифры делла порта и Альберти, шифр Вернама и другие.

Как на языке современной математики можно записать шифры Цезаря, Виженера и Вернама? Вспомним о модулярной арифметике.

Процесс зашифрования исходного текста шифром Цезаря определяется выражением:

$$y_i = (x_i + k) \bmod m,\ i = \overline{1,n},$$

где y_i - буква криптограммы, x_i - буква открытого сообщения, k - ключ шифра, n - длина криптограммы (открытого текста), $m = |A_X|$ - мощность алфавита A_X. Мощность алфавита является число букв (символов), входящих в него. Очевидно, что выражение:

$$x_j = (y_j - k) \bmod m,\ j = \overline{1,n},$$

определяет процесс расшифрования криптограммы.

В шифре Виженера ключ $k^{(d)}$ задается набором из d символов. Такие наборы подписываются под буквами открытого текста $X = x_1, x_2, ..., x_n,\ x_i \in A_X$, до получения периодической ключевой последовательности $\tilde{k} = k_1, k_2, ..., k_n$, $n = sd + r$, где s - число полных периодов $k^{(d)}$, $r = n \bmod d$, а значение d определяет период ключевой последовательности. Процесс шифрования определяется выражением:

$$y_i = \left(x_i + \tilde{k}_i\right) \bmod m,\ i = \overline{1,n}.$$

Если же криптосистема Виженера имеет период $d = n$, то получаем шифр гаммирования:

$$y_i = \left(x_i + \gamma_i\right) \bmod m,\ i = \overline{1,n}.$$

В шифре гаммирования ключевая последовательность носит название гамма-последовательности γ.

Очевидно, что при значении $d = 1$ получаем шифр Цезаря, если $1 < d < n$ получаем шифр Виженера, а при $d = n$ - шифр гаммирования. Частным случаем шифра гаммирования является шифр Вернама, который определен на алфавите $A = \{0,1\}$:

$$y_i = (x_i + \gamma_i) \bmod 2,\ i = \overline{1,n}.$$

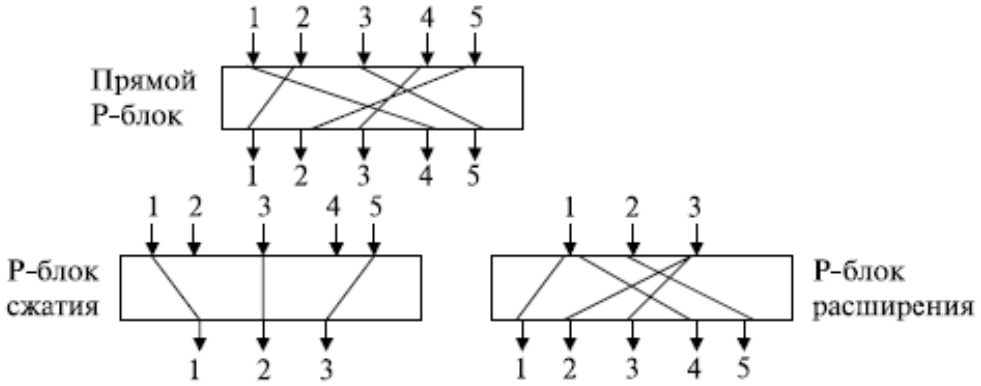
Композиционные шифры строятся на основе шифров замены и перестановки. Существующие симметричные криптосистемы относятся к комбинированным шифрам, так как использование только шифра замены, или только шифра перестановки не обеспечивает стойкость криптосистемы.

По конструктивным принципам современные криптосистемы делятся на поточные криптосистемы и блочные криптосистемы.

Блочные симметричные криптосистемы (блочные шифры) представляют собой семейство обратимых криптографических преобразований блоков (частей фиксированной дины) исходного текста.

Современные блочные шифры не проектируются как единый шифр. Чтобы обеспечивать требуемые свойства (криптостойкостью и имитостойкость) современного блочного шифра, этот шифр формируется как комбинация модулей замены S (substitution) блоков и перестановки P (permutation) элементов блоков входного текста.

P-модуль (блок перестановки) перемещает биты. В современных блочных шифрах мы можем найти три типа P-модулей: прямые P-блоки, P-блоки расширения и P-блоки сжатия.



Можно создавать два ключа для перестановок: один для шифрования и один для дешифрования. Ключи приводятся в таблицах, которые приведены в стандарте того или иного алгоритма шифрования.

S-модуль (блок замены) можно представить себе как миниатюрный шифр замены. Этот блок может иметь различное число входов и выходов. Другими словами, вход к S-модулю может быть n-битовым словом, а выход может быть m-разрядным словом, где m и n - не обязательно одинаковые числа. Хотя S-модуль может быть ключевым или без ключа, современные блочные шифры обычно используют S-модуль без ключей, где отображение от информационных входов к информационным выходам заранее определено.

Чаще всего S-модули представляют собой таблицу замены, упрощенный пример которой приведен на рисунке.

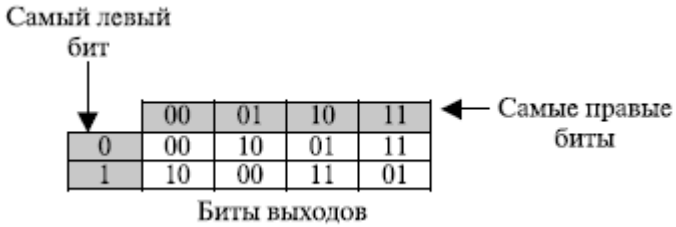
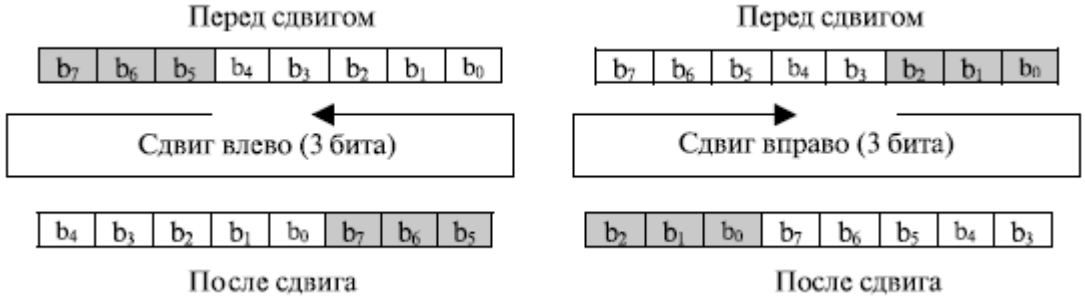


Таблица определяет отношения между входами/выходами для S-модуля размера 3×2. Крайний левый бит входа определяет строку; два самых правых бита входа определяют столбец. Два бита выхода – это значение на пересечении секции выбранной строки и столбца.

Другой компонент, применяемый в некоторых современных блочных шифрах, – **операция циклического сдвига**. Смещение может быть влево или вправо. Круговая операция левого сдвига сдвигает каждый бит в n-битовом слове на k позиции влево; крайние левые k-биты удаляются слева и становятся самыми правыми битами. Круговая операция правого сдвига сдвигает каждый бит в n-битовом слове на k позиций вправо; самые правые k-биты справа удаляются и становятся крайними левыми битами.

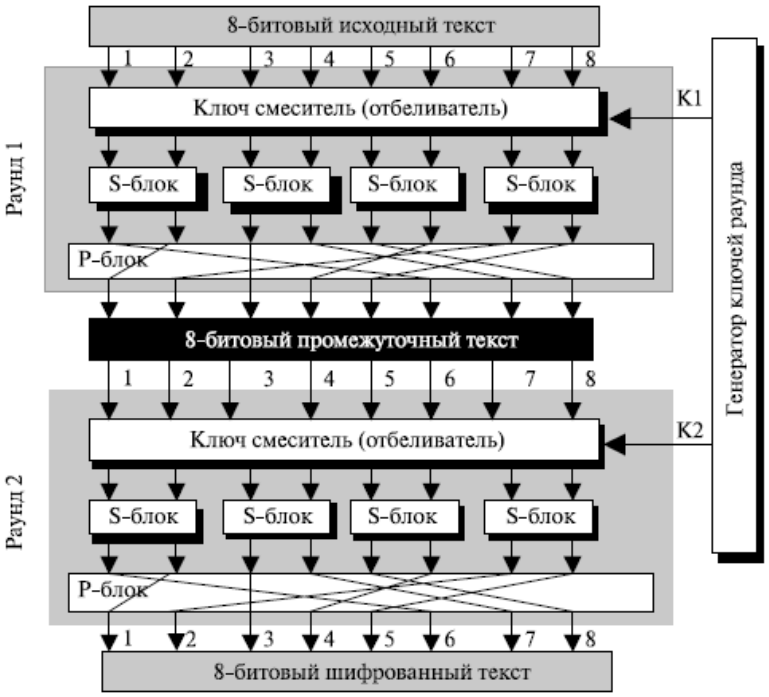


Перечисленные операции блочного шифрования реализуют идею Клода Шеннона о рассеивании и перемешивании. **Рассеивание** должно скрыть отношения между зашифрованным текстом и исходным текстом. Это собьет с толку противника, который использует статистику зашифрованного текста, чтобы найти исходный текст. Рассеивание подразумевает, что каждый символ (символ или бит) в зашифрованном тексте зависит от одного или всех символов в исходном тексте. Другими словами, если единственный символ в исходном тексте изменен, несколько или все символы в зашифрованном тексте будут также изменены. Идея **перемешивания** - в том, что оно должно скрыть отношения между зашифрованным текстом и ключом. Это собьет с толку противника, который стремится использовать зашифрованный текст, чтобы найти ключ. Другими словами, если единственный бит в ключе изменен, все биты в зашифрованном тексте будут также изменены.

Рассеивание и перемешивание могут быть достигнуты использованием повторения составных шифров, где каждая итерация – комбинация S-модулей, P-модулей и других компонентов. Каждая итерация называется**раундом.** Практически все современные блочные шифры раундовые (итерационные). На рисунке представлен пример блочного 2-х раундового шифра.

Первым опытом создания блочной криптосистемы явилась разработанная американской фирмой IBM криптосистема LUCIFER. Блоки открытого и шифрованного текста, обрабатываемые криптосистемой LUCIFER,

представляют собой двоичные векторы длиной 128 бит. Однако полученная криптосистема LUCIFER получилась достаточно громоздкой и обладала низкой производительностью.



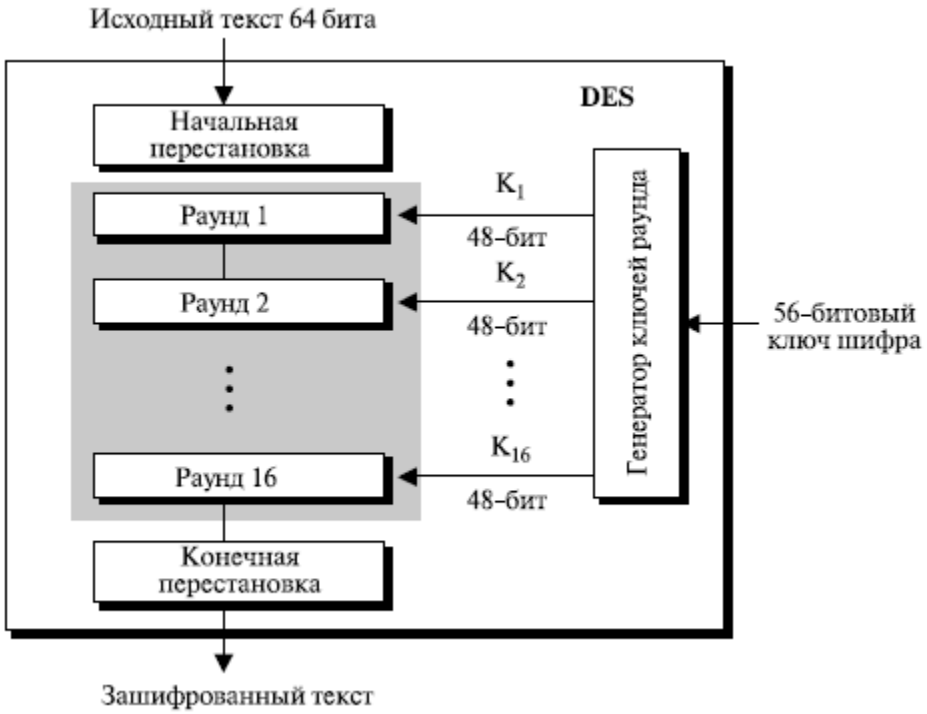
Скорость шифрования при программной реализации криптосистемы не превышала 8 кбайт/с, аппаратная реализация давала скорость шифрования не более 97 кбайт/с. К тому же у разработчиков были опасения по поводу криптостойкости, которые впоследствии подтвердились. Вместе с тем, накопленный разработчиками опыт при создании криптосистемы LUCIFER пригодились при разработки последующих блочных криптосистем.

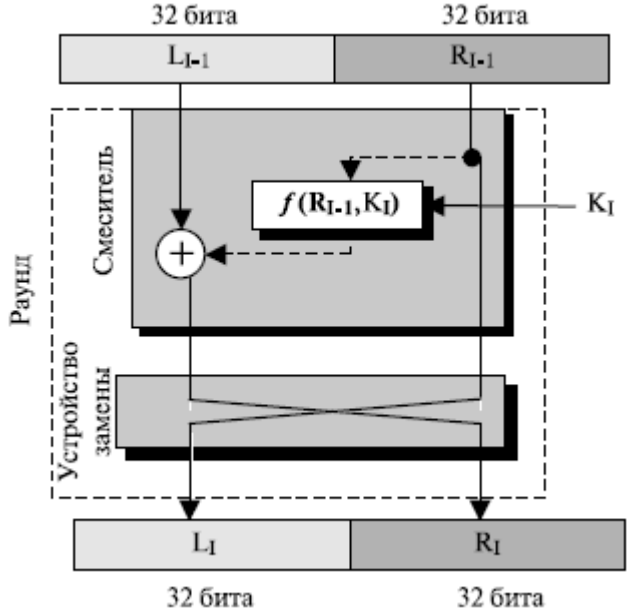
В 1974 году фирмой IBM был разработана криптосистема, получившая название DES (Data Encryption Standart). Криптосистема DES построена по **итеративному** принципу, то есть на основе нескольких однотипных преобразований. Ведущим разработчиком шифра был Хорст Фейстель.

Криптосистема DES – итеративная 16-раундовая обратимая блочная криптосистема на основе схемы Фейстеля. Размер входного блока - 64 бита. Размер ключа – 64 бита, причем каждый восьмой бит ключа, являющийся двоичной суммой предыдущих семи бит, является служебным и в шифровании не участвует. Раундовые ключи $k_1, k_2, ..., k_{16}$ есть алгоритмически вырабатываемые выборки 48 бит из 56 бит ключа криптосистемы.

Криптосистема DES была принята в качестве национального стандарта шифрования в США и опубликована в 1975 году. Это был беспрецедентный случай в истории криптографии.

Открытое опубликование криптосистемы DES привело к тому, что эта криптосистема, как никакая другая, тщательно изучалась криптоаналитиками всего мира.





Процесс криптопреобразования включает три этапа:

- биты исходного сообщения подвергаются начальной перестановке P;
- полученный блок разбивается на две равные части и подвергается 16-ти раундовому шифрованию по схеме Фейстеля;
- полученный после 16-го раунда блок подвергается конечной перестановке IP^{-1}.

За последние два десятилетия вычислительная техника развивалась настолько быстро, что временные и стоимостные затраты на реализацию криптоатаки на криптосистему DES постоянно снижались. Это привело к тому, что использование криптосистемы DES не удовлетворяет требованиям скрытности информации. В настоящее время используются варианты усложненной криптосистемы DES. Наиболее широко известна криптосистема 3DES («тройнойDES»). Ключ криптосистемы 3DES имеет длину 58·3=168 бит. Криптосистема 3DES примерно в три раза медленнее, чем криптосистема DES. Во многих системах защиты информации такое уменьшение скорости шифрования является неприемлемым. В 1984 году Рон Ривест предложил схему усложнения криптосистемы, которая получила название DESX (DESeXtended) и оказалась свободной от недостатков 3DES. Ключ криптосистемы DESX состоит из 56+64+64=184 бит и включает основной ключ шифрования и два «зашумляющих» ключа.

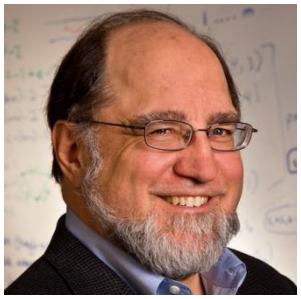
В 1997 году Национальный институт стандартов и технологий США (NIST) объявил о начале программы AES (AdvancedEncryptionStandard) по принятию нового стандарта криптографической защиты взамен устаревшему стандарту DES. Требования к кандидатам: криптоалгоритм должен быть открыто опубликован; криптоалгоритм должен быть симметричным блочным шифром, допускающим размеры ключей в 128, 192 и 256 бит; криптоалгоритм должен быть предназначен как для аппаратной, так и для программной реализации; криптоалгоритм должен быть доступен для открытого использования в любых продуктах; криптоалгоритм подвергается изучению по следующим параметрам: стойкость, стоимость, гибкость, реализуемость в smart-картах.

На конкурс приняты 15 алгоритмов из 12 стран. В финал конкурса вышли криптосистемы: MARS, TWOFISH, RC6, Rijndael, SERPENT. **Криптосистема MARS** выставлена на конкурс фирмой IBM и по своей структуре может быть отнесена к модифицированным шифрам Фейстеля. Достоинствами криптосистемы является высокий уровень защищенности, потенциальная возможность поддержки ключа размером более 256 бит, высокая эффективность на 32 разрядных платформах. Недостаток криптосистемы состоит в сложности ее конструкции. Это, пожалуй, самая сложная криптосистема, представленная на конкурс. **Криптосистема TWOFISH** представлена на конкурс Б. Шнайдером. По своей структуре криптосистема является классическим шифром Фейстеля. Главная особенность криптосистемы – меняющиеся в зависимости от ключа таблицы замен. Достоинствами являются: высокий уровень защиты, удобная реализация в smart-картах, высокая эффективность на любых платформах (в том числе и на 64 разрядных), вычисление раундовых ключей «на лету», допускает произвольную длину ключа до 256 бит. К недостаткам можно отнести высокую сложность алгоритма, что затрудняет его аппаратную и программную реализации. **Криптосистема RC6** представлена на конкурс фирмой RSALab и по своей структуре может быть также отнесена к модифицированным шифрам Фейстеля. Достоинствами криптосистемы является: простая структура алгоритма, быстрая

процедура формирования ключа, потенциальная возможность поддержки ключа размером более 256 бит, длина ключа и число раундов могут быть переменными, высокая эффективность на 32 разрядных платформах. К недостаткам можно отнести: относительно низкий уровень защищенности, невозможность формирования раундовых ключей «на лету». **Криптосистема SERPENT** представлена тремя известными криптоаналитиками Р. Андерсеном, Э. Бихамом, Л. Кнудсеном. Криптосистема является классической SP-сетью. Достоинствами криптосистемы является: высокий уровень защищенности, удобная реализация в smart-картах. К недостаткам относится низкая скорость шифрования. Это самая медленная из всех представленных на конкурс криптосистем. В 2000 году конкурс завершился и победителем была признана криптосистема Rijndael, как имеющая наилучшее сочетание стойкости, стоимости, производительности, эффективности реализации и гибкости. Авторами криптосистемы являются Винсент Райман и ЙоанДамен. **Криптосистема Rijndael**, в настоящее время известная больше как **AES,** представляет собой алгоритм шифрования не использующий схему Фейстеля. Криптосистема имеет ключи размером 128, 192 и 256 бит, входные блоки могут иметь длину 128, 192 и 256 бит. Количество раундов 10, 12 или 14 в зависимости от длины ключа.

Кроме этого достаточно широко используются такие криптосистемы, как IDEA (InternationalDataEncryptionAlgorithm), SAFER+ и SAFER++.

Поточные симметричные криптосистемы (поточные шифры) относятся к шифрам замены, преобразующим посимвольно открытый текст в криптограмму. В современных поточных криптосистемах в качестве шифруемых символов фигурируют биты или даже байты.



Рассмотрим поточные шифры на примере RC4. Это поточный шифр, который был разработан в 1984 г. Рональдом Ривестом. RC4 используется во многих системах передачи данных и протоколах организации сети. RC4 - байт-ориентированный шифр потока, в котором байт (8 бит) исходного текста складывается по модулю 2 с байтом ключа, чтобы получить байт зашифрованного текста. Ключ шифра, из которого сгенерированы однобайтовые ключи в потоке ключей, может содержать от 1 до 256 байтов.

Криптосистема RC4 является собственностью компании RSA Data Security Inc, а ее описание никогда не было опубликовано и предоставлялось партнерам только после подписания соглашения о неразглашении. Однако в сентябре 1994 года алгоритм RC4 был анонимно опубликован. С тех пор сама криптосистема перестала быть секретом, но название RC4 остается торговой маркой. То есть, чтобы получить право заявлять, что в коммерческом программном продукте используется RC4, необходимо приобрести лицензию на этот алгоритм у RSA DataSecurity. Без лицензии можно утверждать лишь то, что используется алгоритм, похожий на RC4 и совпадающий с ним на всем известном множестве тестов. В связи с этим, некоторые компании не имеющие лицензии на RC4 предпочитают называть ее ARC4 (AllegedRC4). Основные

преимущества криптосистемы RC4 - высокая скорость работы и переменный размер ключа. Главным фактором, способствовавшим широкому применению RC4, была простота ее аппаратной и программной реализации. Вместе с тем, RC4 довольно уязвима, если используются не случайные или связанные ключи, или один ключевой поток используется дважды. Криптосистема RC4 применяется в таких продуктах, как MicrosoftOffice, LotusNotes, AdobeAcrobat и др.

В стандарте GSM сотовой связи используется поточный алгоритм шифрования A5. Шифр использует линейный регистр сдвига, чтобы создать ключевой поток. Телефонная связь в GSM осуществляется как последовательность кадров на 228 битов, при этом каждый кадр длится 4,6 миллисекунды. A5 создает поток бит, исходя из ключа на 64 бита. Разрядные потоки собраны в буфере по 228 битов, чтобы складывать их по модулю два с кадром на 228 битов.

В настоящее время в мире существует большое множество поточных шифров, отличающихся сложность ,криптостойкостью и видом реализации. Выбор поточного шифра, как и любого другого шифра, должен соответствовать важности шифруемой информации и требуемой скорости передачи шифрованного сообщения, а также стоимости используемого шифра.

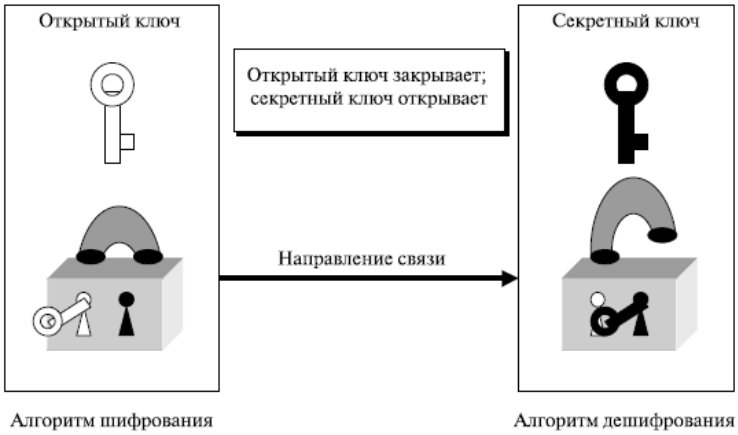
5. Криптосистемы с открытым ключом

Концептуальные отличия между симметричными шифрами и шифрами с открытым ключом базируются на том, как эти системы сохраняют секретность. В криптосистемах с симметричными ключами задача секретности должна быть разделена между двумя людьми (абонентами). В системах шифрования с открытым ключом секретность - персональная задача (неразделенная); человек (абонент) создает и сохраняет свою собственную тайну.

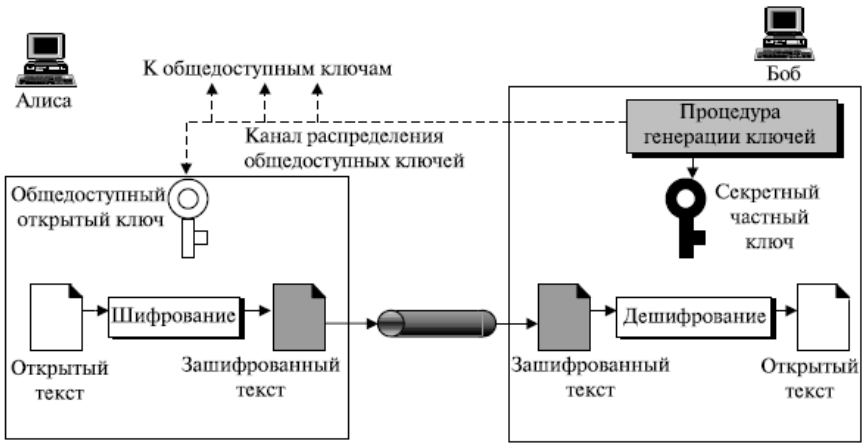
В сообществе n абонентов при использовании криптосистем с симметричными ключами для сохранения секретности требуется n(n-1)/2 общедоступных ключей. В системах шифрования с открытым ключом необходимы только n персональных ключей. Таким образом, сообщество с количеством участников 1 миллион при использовании симметричных шифров требовало бы пятисот миллионов общедоступных ключей, а использование криптосистем с открытым ключом требует 1 миллион персональных ключей.

Обратим внимание на то, что криптография с симметричными ключами базируется на подстановке и перестановке символов (символов или бит), а криптография с открытым ключом - на применении математических функций к числам. В криптографии с симметричными ключами исходный текст и зашифрованный текст представляют как комбинацию символов. Шифрование и расшифрование здесь - это перестановка этих символов или замена одного символа другим. В криптографии с открытым ключом исходный текст и зашифрованный текст - числа; их шифрование и расшифрование – это математические функции, которые применяются к числам, чтобы создать другие числа.

Криптография с открытым ключом использует два отдельных ключа: один секретный (частный) и один открытый (общедоступный), процесс шифрования и расшифрования может быть представлен как процесс запирания и отпирания замков разными ключами. В этом случае замок, запертый открытым ключом доступа, можно отпереть только с соответствующим секретным ключом.



Первый ключ (открытый) подчеркивает асимметричный характер криптографической системы. Ответственность за обеспечение безопасности находится, главным образом, на плечах приемника (в данном случае это Боб). Боб должен создать два ключа: один секретный (частный) и один открытый (общедоступный). Боб не несет ответственность за распределение открытого ключа доступа всему сообществу. Это может быть сделано через канал распределения открытого ключа доступа. Хотя этот канал не обязан обеспечивать секретность, он должен обеспечить установление подлинности и целостность информации о ключе. На данный момент мы принимаем, что такой канал существует.



Важным обстоятельством является то, что Боб и Алиса не могут использовать одно и то же множество ключей для двухсторонней связи. Каждый объект в сообществе создает свой собственный секретный и открытый ключи доступа. На рисунке показано, как Алиса может использовать открытый ключ доступа Боба, чтобы передать Бобу зашифрованные сообщения. Алиса использует открытый ключ Боба для шифрования сообщения, зашифрованное сообщение она передает по открытому каналу связи. Боб с помощью своего секретного ключа расшифровывает сообщение. Если Боб хочет ответить, то Алиса устанавливает свои собственные секретный и открытый ключи доступа.

Для криптосистем с открытым ключом характерно то, что Боб нуждается только в одном секретном ключе, чтобы получать всю корреспонденцию от любого участника сообщества и нуждается в n ключам других участников для связи с ними.

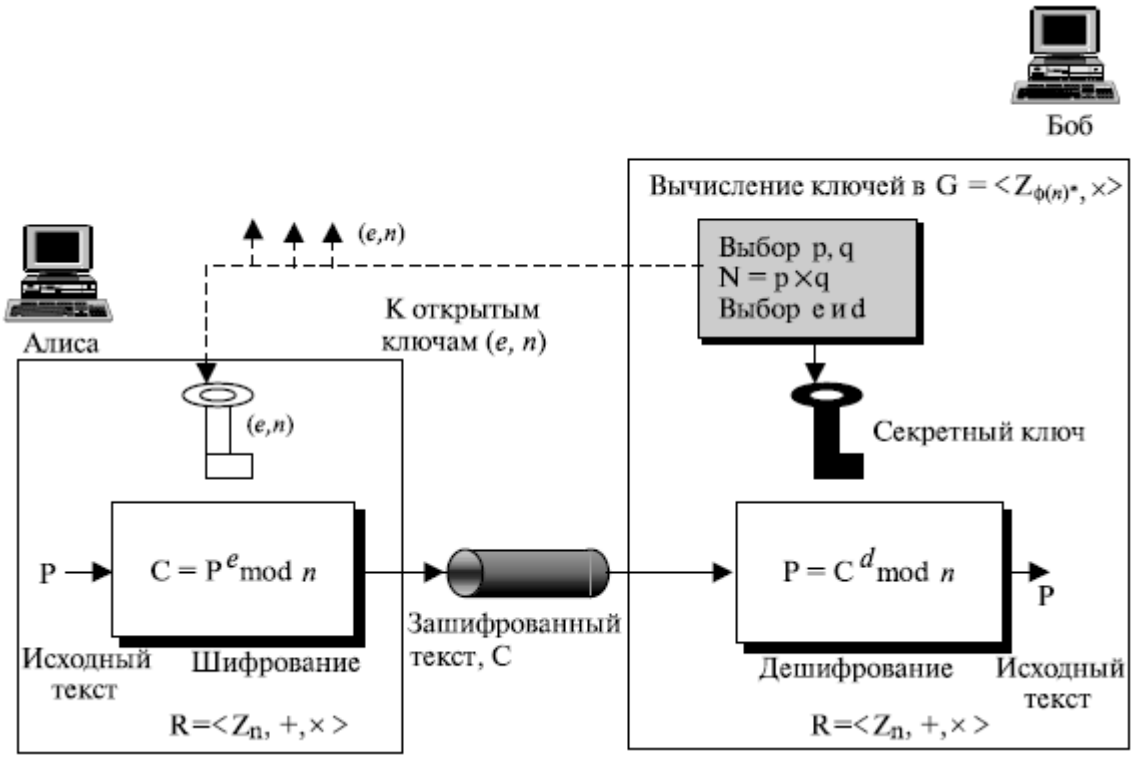
В отличие от криптографии с симметричными ключами, криптографии с открытым ключом исходный текст и зашифрованный текст обрабатываются как целые числа. Сообщение должно перед шифрованием кодироваться как целое число (или множество целых чисел). После расшифрования оно должно быть расшифровано как целое число (или множество целых чисел). Шифрование и расшифрование в криптографии с открытым ключом - математические функции, которые применяются к числам, представляющим исходный текст и зашифрованный текст.

Один из самых известных шифров с открытым ключом является **RSA,** который использует два типа ключей - e и d, где e - открытый, а d - секретный. Предположим, что P - исходный текст и C - зашифрованный текст. Алиса использует математическую функцию $C = P^e \bmod N$, чтобы создать зашифрованный текст C из исходного текста P, а Боб использует $P = C^d \bmod \mathrm{N}$, чтобы извлечь исходный текст (файл), переданный Алисой. Модулей N создается очень большое количество с помощью процесса генерации ключей.

Для шифрования и расшифрования применяют возведение в степень по модулю. Как уже показано выше, при использовании алгоритма возведение в степень по модулю выполнимо в небольшое время. Однако нахождение дискретного логарифма операция трудновыполнимая. Это означает, что Алиса

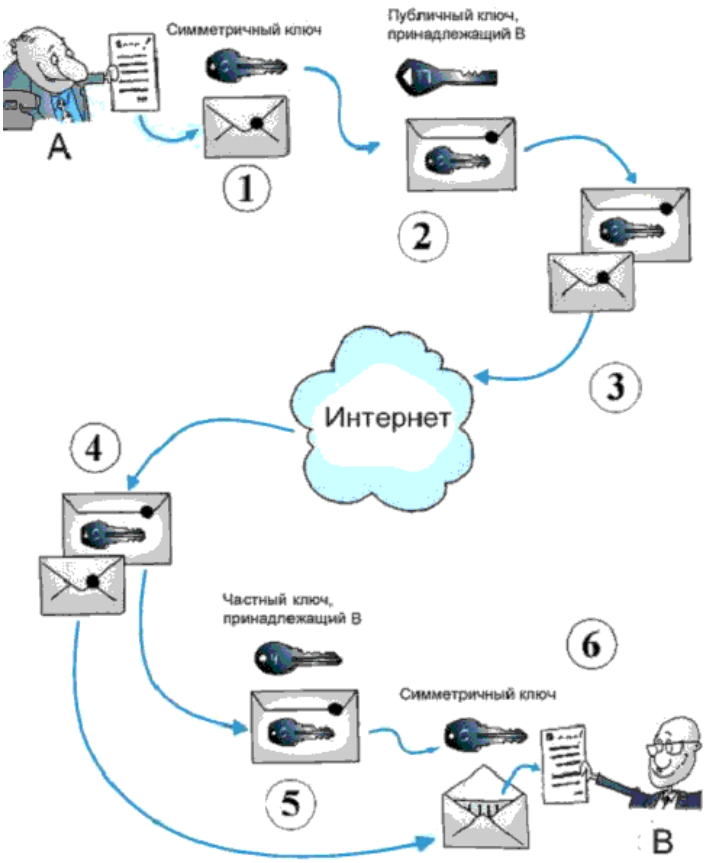
может зашифровать сообщение общедоступным ключом e за небольшое время. Боб также может расшифровать его быстро, потому что он знает d. Но противник (Ева) не может расшифровать это сообщение, потому что она должна вычислить корень e-той степени из C с использованием модульной арифметики или решить задачу факторизации числа N.

В этом состоит идея RSA, однако описание алгоритма RSA в данной книге не приводится, так как его понимание требует определенных математических знаний.



Отметим в заключении один очень важный факт, который иногда неправильно истолковывается.

Появление криптографии с открытым ключом не устраняет потребность в криптографии с симметричными ключами (секретный ключ). Причина в том, что криптография с асимметричными ключами использует математические функции для шифрования и расшифрования намного медленнее, чем криптография с симметричными ключами. Для шифрования больших сообщений криптография с симметричными ключами необходима. С другой стороны, скорость криптографии с симметричными ключами не устраняет потребность в криптографии с открытым ключом. Сегодня системы информационной безопасности нуждаются в обеих системах шифрования. Эти системы шифрования дополняют одна другую. Это факт представлен на рисунке. Для передачи шифрованных сообщений абонент А формирует ключ симметричной криптосистемы и с помощью асимметричной криптосистемы передает его по открытым каналам связи абоненту В. Абонент В расшифровывая полученное сообщение своим секретным ключом получает ключ шифрования симметричного шифра. Теперь он готов к приему криптограммы любого объема.



Кроме того, криптография с открытым ключом необходима для установления подлинности электронных подписей и работы станций по рассылке ключей шифрования.

6. Задачи с примерами их решения

6.1. Задачи обычного уровня сложности (разбираемые с учащимися на уроках)

Простейшие шифры

Задача 1. Пусть дан открытый текст X =КРИПТОГРАФИЯ. Требуется получить криптограмму, используя шифр простой перестановки при заданном ключе $K = \{10,2,3,7,5,8,9,11,12,1,4,6\}$.

Задача 2. Пусть дан открытый текст: X =ИСТОРИЯ_КРИПТОГРАФИИ. Требуется получить криптограмму, используя шифр простой перестановки при заданном ключе $K = \{5,3,4,1,2\}$.

Задача 3. Дано открытое сообщение

X =ЭТО_ШИФР_ВЕРТИКАЛЬНОЙ_ПЕРЕСТАНОВКИ.

Требуется зашифровать данное сообщение шифром вертикальной перестановки используя ключ К=$\{5,2,3,4,1\}$.

Задача 4. Дан открытый текст X =ДОЛГ – ЭТО ТО, ЧТО ОЖИДАЕШЬ ОТ ДРУГИХ, НО НЕ ОТ СЕБЯ. ОСКАР УАЙЛЬД. Задан «магический квадрат»:

2 7 6

9	5	1
4	3	8

Требуется зашифровать открытый текст.

Задача 5. Зашифровать сообщение $X =$ ЛЕГКО КРИТИКОВАТЬ ДРУГИХ – СЛОЖНЕЕ ИЗМЕНИТЬСЯ САМОМУ, с помощью «магического квадрата»:

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Задача 5.

Дан «квадрат Полибия»

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

Зашифровать открытое сообщение $X =$ МАТЕМАТИКА - ЦАРИЦА НАУК.

Задача 6. Имеется криптограмма $Y =$ ПШХБЙХФХОЁАИЕЙЧФЙХУЗУ, полученная применением шифра Цезаря с ключом $K = 5$. Расшифровать криптограмму.

Задача 7. Зашифровать, используя шифр Виженера, открытое сообщение $X =$ ШИФР СКРЫВАЕТ СОДЕРЖАНИЕ ТЕКСТА. Ключ шифра – $K =$ МГТУГА.

Задача 8. Зашифровать сообщение $X =$ КРИПТОГРАФИЯ НАИБОЛЕЕ ВАЖНАЯ ФОРМА РАЗВЕДКИ В СОВРЕМЕННОМ МИРЕ шифром Плейфера с ключом $K =$ ГРОЗА.

Задача 9. Зашифровать текст $X =$ ЛЮБОЙ ШИФР МОЖЕТ БЫТЬ ВСКРЫТ, ЕСЛИ ТОЛЬКО В ЭТОМ ЕСТЬ НАСТОЯТЕЛЬНАЯ НЕОБХОДИМОСТЬ. НОРБЕРТ ВИНЕР с помощью «доски Полибия» используя ключ $K =$ ПОЛИБИЙ.

Задача 10. Криптограмма, полученная при зашифровании сообщения шифром Цезаря, имеет вид

$Y =$ ХПНЬЪШЧЭХЫИМШЫЩШНЙЩЪТЫИРЧЕОСЙЫОНЙЬОХТ.

Расшифровать сообщение при известном ключе К=10.

Примеры решения задач

Простая перестановка

Задача 1. В рассматриваемой задаче в соответствии с заданной перестановкой необходимо десятую букву открытого текста переставить на первое место, вторую и третью буквы оставить на месте, седьмую букву переставить на четвертое место и т.д. Полученная криптограмма будет иметь вид $Y =$ ФРИГТРАИЯКПО.

Задача 2. Рассматриваемая задача в целом аналогична задаче 1. Однако, в данном случае длина ключа меньше, чем длина открытого текста, поэтому открытое сообщение делится на 4 группы по 5 букв (учитывая и пробел) в каждой:

$X =$ИСТОР ИЯ_КР ИПТОГ РАФИИ.

К каждой группе применяется перестановка с заданным ключом и в результате получается криптограмма

$Y =$РТОИСР_КИЯГТОИПИФИРА.

Примечание: В случае, когда открытое сообщение не может быть разделено на l равных групп, т.е. $n_X = l \cdot n_K + r$, где n_X и n_K - длина открытого текста и ключа, соответственно, r остаток, необходимо дополнить открытый текст $n_K - r$ произвольными буквами, называемыми «пустышками».

Задача 3. Запишем данное открытое сообщение в таблицу размером 5×7.

Э	Т	О	_	Ш
И	Ф	Р	_	В
Е	Р	Т	И	К
А	Л	Ь	Н	О
Й	_	П	Е	Р
Е	С	Т	А	Н
О	В	К	И	Я

Последняя ячейка таблицы дополнена произвольной буквой «Я», которая является «пустышкой». Для получения криптограммы, в соответствии с заданным ключом, считываем по столбцам из полученной таблицы буквы. Криптограмма имеет вид:

$Y =$ШВКОРНЯТФРЛ_СВОРТЬПТК_ _ИНЕАИЭИЕАЙЕО.

Задача 4. Запишем текст сообщения в квадрат таким образом, чтобы первая буква сообщения размещалась в ячейке с цифрой 1, вторая буква – в ячейке с цифрой два и т.д. до заполнения таблицы:

О	Т	Э
Т	_	Д
Г	Л	О

Считывает по строкам первую часть криптограммы ОТЭТ-ДГЛО. Повторяя подобные действия, получим конечную криптограмму $Y =$ОТЭТ-ДГЛО,ЖОДООТЧИАТОРЬДШЕДГННЕ,УХИНТ.ЯСБОЕСОАЛЙДАКУРЬ.

Простая замена

Задача 5. Каждая буква (или символ) заменяется на пару букв следующим образом. В таблице отыскивается буква открытого текста, затем определяется строка и столбец, на пересечении которых находится данная буква. Строки и столбцы в заданной «доске Полибия» соответствуют буквам А, Б, В, Г, Д и Е. Каждой букве открытого текста будет соответствовать пара букв, обозначающих строку и столбец, соответственно. Полученная криптограмма имеет вид:

$Y =$ ВБААГБАЕВБААГББГБЕАААЕГЕААВЕБГГЕААВВААГВБЕ.

Задача 6. Уравнение для расшифровки шифра Цезаря имеет вид

$x_i = (y_i - K) \bmod 33,$

где y_i и x_i - i-е буквы криптограммы и открытого сообщения, соответственно.

Тогда получаем:

$x_1 = (y_1 - 5) \bmod 33 = 12 \bmod 33 = 12 \to$ К;

$x_2 = (y_2 - 5) \bmod 33 = 21 \bmod 33 = 21 \to$ У;

$x_3 = (y_3 - 5) \bmod 33 = 18 \bmod 33 = 18 \to$ Р;

$x_4 = (y_4 - 5) \bmod 33 = -3 \bmod 33 = 30 \to$ Ь;

$x_5 = (y_5 - 5) \bmod 33 = 6 \bmod 33 = 6 \to$ Е и т.д.

В результате получаем исходный текст $X =$ КУРЬЕР ПРИБЫВАЕТ ПЕРВОГО.

В результате получаем криптограмму $Y =$ ХЭГНЕВИБЕРНУВЕЬ.

Задача 7. Выражение для шифра Виженера имеет вид:

$y_i = (x_i + k_i^d) \bmod 33,$

где y_i, x_i и k_i^d - i-е буквы криптограммы, открытого сообщения и ключевой последовательности периода d, соответственно.

Тогда имеем:

$y_1 = (x_1 + k_1^6) \bmod 33 = (26 + 14) \bmod 33 = 7 \to$ Ё;

$y_2 = (x_2 + k_2^6) \bmod 33 = (10 + 4) \bmod 33 = 14 \to$ М;

$y_3 = (x_3 + k_3^6) \bmod 33 = (22 + 20) \bmod 33 = 9 \to$ З;

$y_4 = (x_4 + k_4^6) \bmod 33 = (18 + 21) \bmod 33 = 6 \to$ Е;

$y_5 = (x_5 + k_5^6) \bmod 33 = (19 + 4) \bmod 33 = 23 \to$ Х;

$y_6 = (x_6 + k_6^6) \bmod 33 = (12 + 1) \bmod 33 = 13 \to$ Л;

$y_7 = (x_7 + k_1^6) \bmod 33 = (18 + 14) \bmod 33 = 32 \to$ Ю и т.д.

В результате получим криптограмму:

$Y =$ ЁМЗУХЛЮЯХФИУЯТЧЩФЗНСЬЩЦЁШХЁФ.

Задача 8. Сформируем таблицу размером 8×4 и заполним ее буквами русского алфавита, начиная с ключевого слова. Учтем, что в русском алфавите буквы Е и Ё можно считать эквивалентными.

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

Разобьем открытый текст на биграммы

$X =$ КР ИП ТО ГР АФ ИЯ НА ИБ ОЛ ЕЕ ВА ЖН АЯ ФО РМ АР АЗ ВЕ ДК ИВ СО ВР ЕМ ЕН НО ММ ИР ЕЯ.

Последняя биграмма составлена добавлением «буквы-пустышки».

Анализ полученных биграмм открытого текста показывает, что существуют биграммы ЕЕ и ММ не позволяющие применить для них алгоритм шифрования. В таком случае можно поступить следующим образом:

а) между буквами биграмм ЕЕ и ММ вставить произвольные «буквы-пустышки», например, ЕВЕ и МОМ;

б) удалить из открытого текста одну из букв биграммы.

Рассмотрим второй способ. Удалим буквы Е и М из слов НАИБОЛЕЕ и СОВРЕМЕННОМ, а также одну из удвоенных согласных Н в слове СОВРЕМЕННОМ. Это приведет к другому разбиению открытого текста на биграммы:

X =КР ИП ТО ГР АФ ИЯ НА ИБ ОЛ ЕВ АЖ НА ЯФ ОР МА РА ЗВ ЕД КИ ВС ОВ РЕ МЕ НО МИ РЕ.

В соответствии с алгоритмом криптографического преобразования шифра Плейфера для биграмм открытого текста получаем биграммы криптограммы: КР→ЖА, ИП→ЕТ, ТО→ЪИ, ГР→РО, АФ→КЬ и т.д.

В результате получается криптограмма: Y = ЖАЕТЪИРОКЬНЪКДЛОБИМГРККДЬЧЗОКВОБАДНГЛЙРЦЗДГЖНЖИДНЙ ГЖ.

Задача 14. В соответствии с алгоритмом шифрования сформируем таблицу:

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

Замене подлежат только согласные буквы. Тогда получаем: В→Ш, С→Л, Т→К, Р→М, Ч→Г и т.д.

В результате имеем криптограмму:

Y =ШЛКМЕГА ОКРЕПЯЕКЛЯ.

Криптоанализ («взлом») простейших шифров

Метод полного перебора

Задача 1. Имеется криптограмма:

Y =СХТХУЦЖ,

полученная шифром Цезаря. Требуется методом полного перебора (brute-force attack) определить ключ шифра и прочесть сообщение.

Задача 2. Определить ключ шифра Цезаря, если известна пара «открытый текст-криптограмма»:

X =КРИПТОЛОГИЯ – Y =ПХНФЧУРУЗНД.

Задача 3. Определить ключ шифра Цезаря, если даны пары «открытый текст-криптограмма»:

1) X =АПЕЛЬСИН – Y =САЦЬНВЩЮ;

2) X =АБРИКОС – Y =ЫЬЛГЕЙМ.

Задача 4. Дешифровать сообщения, зашифрованные шифром Цезаря:

Y =ГРХГРГРГУЛЕЦ.

Бесключевые методы «взлома» простейших шифров

Задача 5. Методом чтения в колонках дешифровать криптограмму:

$Y =$СШЫУЙА,

если известно, что при шифровании использована не равновероятная гамма, у которой все символы, кроме А, Б, И имеют нулевую вероятность.

Априорно известно, что криптограмма представляет собой зашифрованное название одной из стран мира.

Задача 6. Даны две криптограммы:

$Y =$ВЖТЕЛД;

$Y' =$ВЕЖСИЛБ.

Известно, что при зашифровании текстов использовалась одна и та же γ-последовательность, причем вторая криптограмма Y' есть результат зашифрования текста, полученного за счет видоизменения первого текста, а именно, за счет вставки после первой буквы произвольной буквы Г.

Требуется определить γ-последовательность и прочитать текст.

Задача 7. Методом чтения в колонках дешифровать криптограмму:

$Y =$ГЪЩРТДМББ,

полученную применением не равновероятной γ-последовательности, у которой все символы, кроме А, К, О, Ф имеют нулевую вероятность.

Задача 8. Даны две криптограммы:

$Y =$ЛЭМЭВЮУБЛНЯХ;

$Y' =$ЛЭМВЯВЯУЬБЯВБ.

Известно, что при зашифровании текстов использовалась одна и та же γ-последовательность, причем вторая криптограмма Y' есть результат зашифрования видоизмененного первого текста, полученного за счет вставки после третьей буквы произвольной буквы Ф.

Требуется определить γ-последовательность и прочитать текст.

Примеры решения задач

Задача 1. Количество возможных ключей шифра равно 33. Последовательно перебирая ключи и подставляя их в алгоритм расшифрования

$x_i = (y_i - K) \bmod 33,\ i = \overline{1,7},$

получим результат, который представлен в таблице 1.

Как видно из таблицы, в большинстве случаев достаточно расшифровать три-четыре буквы и проверить текст на «читаемость», а в отдельных случаях достаточно расшифровать одну-две буквы.

Открытое сообщение $X =$КОЛОМНА, используемый ключ $K = 7.$

Таблица 2

K	X	K	X
1	РФСФ	18	АДБД
2	ПУРУСФ	19	ЯГАГ
3	ОТПТР	20	ЮВЯВ
4	НСОСП	21	ЭАЮ
5	МРНР	22	Ь
6	ЛПМ	23	Ы
7	КОЛОМНА	24	Ъ
8	ЙН	25	ЩЭЪ
9	ИМЙ	26	ШЬ
10	ЗЛИЛ	27	ЧЫШ
11	ЖКЗ	28	ЦЪ
12	ЁЙ	29	ХЩ
13	ЕИЁ	30	ФШХ
14	ДЗЕЗ	31	УЧФ
15	ГЖД	32	ТЦУЦ
16	ВЁГЁ	33	СХТХУЦЖ
17	БЕВЕЁ		

Задача 2. Для определения ключа воспользуемся уравнением зашифрования

$y_i = (x_i + K) \bmod 33,\ i = \overline{1,11}.$

Подставим в выражения номера первых букв текста и криптограммы

$17 = (12 + K) \bmod 33.$

Данное уравнение справедливо только при $K = 5$. Проверяя данный ключ для следующих букв, убеждаемся в справедливости сделанного заключения.

Задача 4. $X =$ АНТАНАНАРИВУ, $K = 3$.

Задача 5. Для решения задачи дешифрования необходимо последовательно выполнить следующие действия:

1) расшифровать криптограмму, используя в качестве ключевой последовательности следующие гаммы:

$\gamma_1 =$ АААААА, $\gamma_2 =$ БББББББ, $\gamma_3 =$ ИИИИИИ;

2) полученные данные свести в таблицу:

	С	Ш	Ы	У	Й	А
А	**Р**	Ч	Ъ	Т	**И**	**Я**
Б	П	Ц	Ш	**С**	З	Ю
И	З	**О**	**С**	Й	А	Ц

3) проанализировать полученную таблицу.

Анализ полученной таблицы позволяет сделать вывод, что открытый текст: $X =$ РОССИЯ, а гамма - $\gamma =$ АИИБАА.

Задача 6. Определим значения γ-последовательности и текста начиная с момента вставки:

$\gamma_2 = (y'_2 - \tilde{x}) \bmod 33 = (6-4) \bmod 33 = 2 \to$ Б;

$x_2 = (y_2 - \gamma_2) \bmod 33 = 6 \to$ **Е**;

$\gamma_3 = (y'_3 - x_2) \bmod 33 = 2 \to$ Б;

$x_3 = (y_3 - \gamma_3) \bmod 33 = 18 \to$ **Р** и т.д.

В результате получаем единственный возможный вариант открытого сообщения $X =$ БЕРЕЗА, а $\gamma -$ последовательность имеет вид - $\gamma =$ АББАГГ.

Задача 7. $X =$ ВЕНЕСУЭЛА, $K =$ АФККАООФА.

Задача 8. $X =$ КРИПТОГРАММА, $K =$ АЛГМООППКАСФ.

6.2. Задачи повышенной степени сложности

Шифры перестановки

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1. Сочетаемость букв русского языка

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	**А**	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	**Б**	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	**В**	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	**Г**	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	**Д**	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	**Е**	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	**Ж**	е, и, д, а, н	71	29
89	11	о, е, а, и	**З**	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	**И**	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	**К**	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е,	**Л**	и, е, о, а, ь, я,	75	25

		о, а		ю, у		
80	20	я, ы, а, и, е, о	**М**	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о, а, и, е	**Н**	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	**О**	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	**П**	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	**Р**	а, е, о, и, у, я ,ы, н	80	20
69	31	с, т, в, а, е, и, о	**С**	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	**Т**	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	**У**	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	**Ф**	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	**Х**	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	**Ц**	и, е, а, ы	93	7
82	18	е, а, у, и, о	**Ч**	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	**Ш**	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	**Щ**	е, и, а	97	3
0	100	м, р, т, с, б, в, н	**Ы**	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	**Ь**	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	**Э**	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	**Ю**	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	**Я**	в, с, т, п, д, к, м, л	16	84

Таблица 2. Сочетаемость букв английского языка

Г	С	Слева		Справа	Г	С
19	81	l,c,d,m,n,s,w,t,r,e,h	**A**	n,t,s,r,l,d,c,m	6	94
55	45	y,b,n,t,u,d,o,s,a,e	**B**	e,l,u,o,a,y,b,r	70	30
61	39	u,o,s,n,a,i,l,e	**C**	h,o,e,a,i,t,r,l,k	59	41
52	48	r,i,l,a,n,e	**D**	e,i,t,a,o,u	54	46

8	92	c,b,e,m,v,d,s,l,n,t,r,h	**E**	r,d,s,n,a,t,m,e,c,o	21	79
69	31	s,n,f,d,a,i,e,o	**F**	t,o,e,i,a,r,f,u	52	48
36	64	o,d,u,r,i,e,a,n	**G**	e.h.o.r.a.t.f.w.i.s	42	58
7	93	g,e,w,s,c,t	**H**	e,a,i,o	90	10
13	87	f,m,w,e,n,l,d,s,r,h,t	**I**	n,t,s,o,c,r,e,m,a,l	17	83
28	72	y,w,t,s,n,e,c,b,a,c	**J**	u,o,a,e,m,w	88	12
53	47	y,u,i,n,a,r,o,c	**K**	e,i,n,a,t,s	68	32
52	48	m,p,t,i,b,u,o,e,l,a	**L**	e,i,y,o,a,d,u	65	35
69	31	s,d,m,r,i,a,o,e	**M**	e,a,o,i,p,m	71	29
89	11	u,e,o,a,i	**N**	d,t,g,e,a,s,o,i,c	32	68
21	79	o,d,l,p,h,n,e,c,f,s,i,r,t	**O**	n,f,r,u,t,m,l,s,w,o	18	82
47	53	r,l,t,n,i,p,m,a,o,u,e,s	**P**	o,e,a,r,l,u,p,t,i,s	59	41
20	80	o,n,l,e,d,r,s	**Q**	u	100	0
70	30	p,i,u,t,a,o,e	**R**	e,o,a,t,i,s,y	61	39
48	52	d,t,o,u,r,n,s,i,a,e	**S**	t,e,o,i,s,a,h,p,u	41	59
43	57	u,o,d,t,f,e,i,n,s.a	**T**	h,i,o,e,a,t,r	38	62
35	65	p,f,t,l,b,d,s,o	**И**	n,s,t,r,l,p,b,c	8	92
88	12	r,u,o,a,i,e	**V**	e,i,o,a	99	1
48	52	g,d,y,n,s,t,o,e	**W**	a,h,i,e,o,n	80	20
95	5	u,n,i,e	**X**	p,t,i,a,u,c,k,o	38	62
24	76	b,n,a,t,e,r,l	**Y**	a,o,s,t,w,h,i,e,d,m	38	62
88	12	o,n,a,i	**Z**	e,i,w	86	14

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А. Марковым (1856-1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 3. Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Пример решения

Дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

С	В	П	О	О
З	Л	У	Й	Ь
С	Т	Ь	_	Е
Д	П	С	О	К
К	А	Й	З	О

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	О	С	П	О
Л	Ь	З	У	Й
Т	Е	С	Ь	_
П	О	Д	С	К
А	З	К	О	Й

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Задания для учащихся: Расшифровать фразу, зашифрованную шифром перестановки:

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ

15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16. П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
23. ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
24. ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Шифр двойной перестановки

Пример решения

Дан шифр-текст: ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И
Д	Ь	Н	_	Е

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов**2 4 3 5 1:**

О	Ч	Е	Т	Ы
О	_	У	С	Т
С	Р	О	Ч	Н
Р	А	Н	И	Т
Ь	_	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

С	Р	О	Ч	Н
О	_	У	С	Т
Р	А	Н	И	Т
Ь	_	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст: СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задание для учащихся: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛППНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

Шифр простой замены

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 4. Частоты букв русского языка
(в 32-буквенном алфавите со знаком пробела)

-	О	Е,Ё	А

0,175	0,090	0,072	0,062
И 0,062	Т 0,053	Н 0,053	С 0,045
Р 0,040	В 0,038	Л 0,035	К 0,028
М 0,026	Д 0,025	П 0,023	У 0,021
Я 0,018	Ы 0,016	З 0,016	Ь,Ъ 0,014
Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006
Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002

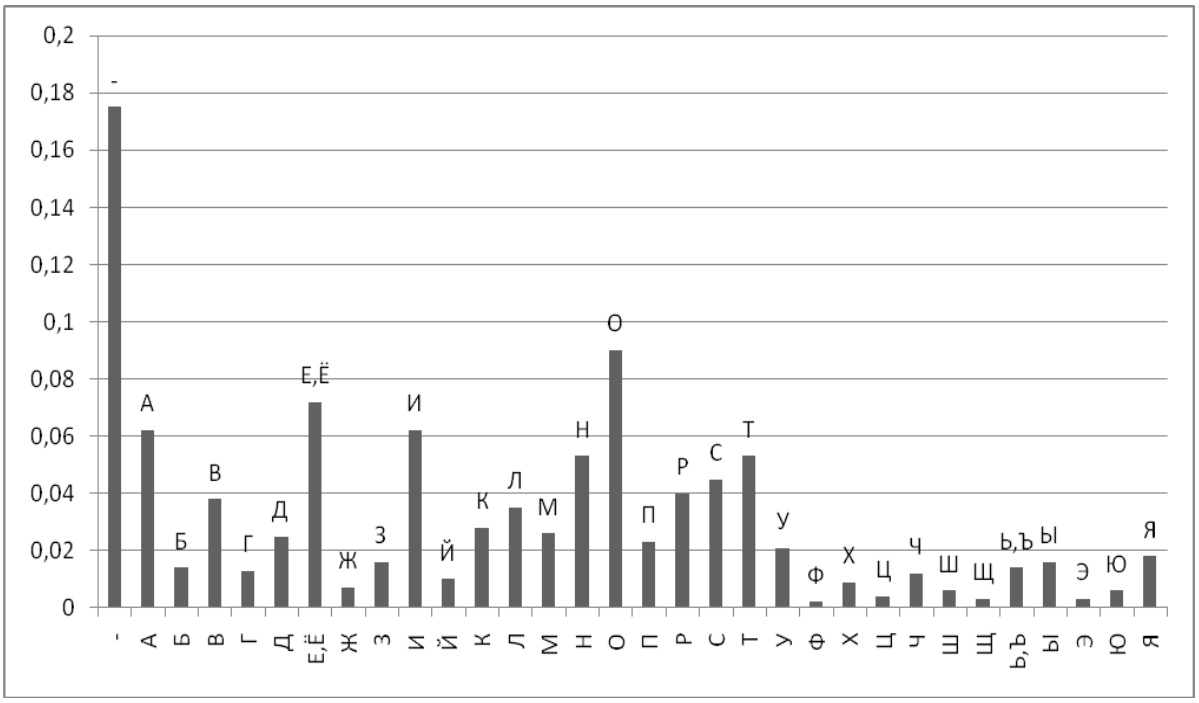


Рисунок 6. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,

СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Таблица 5. Таблица частот биграмм русского языка
ЧАСТЬ 1

	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
И	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	

ЧАСТЬ 2

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
А	26	31	27	3	1	10	6	7	10	1			2	6	9
Б	8	1		6						1	11				2
В	6	19	6	7		1	1	2	4	1	18	1	2		3
Г	7			2											
Д	6	8	1	10			1	1	1		5	1			1
Е	39	37	33	3	1	8	3	7	3	3			1	1	2
Ж		1													
З	3	1		2							4				4
И	11	29	29	3	1	17	3	11	1	1			1	3	17
И	3	10	2				1	3	2						
К	10	3	7	10			1								
Л		3	1	6		4		1			2	30		4	9
М	2	5	3	9	1			2			5	1	1		3
Н	1	9	9	7	1		5	2			36	3			5
О	43	50	39	3	2	5	2	12	4	3			2	3	2
П	41	1		6							2				2

ЧАСТЬ 3

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2
С	8	1	7	1	2	25			6		40	13	3	9	27	11
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5
Ф	2					2			2						1	
Х	4	I	4	1	3	1		2	3		4	3	3	4	18	5

Ц	3					7			10		2				1	
Ч	12					23			13		2			6		
Ш	5					11			14		1	2		2	2	
Щ	3					8			6					1		
Ы		1	9	1	3	12		2	4	7	-3	6	6	3	2	10
Ь		2	4	1	1	2		2	2		6		3	13	2	4
Э											1			1		
Ю		2	1	2	1			3	1		1		1	1	1	3
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6

ЧАСТЬ 4

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Р	1	5	9	16		1	1	1	2		8	3			5
С	4	11	82	6		1	1	2	2		1	8			17
Т	26	18	2	10				1			И	21			4
У	7	14	7			1		8	3	2				9	1
Ф	1	1													
Х	3	4	2	2	1			1							
Ц				1							1				
Ч			7	1					1			1			
Ш				1								1			
Щ				1											
Ы	3	9	4	1		16		1	2						
Ь	1	11	3					1	4				1	3	1
Э		1	9												
Ю	1	1	7				1	1		4					
Я	3	6	10			2	1	4	1	1			1	1	1

Таблица 6. Таблица частот биграмм английского языка
ЧАСТЬ 1

	A	B	C	D	E	F	G	H	I	J	K	L	M

A	4	20	28	52	2	11	28	4	32	4	6	62	23
B	13	0	0	0	55	0	0	0	8	2	0	22	0
C	32	0	7	1	69	0	0	33	17	0	10	9	1
D	40	16	9	5	65	18	3	9	56	0	1	4	15
E	84	20	55	125	51	40	19	16	50	1	4	55	54
F	19	3	5	1	19	21	1	3	30	2	0	11	1
G	20	4	3	2	35	1	3	15	18	0	0	5	1
H	101	1	3	0	270	5	1	6	57	0	0	0	3
I	40	7	51	23	25	9	11	3	0	0	2	38	25
J	3	0	0	0	5	0	0	0	1	0	0	0	0
K	1	0	0	0	11	0	0	0	13	0	0	0	0
L	44	2	5	12	62	7	5	2	42	1	1	53	2
M	52	14	1	0	64	0	0	3	37	0	0	0	7

ЧАСТЬ 2

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	167	2	14	0	83	76	127	7	25	8	1	9	1
B	0	11	0	0	15	4	2	13	0	0	0	15	0
C	0	50	3	0	10	0	28	11	0	0	0	3	0
D	6	16	4	0	21	18	53	19	5	15	0	3	0
E	146	35	37	6	191	149	65	9	26	31	12	5	0
F	0	51	0	0	26	8	47	6	3	3	0	2	0

G	4	21	1	1	20	9	21	9	0	5	0	1	0
H	2	44	1	0	3	10	18	6	0	5	0	3	0
I	202	56	12	1	46	79	117	1	22	0	4	0	3
J	0	4	0	0	0	0	0	3	0	0	0	0	0
K	2	2	0	0	0	6	2	1	0	2	0	1	0
L	2	25	1	1	2	16	23	9	0	1	0	33	0
M	1	17	18	1	2	12	3	8	0	1	0	2	0

ЧАСТЬ 3

	A	B	C	D	E	F	G	H	I	J	K	L	M
N	42	10	47	122	63	19	106	12	30	1	6	6	9
O	7	12	14	17	5	95	3	5	14	0	0	19	41
P	19	1	0	0	37	0	0	4	8	0	0	15	1
Q	0	0	0	0	0	0	0	0	0	0	0	0	0
R	83	8	16	23	169	4	8	8	77	1	10	5	26
S	65	9	17	9	73	13	1	47	75	3	0	7	11
T	57	22	7	1	76	5	2	330	126	1	0	14	10
U	11	5	9	6	9	1	6	0	9	0	1	19	5
V	7	0	0	0	72	0	0	0	28	0	0	0	0
W	36	1	1	0	38	0	0	33	36	0	0	4	1
X	1	0	2	0	0	1	0	0	3	0	0	0	0
Y	14	5	4	2	7	12	2	6	10	0	0	3	7
Z	1	0	0	0	4	0	0	0	0	0	0	0	0

ЧАСТЬ 4

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	7	54	7	1	7	44	124	6	1	15	0	12	0
O	134	13	23	0	91	23	42	55	16	28	0	4	1
P	0	27	9	0	33	14	7	6	0	0	0	0	0
Q	0	0	0	0	0	0	0	17	0	0	0	0	0
R	16	60	4	0	24	37	55	6	11	4	0	28	0
S	12	56	17	6	9	48	116	35	1	28	0	4	0
T	6	79	7	0	49	50	56	21	2	27	0	24	0
U	31	1	15	0	47	39	31	0	3	0	0	0	0
V	0	5	0	0	0	0	0	0	0	0	0	3	0
W	8	15	0	0	0	4	2	0	0	1	0	0	0
X	0	1	5	0	0	0	3	0	0	1	0	0	0
Y	5	17	3	0	4	16	30	0	0	5	0	0	0
Z	0	0	0	0	0	0	0	0	0	0	0	0	0

Пример решения

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

2915 10 17 2922 25 31 15 33 3541 43 45 355745 25 17 59 1510 25 41 25 69,59 78 2982 25 78 25 17 151088 90 78 25 62 25 2210 57 73 79 3567 78 90 88 29 45 3529,54 57 90 31 90 7322 88 15 88 29 1517 69 41 25 15,70 17 90 57 4359 15 78 15 6222 25 17 57 25 6988 1582 17 25 88 29 45 35…

Подсчитаем частоты шифрообразований:

Обозначение	29	15	10	17	22	25	31	33	35	41	43	45	57
Количество	7	10	4	7	4	12	2	1	5	3	2	4	5

Обозначение	59	69	78	82	88	90	62	73	79	67	54	70
Количество	3	3	4	2	6	5	1	2	1	1	1	1

Из таблица частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем Ии А, что не противоречит таблице частот шифр-текста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А $\begin{pmatrix} А \\ И \end{pmatrix}$, 88=$\begin{pmatrix} Н \\ Т \end{pmatrix}$. Теперь третье слово в третьей строке имеет 4 варианта:

- 29=И, 88=Н: 22 Н Е Н И Е
- 29=И, 88=Т: 22 Т Е Т И Е
- 29=А, 88=Н: 22 Н Е Н А Е
- 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…ВТОЛПЕ…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И82 О Р О Л ЕСН 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь41 43 Т ЬВТ О Л П ЕС О 41 О 69,
П Р ИК О Р О Л ЕСН А Р О Д О МС В 73 79 Ь67 Р А Н И Т Ь
И, 54 В А 31 А 73М Н Е Н И ЕЛ 69 41 О Е,
70 Л А В 43П Е Р Е ДМ О Л В О 69Н ЕК Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ: И Е С Л ИМ О Ж Е Ш Ь Б Ы Т ЬВТ О Л П ЕС О Б О Ю,
П Р И К О Р О Л Е С Н А Р О Д О МС В Я З ЬХ Р А Н И Т Ь
И,У В А Ж А Я М Н Е Н И ЕЛ Ю Б О Е,
Г Л А В Ы П Е Р Е Д М О Л В О Ю Н ЕК Л О Н И Т Ь…

Задания для учащихся:

1.

5862323999312958726299581354155631633972841513567715825656565854297756–
3999563156773212155431487663155213397239541672393272625858 15,3762775239133972393239316254397784392131391672629958131554561346163958139516151362124631396272157754561356628431393256765863627233621239546233625852399199622913621246313958135 6.5631633972841582563931314862136276313912393256561672393331395439531256543756773162 58,39377215773954153156621672395677543999581354623131487 6,9516721554126231336258525676565631487 6 167239826258583954.

2.

3925203482636646352025828639517435516620443725275135442090375125255163912011374648252037615114828266823529829125517451247851245946865144742025373 7,37448231113782

5146255134822537828637252751354420903751252548444682782551145118375944,51748235209037594466908225254844376110442018204437,86612025865139668651441066828646513510 37665146513951636639599137.56465186206620824666592435101837785135182025379120903763,4651,66511814206625513582911014294620462044352091143756254878376666148224513920253763,35108651395124374682143744255118377837912537789125203146516151662551392548783937242078
1018355191,2551258210248214593146245114422551185139253744202537592420252548443951743551662044,665637462059,5646515161826674825682253782372527513544209037512525516361829151742066255166463725823744828246664448661420,82661437514666104666463910824639372437442059101835519120.

3.

74292327179971254932293427633225179960
62253495295359822771297799 3427911799714999271560322550271762279527502591325977
952950259959,2599742953255917992591234971251799604925343225719527822732322529501725157799325977629525539529233225179960 341535172799277125122599952945497429.
6295276334277117271225,5027176227952750259132293595295025992917298249836225172750276295253459749925715027532562291732251799491771355329322917
322915492349278232293427633225952950259929771027122525502595593425712932493549
952753279571499525712932492782749549994923328983742599742953595015257425716249992932493549532962258249322977104983591799952591179971.34153562251715273432498325629949822915603225629549822732273249273449177425718983822917174971257112259535232791532982273289.742923271799712549
3229342763322517996095295025998934251799491229279917352562994982495329674927916295251295298282322512252550271762272327324935.

4.

4823184094356253942553
153591354035,5223525340359435402394239152944924238489942364555315185391,2453882362122576942364352449,359449885348942324,4191359123523149155391.47913541496284916235359141238491253129243564352735885394239135,52359135553553359425846429912324,523540152348236253559449244823494035242541499189945394232453915324942315536249125249,125315124960531849942362849155534149.53403594354023,622948622362846235251815622588539425531852352453312394255362354815492723,643524494125242335915523885394942976842540942324356455536438918491622525942364499125256435419125629149885384535249941549491523552524238489353135419135 –
9135.5223523576-

9135645553151853918440244927251884914952351835912453915324629153189435914 9.

5.

79 6131 96 28 35 85 52263024215285594979308879493052795985263024215 9
8542798861283586509628523050,24309674215990593096302485618626968588799679246179112852797831 85,-215030968531216159318511267924967959357931599630315221506179113121963585613185,212679783050286786856130 35:35792424677928243061,3596856121246921359052303 5,617996502152906186119679593 5,42247996794986114930 59,4979527959866949303521592630527911264630618569 86,88795228678630885221422 1,967949618630673052863042286786,42218879963052793052856979,61308559267996783061617930242174306121503031795061214979429621593561863026968629853185..

6.

562754542756513282166349276311307335235489702763274932703516978216677327513056326370296327493273295473274829132982568227955427352718512 9,97562770296330515135156389481 6.16631511513082294965275432633049296127633248 30-275651351556302332271170273527183256296389823023,27823051305111157335295470274965323830633073353223568216677049563529971 6.8227495127135129543027822773164956326370296327493273295482159516732735327015563038326332 92-732754113061301882325130496327182982821667613092295616.27824916821663613092295616732754131524511632709227242963732749561673298289513013.

7.

342868911383106527684910266527687526397853758353182636629 1.2610745313491083106553533668722810281318861027537539836857261810915357365365286891 10,836875271334132413185336745336107410365736 13,83687410911091103613682674186234102710361075261386396874361 0.831810342810,2657265062276883686557861 3.265726491083106553341913275375395334751375685068158318688353261027 53.491083106553102774687268274 4,836828726818133480137268911075271 0,83682610,752610186815682813862862531396132713741018752634-911336266827105 3,74108613267544,341027131839443674 53.34831853656886131526139136682653961 0,53184428689123266826287875751036281318-342644365727726827683457343468186826,23261074531572185347 –752613183444263653 74,862857965315,7468722810181036133668138653346826366813537583577526532628576 5.

Заключение

Важность криптографии в защите информации, как это было показано в книге, трудно переоценить. Однако, современные системы защиты информации используют и другие методы и способы обеспечения информационной безопасности информационных и телекоммуникационных систем и сетей. В основе каждого из этих методов или способов лежат математические законы или физические явления, требующие отдельного внимательного рассмотрения. Настоящим пособием авторы открывают целую серию методических пособий для учителей инженерных классов, посвященную современным системам обеспечения информационной безопасности, информационно-телекоммуникационным системам и сетям, и их программному обеспечению.

Список использованной литературы

1. Бабаш А.В. и др. Информационная безопасность. История защита информации в России: Учебное пособие /Под редакцией А.В. Бабаш, Е.К. Баранова, Д.А. Ларина. – М.: КДУ, 2015.
2. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2014.
3. Бутырский Л.С., Ларин Д.А., Шанкин Г.П. Криптографический фронт Великой Отечественной. – М.: Гелиос АРВ, 2013.
4. Синх С. Книга шифров: тайная история шифров и их расшифровки. – М.: Мир энциклопедий Аванта+, 2009.
5. Черчхауз Р.Ф. Коды и шифры. Юлий Цезарь, «Энигма», Интернет. – М.: Издательство «Весь Мир», 2005.
6. Кан Д. Война кодов и шифров. – М.: Рипол Классик, 2004.
7. Соболева Т.А. История шифровального дела в России. – М.: ОЛМА-ПРЕСС-Образование, 2002.
8. Кан Д. Взломщики кодов. – М.: Центрполиграф, 2000.
9. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для вузов / Под ред. В.А. Садовничего. – М.: Высш. шк., 1999.
10. Жельников В. Криптография о папируса до компьютера. – М.: ABF, 1996.
11. Болелов Э.А. Криптографические методы защиты информации. Часть 1. Симметричные криптосистемы. – М.:МГТУ ГА, 2011.
12. Болелов Э.А. Криптографические методы защиты информации. Часть 2. Асимметричные криптосистемы. – М.:МГТУ ГА, 2013.
13. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2010.
14. Харин Ю.С. и др. Математические и компьютерные основы криптологии: Учеб. пособие. – Мн.: Новое знание, 2003.

15. Танова Э.В. Введение в криптографию: как защитить свое письмо от любопытных. Элективный курс: учебное пособие. – М.: БИНОМ. Лаборатория знаний, 2007.
16. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – М.: Горячая линия-Телеком, 2002.
17. Бабаш А.В., Шанкин Г.П. Криптография. /Под редакцией В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007.
18. Фомичев В.М. Дискретная математика и криптология. Курс лекций /Под ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.
19. Шеннон К. Теория связи в секретных системах. – М.: ИЛ, 1963.