Городская открытая научно-практическая конференция

 школьников и студентов «Содружество»

Тема: Криптология: точки соприкосновения математики и языкознания

АВТОР: Пушко Дарья

Россия, г.Зеленогорск

Красноярского края

школа №164, 10А класс

РУКОВОДИТЕЛИ: Камышенко Г.Н.,

Линдт Т.Л.

учителя гимназии №164

Зеленогорск

2006

**ОГЛАВЛЕНИЕ**

|  |  |
| --- | --- |
| ВВЕДЕНИЕ  | 3 |
| I ГЛАВА КРИПТОГРАФИЯ: ИСТОРИЯ И СОВРЕМЕННОСТЬ ТАЙНОПИСЬ В РОССИИ ШИФРЫ ПОДПОЛЬЯ ДВОИЧНАЯ СИСТЕМА СЧИСЛЕНИЯ В ЦИФРАХ  | 4-7810 |
| II ГЛАВА РОЛЬ ЯЗЫКА В СОСТАВЛЕНИИ И РАЗГАДКЕ ШИФРОВ ЛИТЕРАТУРНЫЙ КРИПТОАНАЛИЗ ЗАКЛЮЧЕНИЕ  | 11-1417 |
| СПИСОК ЛИТЕРАТУРЫ  | 18 |
|  |  |

**ВВЕДЕНИЕ**

Уже неоднократно обсуждалась проблема совмещенного изучения двух, а то и несколько предметов школьной программы. В жизни невозможно обойтись без предметов, которые являются базовыми для школьной программы: элементарных основ физики, математики, химии, литературы, информатики. Изучая каждый предмет по отдельности, трудно понять всю его значимость и роль. Существуют и такие науки, где важен не только математический склад ума и умение использовать законы естественных наук, но и знания в гуманитарной области.

Неоспорим и тот факт, что все наиболее существенные открытия нашего времени происходят не в одной изолированной науке, а при непосредственном взаимодействии с другими дисциплинами. Следствием этого является важность междисциплинных проблем, однако основной акцент пока делается лишь на связях между предметами одного цикла – только естественного или гуманитарного. Между тем наука давно уже осознала и признала необходимость «наведения мостов» между естественными и гуманитарными дисциплинами, такими как языкознание и математика. В связи с введением профильного обучения большое значение приобрела проблема создания такого курса, который бы объединял две центральные дисциплины каждого цикла – языкознание и математику, представляется весьма **актуальной**. Наука криптология как раз совмещает в себе два этих основных предмета школьного образования.

**Цель работы**: изучив литературу по криптологии, выявить связь между лингвистикой и математикой.

Логичным следствием этого явились поставленные нами **задачи**:

* выяснить, что включает в себя понятие «криптология»;
* узнать, какие известны способы шифрования;
* изучить сферы использования шифров;
* выявить роль языка в разгадке шифров.

**I ГЛАВА**

**КРИПТОГРАФИЯ: ИСТОРИЯ И СОВРЕМЕННОСТЬ**

Исторически криптография зародилась из потребности передачи секретной информации. Длительное время она была связана только с разработкой специальных методов преобразования информации с целью ее представления в форме недоступной для потенциального злоумышленника. С началом применения электронных способов передачи и обработки информации задачи криптографии начали расширяться.

В настоящее время, когда компьютерные технологии нашли массовое применение, проблематика криптографии включает многочисленные задачи, которые не связаны непосредственно с засекречиванием информации. Современные проблемы криптографии включают разработку систем электронной цифровой подписи и тайного электронного голосования, протоколов электронной жеребьевки и идентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и т.п. Специфика криптографии состоит в том, что она направлена на разработку методов, обеспечивающих стойкость к любым действиям злоумышленника, в то время как на момент разработки криптосистемы невозможно предусмотреть все способы атаки, которые могут быть изобретены в будущем на основе новых достижений теории и технологического прогресса.

Криптоанализ – наука (и практика ее применения) о методах и способах вскрытия шифров. Криптография и криптоанализ составляют единую область знаний – криптологию, которая в настоящее время является областью современной математики, имеющий важные приложения в современных информационных технологиях.

Термин «криптография» ввел Д.Валлис. Потребность шифровать сообщения возникла очень давно. В V – VI вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли скиталами. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полоску папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное он мог, только взяв свою скиталу и намотав на нее без пропусков эту полосу.

Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать его лентой с шифрованным сообщением, сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так можно определить диаметр скиталы.

В Древней Греции (II в. до н. э.) был известен шифр, называемый **«квадрат Полибия»**. Это устройство представляло собой квадрат 5\*5, столбцы и строки которого нумеровались от 1 до 5. В каждую клетка этого квадрата записывалась одна буква (в греческом алфавит одна клетка оставалась пустой, а в латинском в одну клетку записывалось две буквы: I, J).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 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 |

В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

 Например[[1]](#footnote-1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13  | 34 | 22 | 24 | 44 | 34 | 15 | 42 | 22 | 34 | 43 | 45 | 32 |
| C  | O | G | I | T | O | E | R  | G | O | S | U | M |

**Шифр Цезаря**

В I в до н. э. Гай Юлий Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (А) на четвертую (D), вторую (В) – на пятую (Е), наконец, последнюю – на третью:

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

Сообщение об одержанной им победе выглядело так: YHQL YLGL YLFL[[2]](#footnote-2)

Император Август (I в. до н. э.) в своей переписке заменял первую букву на вторую, вторую – на третью и т.д., наконец, последнюю – на первую:

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

Его любимое изречение было: GFTUJOB MFOUF[[3]](#footnote-3)

Квадрат Полибия, шифр Цезаря входят в класс шифров, называемых «подстановка» или «простая замена». Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь комбинация.

К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В каждом из них в прямоугольник [n\*m] сообщение вписывается заранее обусловленным способом, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв ключа – буквенного ключевого слова. Так, ниже в первом прямоугольнике столбцы нумеруются в обычном порядке следования – слева направо, а во втором – в порядке следования букв слова «Петербург».

Используя расположение букв этого ключа в алфавите, получим набор чисел
[5 3 8 4 6 1 9 7 2]:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | 3 | 8 | 4 | 6 | 1 | 9 | 7 | 2 |
| п | р | и | л | е | п | л | я | я |
| с | я | п | р | е | м | у | д | р |
| у | м | п | р | е | м | у | д | р |
| б | у | д | е | ш | ь | а | б | в |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| п | р | и | л | е | п | л | я | я |
| р | д | у | м | е | р | п | я | с |
| у | м | п | р | е | м | у | д | р |
| в | б | а | ь | ш | е | д | у | б |

В первом случае шифрованный текст найдем, если будем выписывать буквы очередного столбца в порядке следования столбцов (прямом или обратном), во втором, - если будем выписывать буквы столбца в порядке следования букв ключа. Таким образом будем иметь:

1. прувр дмбиу палмр ьеееш прмел пудяя дуясрб;
2. пммья ррвря мулрр епсуб еееешя ддбил пдлууа.

К классу «перестановка» принадлежит и шифр, называемый **«решетка Кардано»**. Это прямоугольная карточка с отверстиями, чаще всего квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов в карточке четно. Карточка сделана так, что при ее последовательном использовании (поворачивании) каждая клетка лежащего под ней листа окажется занятой. Карточку сначала поворачивают вдоль вертикальной оси симметрии на 180є, а затем вдоль горизонтальной оси также на 180є. И вновь повторяют ту же процедуру:

Если решетка Кардано – квадрат, то возможен второй вариант самосовмещений фигуры, а именно, последовательные повороты вокруг центра квадрата на 90є.

Рассмотрим примеры:

Легко прочесть зашифрованное квадратной решеткой Кардано сообщение:

«вавочс муноти мыжрое ьухсой мдосто яаснтв»[[4]](#footnote-4)

Второе сообщение:

«ачшдеалб еымтяовн лыриелбм

оянгеаюш дтинрент еоеыпрни»[[5]](#footnote-5)

также нетрудно расшифровать, пользуясь прямоугольной решеткой.

**ТАЙНОПИСЬ В РОССИИ**

Первое известное применение тайнописи в России относится к XIII в. Эту систему называли **«тарабарской грамотой»**. В этой системе согласные буквы заменяются по схеме:

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

(при шифровании буквы, расположенные на одной вертикали, переходят одна в другую), остальные буквы остаются без изменения. Так, известная пословица, записанная этим шифром, выглядит так: «МЫЩАЛ ЧОСОШ ЫСПИЕК»[[6]](#footnote-6).

Образцом алфавита, придуманного во второй половине XVII в. специально для передачи секретных сообщений, может служить **тайнопись «уголки»** и ключ к ней. Эта тайнопись состоит в замене обычных букв угольниками и четырехугольниками, заимствованными из решетки, составленной из двух параллельных линий, пересеченных двумя такими же линиями под прямым углом. В полученных клетках размещены по четыре и три буквы в порядке следования букв алфавита. В тайнописи буквы заменяются, при этом первая – простым угольником, а следующие – те же угольником с одной, двумя или тремя точками, смотря по месту буквы в нем.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| а |  | б |  | в |  | г |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| д |  | е |  | ё |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ж |  | з |  | и |  | й |

 |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| к |  | л |  | м |  | н |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| о |  | п |  | р |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| с |  | т |  | у |  | ф |

 |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| х |  | ц |  | ч |  | ш |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| щ |  | ъ |  | ы |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ь |  | э |  | ю |  | я |

 |

Ключ к шифру «уголки»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **.** |  | **:** |  | **:.** |

 |

В эпоху Петра I в качестве системы шифрования широко употреблялась «цифирь» или **«цифирная азбука»**. Цифирь – это шифр простой замены, в котором буквам сообщения соответствовали шифрообозначения, представляющие собой буквы, слоги, слова или какие-нибудь другие знаки. При этом использовались и «пустышки» - шифрообозначения, которым не соответствовали никакие знаки открытого текста, то есть передаваемого сообщения. В госархиве сохранились письма Петра, в которых он передавал цифири различным деятелям для корреспонденции (П.А.Толстому, А.Д.Меньшикову и т.д.).

В эпоху царствования Елизаветы Петровны обычным делом была перлюстрация переписки иностранных дипломатов. Результаты этой «работы» несколько раз в месяц докладывались царице. Некоторое время «специалисты» по перлюстрации пропускали те места корреспонденций, смысл которых им был непонятен. В 1742 г. канцлер А.П.Бестужев-Рюмин пригласил на службу в коллегию иностранных дел математика, академика Петербургской АН Христиана Гольдбаха. С этого времени перлюстраторам было дано распоряжение тщательно копировать письма, не опуская при этом кажущихся им мелочей. В результате только за июль – декабрь 1743 г. Х.Гольдбах смог дешифровать 61 письмо министров прусского и французского дворов. В итоге переписка иностранных послов в конце XVIII в. перестала быть тайной для дешифровальной службы России. За свою успешную работу Х.Гольдбах был пожалован в тайные советники с ежегодным окладом в 4500 руб.

**ШИФРЫ ПОДПОЛЬЯ**

1. **Тюремная азбука** – аналог квадрата Полибия.

Она позволяла путем перестукивания сообщаться заключенным разных камер. Эта азбука устроена так: в прямоугольник 6\*5 записываются буквы русского алфавита в обычном порядке следования, кроме букв «Ё», «Й» и «Ъ». В результате получается таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | А | Б | В | Г | Д |
| 2 | Е | Ж | З | И | К |
| 3 | Л | М | Н | О | П |
| 4 | Р | С | Т | У | Ф |
| 5 | Х | Ц | Ч | Ш | Щ |
| 6 | Ь | Ы | Э | Ю | Я |

 Каждая из основных букв русского алфавита (без букв «Ё», «Й» и «Ъ») определяется парой чисел – номером строки и столбца. Поэтому вопрос: «Кто здесь?» изображается следующим образом:

**.. ..... .... ... ... .... .. ... . ..... .. . .... .. ...... . .... ......**

1. **Парный шифр**, ключом которого являетсяфраза, содержащая 15 разных букв. Подписывая под этими буквами буквы в алфавитном порядке, не вошедшие в этот ключ, получаем разбиение 30 основных букв русского алфавита на пары. Чтобы получить из сообщения шифрованный текст, заменяют каждую букву сообщения своим напарником. Так, выбирая в качестве ключа фразу «железный шпиц дома лежит», получим разбиение основных букв русского алфавита на пары, как указано ниже:

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

ЖЕЛЕЗНЫЙ ШПИЦ ДОМА ЛЕЖИТ

Б В Г К Р С У Ф Х Ч Щ Ь Э Ю Я

Таким образом, получаем отображение букв основного алфавита (без букв «Ё», «Й» и «Ъ») на последовательность, состоящую из тех же букв:

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

Поэтому сообщение «Встреча отменяется, явка раскрыта», переходит в следующий шифротекст: «ЕЫЯНВ ЦЮЬЯЭ ВРТВЯ ЫТТЕЗ ЮНЮЫЗ НСЯЮ»

Очевидно, что в качестве ключа можно также использовать любую фразу, в которой имеется не менее 15 разных букв основного алфавита.

1. **По стихотворению** – вариант шифра «по книге».

Корреспонденты договариваются о достаточно объемном стихотворном произведении, которое заучивают наизусть. Например, роман «Евгений Онегин» или поэма «Кому на Руси жить хорошо». Каждую букву сообщения шифруют парой чисел – номером строки, где встречается эта буква, и номером буквы в ней.

Пусть выбрана поэма «Кому на Руси жить хорошо». Пролог поэмы начинается строфой:

|  |  |  |  |
| --- | --- | --- | --- |
| 12345678 | В каком году – рассчитывай,В какой земле – угадывай,На столбовой дороженькеСошлись семь мужиков:Семь временнообязанных,Подтянутой губернииУезда Терпигорева,Пустопорожней волости, | 910111213141516 | Из смежных деревень:Заплатова, Дырявина,Разутова, Знобишина,Горелова, Неелова – Неурожайка тож,Сошлися и сзаспорили:Кому живется весело,Вольготно на Руси? |

Для удобства шифрования (выбранного стихотворения) записывают в виде таблицы нижеследующим способом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |  |
| 1 | В | к | а | к | о | м | г | о | д | у | р | а | с | с | ч | и | т | ы | в | а | й | 1 |
| 2 | В | к | а | к | о | й | з | е | м | л | е | у | г | а | д | ы | в | а | й |  |  | 2 |
| 3 | Н | а | с | т | о | л | б | о | в | о | й | д | о | р | о | ж | е | н | ь | к | е | 3 |
| 4 | С | о | ш | л | и | с | ь | с | е | м | ь | м | у | ж | и | к | о | в |  |  |  | 4 |
| 5 | С | е | м | ь | в | р | е | м | е | н | н | о | о | б | я | з | а | н | н | ы | х | 5 |
| 6 | П | о | д | т | я | н | у | т | о | й | г | у | б | е | р | н | и | и |  |  |  | 6 |
| 7 | У | е | з | д | а | Т | е | р | п | и | г | о | р | е | в | а |  |  |  |  |  | 7 |
| 8 | П | у | с | т | о | п | о | р | о | ж | н | е | й | в | о | л | о | с | т | и |  | 8 |
| 9 | И | з | с | м | е | ж | н | ы | х | д | е | р | е | в | е | н | ь |  |  |  |  | 9 |
| 10 | З | а | п | л | а | т | о | в | а | Д | ы | р | я | в | и | н | а |  |  |  |  | 10 |
| 11 | Р | а | з | у | т | о | в | а | З | н | о | б | и | ш | и | н | а |  |  |  |  | 11 |
| 12 | Г | о | р | е | л | о | в | а | Н | е | е | л | о | в | а |  |  |  |  |  |  | 12 |
| 13 | Н | е | у | р | о | ж | а | й | к | а | т | о | ж |  |  |  |  |  |  |  |  | 13 |
| 14 | С | о | ш | л | и | с | я | и | з | а | с | п | о | р | и | л | и |  |  |  |  | 14 |
| 15 | К | о | м | у | ж | и | в | е | т | с | я | в | е | с | е | л | о |  |  |  |  | 15 |
| 16 | В | о | л | ь | г | о | т | н | о | н | а | Р | у | с | и |  |  |  |  |  |  | 16 |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |  |

Пользуясь такой таблицей, нетрудно шифровать и расшифровывать любое сообщение, например:

«14,5 5,5 7,5 5,10 2,5 2,1 2,12 6,3 8,5 15,7 13,2 7,8 14,7 7,6 5,4 6,6 7,2 12,5 5,4 11,3 10,13 5,15 2,1 15,1 1,16 3,3 5,3 6,14 13,1 4,5 8,4 5,4».[[7]](#footnote-7)

**ДВОИЧНАЯ СИСТЕМА СЧИСЛЕНИЯ В ЦИФРАХ**

Языкознание и информатика – казалось бы, предметы абсолютно несовместимые. Но как представить текстовую информацию на ЭВМ, если для компьютера вся система счисления представлена в виде двоичного кода? В этом опять помогает криптография с ее возможностью кодировать и декодировать информацию разными методами. Мы попытались рассмотреть ее роль и в этом аспекте.

Итак, общий вид числа принято записывать так: an an-1 an-2…a1 a0.

Это число в десятичной системе счисления может быть представлено следующей записью: an\*10n + an-1\*10n-1+an-2\*10n-2…+a1\*101 +a0\*1010.

Если обозначить через d основание системы счисления, то для перевода записи числа из десятичной в данную систему нужно последовательно делить его на d так, как показано ниже. Например, запишем число 74 в двоичной системе счисления.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 74 |  |  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 6 |  |  | 37 |  |  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 14 |  |  | 2 |  |  | 18 |  |  | 2 |  |  |  |  |  |  |  |  |  |
|  | 14 |  |  | 17 |  |  | 18 |  |  | 9 |  |  | 2 |  |  |  |  |  |  |
|  | 0 |  |  | 16 |  |  | 0 |  |  | 8 |  |  | 4 |  |  | 2 |  |  |  |
|  |  |  |  | 1 |  |  |  |  |  | 1 |  |  | 4 |  |  | 2 |  |  | 2 |
|  |  |  |  |  |  |  |  |  |  |  |  |  | 0 |  |  | 2 |  |  | 1 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 0 |  |  |  |

В итоге получаем число: (0)1001010

1001010(2) = 1\*26 + 0\*25 + 0\*24 + 1\*23 + 0\*22 + 1\*21 + 0\*01=74(10)

Для составления и расшифровки шифрограмм используются квадратные решетки 8\*8 (решетка Кардано); поэтому, если запись числа в двоичной системе содержит меньше цифр, то слева приписывают нули, чтобы всего было 8 (в примере он приписан слева, так как цифр получилось семь).

Ниже показано построение решетки с помощью чисел в двоичной системе счисления (1 – вырезать, 0 – нет).

Так у нас получится следующая шифрограмма:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Х | Н | Г | Е | А | Л | Б | Л |
| Я | В | И | Е | Д | О | К | Л |
| И | Р | Е | Н | Х | Е | Л | Г |
| А | П | С | Б | У | О | Т | В |
| О | Г | П | Л | Я | Д | У | Л |
| Н | О | И | С | Е | Н | В | Т |
| Е | Ы | Ж | Д | Д | Н | З | У |
| Н | А | М | Л | Ы | В | Ь | И |

**II ГЛАВА**

«На берегу пустынных волн

Стоял он, дум великих полн,

И вдаль глядел...»

**РОЛЬ ЯЗЫКА В СОСТАВЛЕНИИ И РАЗГАДКЕ ШИФРОВ**

Термин «шифр» имеет арабское происхождение. В начале XV в. арабы опубликовали энциклопедию «Шауба Аль-Аща», в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. В этом разделе есть и перечень букв в порядке их повторяемости на основе изучения текста Корана. Заметим, что и для русского алфавита есть подобный перечень.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Буква | Относит. частота | № | Буква | Относит. частота | № | Буква | Относит. частота |
| 0123456789 | абвгде, ёжзий | 0,0620,0140,0380,0130,0250,0720,0070,0160,0620,010 | 10111213141516171819 | клмнопрсту | 0,0280,0350,0260,0530,0900,0230,0400,0450,0530,021 | 2021222324252627282930 | фхцчшщыь, ъэюя | 0,0020,0090,0040,0120,0060,0030,0160,0140,0030,0060,018 |

Итак, в русском тексте чаще всего встречается буква «О», затем буква «Е» и на третьем месте стоят буквы «И» и «А». Реже всего – буквы «Щ» и «Ф».

Неудобство шифров типа «подстановка» в случае использования стандартного алфавита очевидно. Таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для дешифрования всего сообщения. Поэтому обычно пользуются разными приемами, чтобы затруднить дешифрование. Для этой цели используют многобуквенную систему шифрования – систему, в которой одному символу отвечает одна или несколько комбинаций двух и более символов. Другой прием – использование нескольких алфавитов. В этом случае для каждого символа употребляют тот или иной алфавит в зависимости от ключа, который связан каким-нибудь способом с самим символом или с его порядком в передаваемом сообщении.

В процессе шифрования (и дешифрования) используется таблица **(«таблица Виженера»**), которая устроена следующим способом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите. Ниже представлена таблица, составленная из 31 буквы русского алфавита (без букв «Ё» и «Ъ»). Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово – ключ (например, «монастырь») и подписывается с повторением над буквами сообщения.

Таблица Виженера

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

Чтобы получить шифрованный текст, находят очередной знак ключа, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном. В данном примере сначала находим столбец, отвечающий букве «М» ключа, а затем строку, соответствующую букве «Р» открытого текста. На пересечении выделенных столбца и строки находи букву «Э». Так продолжая дальше, находим шифрованный текст полностью:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| м | о | н | а | с | т | ы | р | ь | м | о | н | а | с | т | ы | р | ь | м | о | н |
| р | а | с | к | и | н | у | л | о | с | ь | м | о | р | е | ш | и | р | о | к | о |
| э | о | я | к | щ | а | п | ы | й | ю | й | щ | о | в | ч | ф | ш | л | ь | ш | ы |

Наконец, к сообщению можно применять несколько систем шифрования.

Аббат Тритемиус – автор первой печатной книги о тайнописи (1518 г.) – предложил несколько шифров и среди них шифр, который можно считать усовершенствованием шифра Г.Ю.Цезаря. Этот шифр устроен так. Все буквы алфавита нумеруются по порядку (от 1 до 33 в русском варианте). Затем выбирают какой-нибудь ключ, например «Вологда», и подписывают сообщением с повторением, как показано ниже:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| о | п | е | р | а | ц | и | я | н | а | ч | и | н | а | е | т | с | я | в | в | о | с | к | р | е | с | е | н | ь | е |
| в | о | л | о | г | д | а | в | о | л | о | г | д | а | в | о | л | о | г | д | а | в | о | л | о | г | д | а | в | о |

Чтобы получить шифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 33, то из нее вычитают 33. В результате получается последовательность чисел от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст. Разбивая этот текст на группы особой длины (например, по 5), получают шифрованное сообщение:

«СЯСАД ЫЙВЭМ ЖМТБЗ ВЮОЁЖ ПФЪЭФ ХЙОЯФ»

Если под ключом понимать однобуквенное слово «В» (в русском варианте), то мы получим шифр Г.Ю.Цезаря. В этом случае для того же текста шифрованное сообщение принимает вид

«СТЗУГ ЩЛВРГ ЪЛРГЗ ХФВНЕЕ СФНУЗ ФЗРЯЗ»

Появившийся в XVIII в. шифр «по книге» можно рассматривать как дальнейшее усовершенствование шифра Г.Ю.Цезаря. Чтобы воспользоваться этим шифром, два корреспондента договариваются об определенной книге, имеющейся у каждого из них. Например, Я.Гашек «Похождения бравого солдата Швейка» (Москва, 1997). В качестве ключа каждый из них может выбрать «слово» той же длины, что и передаваемое сообщение. Этот ключ кодируется парой чисел, а именно номером страницы и номером строки на ней, и передается вместе с шифрованным сообщением. Например, (287,2) определяет «слово», то есть текст избранной книги: «Внимательно прочитав эту страницу, офицеры ничего не поняли…». Этому ключу отвечает последовательность чисел (от 1 до 33):

В н и м а т е л ь н о п р о ч и т а в э т у с т р а н и ц у…

03 15 10 14 01 20 06 13 30 15 16 17 18 16 25 10 20 01 03 31 20 21 19 20 18 01 15 10 24 21…

Зная этот ключ, можно легко расшифровать переданное сообщение. Например,

«РОНЮП ЕЧХВШ РХЩЮЩ ХУШРМ ШВЧФА»[[8]](#footnote-8)

Примером нераскрываемого шифра может служить «одноразовый шифровальный блокнот» - шифр, в основе которого лежит та же идея, что и в алфавите Г.Ю.Цезаря. Назовем расширенным алфавитом совокупность букв алфавита, знака пробела между словами и знаков препинания [. , : ; ! ? ( ) – “]. Число символов расширенного алфавита в русском варианте равно 44. Занумеруем символы расширенного алфавита числами от 0 до 43. Тогда любой передаваемый текст можно рассматривать как числовую последовательность {an} множества А={0, 1, 2, …, 43}.

Предположим, что имеем случайную последовательность {сn} из чисел множества А той же длины, что и передаваемый текст (ключ). Складывая по модулю 44 число an передаваемого текста с соответствующим числом сn ключа

an + сn ≡ bn (mod 44), 0 ≤ bn ≤ 43,

получим последовательность {bn} знаков шифрованного текста. Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

an ≡ сn - bn (mod 44), 0 ≤ an ≤ 43,

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота. В каждом из них на нескольких листах напечатана случайная последовательность чисел множества А. Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет его второму абоненту, получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Нетрудно увидеть, что одноразовый шифр не раскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

Случайная последовательность чисел множества А может быть получена при помощи «вертушки со стрелкой». Обод вертушки разделен на 44 равные части (дуги). Каждая из них помечена числами от 0 до 43. Запуская вертушку, получим какое-нибудь из чисел множества А. Продолжая так дальше, можем получить случайную последовательность любой длины.

С появлением радио- и телеграфных линий всякую информацию удобно передавать, используя двоичный код, например азбуку Морзе. В современных системах шифрования обычно шифруют сообщения, записанные двоичным кодом (чередование 0 и 1).

**ЛИТЕРАТУРНЫЙ КРИПТОАНАЛИЗ**

Первые шаги литературного криптоанализа связаны с появлением рассказа американского писателя Эдгара По «Золотой жук». Этот рассказ и по сей день остается непревзойденным художественным произведением на тему о дешифровании.

Про Эдгара По можно сказать, что он неизбежно должен был заинтересоваться криптоанализом. Хотя По неоднократно пространно рассуждал о логике и писал рассказы с логично построенными сюжетами, он увлекался и такими иррациональными предметами, как френология и гипноз. А поскольку криптоанализ обладал качествами, которые импонировали Эдгару По в науках, и вместе с тем от криптоанализа исходил неземной свет мистики; двойственный характер этой области человеческих знаний пришелся впору раздвоенной натуре По. Научность импонировала интеллекту писателя, а таинственность была созвучна его эмоциям. Первые упоминания о криптоанализе у По появились в статье «Загадочное и головоломное», и уже позже отразились в его литературных творениях детективного характера.

Чтобы поподробнее рассмотреть использование криптографии в рассказе «Золотой жук», мы приводим отрывок из этой книги:

«... Легран разогрел пергамент и дал его мне. Между черепом и козленком, грубо начертанные чем-то красным, стояли такие знаки:

53##+305))6\*;4826)4#.)4#.);806\*,48+8||60))85;;]8\*;:#\*8+83(88)5\*+;46(;88\*96\*?;8)\*#(;485):5\*+2:\*#(;4956\*2(5\*=4)8||8\*;4069285);)6+8)4##;1#9;48081;8:8#1;48+85;4)485+528806\*81(#9;48;(88;4(#?34;48)4#;161;:188#?

* Что ж! – сказал я, возвращая Леграну пергамент, - меня это не подвинуло ни на шаг...
* И все же, - сказал Легран, - она не столь трудна, как может сперва показаться. Эти знаки, конечно, - шифр; иными словами, они скрывают словесную запись...

... Прежде всего, как всегда в этих случаях, возникает вопрос о языке криптограммы. Принцип решения (в особенности это относится к шифрам простейшего типа) в значительной мере зависит от языка. Выяснить этот вопрос можно только одним путем, испытывая один язык за другим и постепенно их исключая, пока не найдешь решение. С нашим пергаментом такой трудности не было; подпись давала разгадку. Игра словами «kid» и «Kidd» возможна лишь по-английски. Если бы не это, я начал бы поиски с других языков... Но я уже знал, что криптограмма написана по-английски.

... Как видите, текст криптограммы идет в сплошную строку. Задача намного была бы проще, если б отдельные слова были выделены просветами... Но просветов в строке не было, и я принялся подсчитывать однотипные знаки, чтобы узнать, какие из них чаще, какие реже встречаются в криптограмме. Закончив подсчет, я составил такую таблицу:

|  |  |
| --- | --- |
| Знак | Сколько раз встречается |
| 8;4)#\*56+109 и 2: и 3?||= и ] | 342719161514121187654321 |

В английской письменной речи самая частая буква – Е. Далее идут в нисходящем порядке: A, O, I, D, H, N, R, S, T, U, Y, C, F, G, L, M, W, B, K, P, Q, X, Z».

В процессе расшифровывания герой приходит к следующему результату:

|  |  |  |
| --- | --- | --- |
| Знак | Сколько раз встречается | Какую букву означает |
| 8;4)#\*56+ | 34271916151412118 | ethronaid |

Вот криптограмма представлена в расшифрованном виде:

«A good glass in the bishop’s hostel in the devil’s seat twenty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death’s head a bee line from the tree through the shot fifty feet out»

(Хорошее стекло в трактире епископа на чертовом стуле – 21°15` северо-северо-восток – главный сук седьмая ветвь восточная сторона – стреляли из левого глаза мертвой головы – прямая от дерева через выстрел на 50 футов.)

Итак, вот что значили слова из непонятного изречения:

Трактир епископа – со старинной фамилией Веззор, владельцы усадьбы в 4 милях к

северу от острова;

высокий скалистый утес – название;

чертов стул – в скале ниша в виде кресла;

хорошее стекло – подзорная труба (выражение моряков);

21°15` северо-северо-восток – указывает на положение трубы;

она показывает на дерево, где находится череп;

пустить пулю в левую глазницу;

через выстрел прямо от ствола на 50 футов вперед – там клад.

Расшифровав каждое из слов послания, герой смог отыскать зарытые сокровища.

«Золотой жук» Эдгара По – не единственное литературное произведение, в котором использованы шифрограммы. Среди них и «Момент истины» В.О.Богомолова, и «Дети капитана Гранта» Ж.Верна, и «В круге первом» А.И.Солженицына, но наиболее необычно показано шифрование в книге А.К.Дойля «Пляшущие человечки». В своей книге автор использует не привычные буквы, числа, символы или принцип решетки, а ... «пляшущих человечков». Изображаемые человечки выполняют ту же функцию, что и знаки в криптограмме. Каждая фигурка отличалась от всех остальных, при этом означая какую-либо букву алфавита. Приводим некоторые из шифровок из книги:

1. ИЛСИПРИХОДИ

1. НИКОГДА

1. ЯЗДЕСЬАБСЛЕНИ

А ключ к разгадке шифра лежит в основах языка:

* + повторяемость гласных чаще, чем согласных букв;
	+ в русском языке чаще остальных повторяются буквы «О», «А» и «Е»;
	+ логическая связь между словами.

 **ЗАКЛЮЧЕНИЕ**

В ходе работы над данной темой мы пришли к следующим выводам:

1. Наука, занимающаяся способами преобразования информации с целью ее защиты от незаконных пользователей, называется криптографией. А криптоанализ – наука (и практика ее применения) о методах и способах вскрытия шифров. Вместе они образуют область знаний, называемую криптологией.
2. Существует два класса шифров:
* «перестановка», или «маршрутная транспозиция»;
* «подстановка», или «простая замена».
1. Практика шифрования зародилась еще до нашей эры в Древней Греции. Первым дешифровальщиком был Аристотель. Позже появились такие шифры, как
* «Квадрат Полибия»;
* «Шифр Цезаря» (он находит применение и сегодня, но в усложненной форме);
* «Решетка Кардано»;
* «Таблица Виженера»;
* «одноразовый шифровальный блокнот»;
* «вертушка со стрелкой».
1. Тайнопись в России впервые начала применяться в XIII в. Первая система шифрования называлась «тарабарской грамотой». Во второй половине XVII в. появился тайный алфавит, или шифр «уголки». В эпоху Петра I начала употребляться для секретной переписки «цифирная азбука».
2. Среди шифров подполья можно выделить три наиболее используемых:
* «Тюремная азбука»;
* «Парный шифр»;
* «По стихотворению».
1. Ключ к разгадке шифров лежит в основах языка:
* повторяемость гласных чаще, чем согласных букв;
* в русском языке чаще остальных повторяются буквы «О», «А» и «Е», а в английском – «Е», «А», «О»;
* логическая связь между словами.
1. Среди произведений детективного жанра первопроходцами в использовании кодирования и декодирования информации являлись:
* По Э. «Золотой жук»;
* Конан Дойль А. «Пляшущие человечки»
* Богомолов В.О. «Момент истины»;
* Солженицын А.И. «В круге первом»;
* Ж.Верн «Дети капитана Гранта», «Жангада».

**СПИСОК ЛИТЕРАТУРЫ**

1. Аршинов М.Н., Садовский Л.Е. Коды и математика (рассказы о кодировании). – М.: Наука, Главная редакция физико-математической литературы, 1983.
2. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. – М.:ТЕИС, 1994.
3. Кан Д. Взломщики кодов. Пер. с англ. Ключевского А.– М.: ЗАО Центр-полиграф, 2000.
4. Методический журнал «Русский язык в школе». – М.: Просвещение, № 2, март – апрель, 1989.
5. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – Спб.: издательство Лань, 2000.
6. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999.
7. Периодическое издание «Первое сентября». Статья по теме: Математические загадки детективного сюжета (криптография)
8. По Э.А. Собрание сочинений. В 4-х т. Т. 3. Пер. с англ. – Х.: Фолио, 1995.
1. «Cogito, ergo sum» - «Я мыслю, следовательно, существую» (лат.) – Р.Декарт [↑](#footnote-ref-1)
2. «Veni, vidi, vici» - «Пришел, увидел, победил» (лат.) – Г.Ю.Цезарь [↑](#footnote-ref-2)
3. «Festina lente» - «Торопись медленно» (лат.) [↑](#footnote-ref-3)
4. «В чужой монастырь со своим уставом не ходят» [↑](#footnote-ref-4)
5. «Да, были люди в наше время –

 Не то, что нынешнее племя – богатыри» (М.Ю.Лермонтов) [↑](#footnote-ref-5)
6. «Рыба с головы гниет» [↑](#footnote-ref-6)
7. «Иванову доверять нельзя явки сменить». [↑](#footnote-ref-7)
8. «Над Россией безоблачное небо» [↑](#footnote-ref-8)