**Введение**

криптография шифрование плейфер тритемиус

С давних пор любимой игрой всех мальчишек были попытки изобретения специального алфавита для обмена секретными сообщениями. Конечно, это было связано больше с детским желанием поиграть в шпионов, чем с реальной угрозой перехвата передаваемой информации посторонними лицами. Однако в мире взрослых такая угроза, несомненно, существует, и конфиденциальность многих сообщений чрезвычайно важна. С наступлением информационного века кодирование и шифры, ранее представлявшие интерес лишь для политической и социальной элиты, стали необходимыми для нормального функционирования общества в целом, поэтому актуальность данной работы очень высока.

Криптография, то есть искусство кодированного письма, появилась с возникновением самой письменности. Хотя еще египтяне и жители Месопотамии использовали методы шифрования, первыми, кто серьезно занялся криптографией, были древние греки и римляне - враждующие культуры, для которых тайное общение являлось ключевым элементом военных успехов. Такая секретность привела к появлению нового типа соперников - тех, кто называл себя хранителями тайны, - криптографов, и тех, кто надеялся раскрыть ее, - криптоаналитиков.

При взрывном росте вычислительной мощности именно шифры, а не традиционные соображения секретности играют ведущую роль в передаче секретной информации. Но способов шифрования великое множество и в одной работе всех их рассмотреть невозможно.

Цель курсовой работы: узнать, что такое и чем занимается наука криптография; познакомиться с основными понятиями и терминами в области шифрования; выяснить, на какие группы делятся криптосистемы (шифры); определить, чем отличаются симметричные и асимметричные методы шифрования; изучить симметричные криптосистемы на примере шифров Плейфера и Тритемиуса, разделить их на группы; найти и решить возможные проблемы при зашифровке и расшифровывании текста с помощью шифров Плейфера и Тритемиуса.

**1. Криптография как наука**

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации - обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Ключ - секретная информация, используемая криптографическим алгоритмом при шифровании / расшифровке сообщений. При использовании одного и того же алгоритма результат шифрования зависит от ключа. Ключи различаются согласно алгоритмам, в которых они используются:

) Симметричные ключи - ключи, используемые в симметричных криптосистемах. Главное свойство симметричных ключей (криптосистем): для шифрования и расшифровывания секретного сообщения необходимо использовать один и тот же ключ (либо ключ для обратного преобразования легко вычисляется из ключа для прямого преобразования, и наоборот).

) Асимметричные ключи - ключи, используемые в асимметричных алгоритмах, где шифрование и расшифровывание производится с помощью закрытого (известного только владельцу) и открытого (ключ, который может быть опубликован посторонним лицам для проверки подлинности документа) ключей.

В данной работе будут рассмотрены только симметричные криптосистемы.

**Шифры и шифрование**

Шифр - это какая-либо система преобразования текста с ключом для обеспечения секретности передаваемой информации. Шифр может представлять собой совокупность условных знаков (условная азбука, пример: шифр Тритемиуса), либо алгоритм преобразования букв и цифр (пример: шифр Плейфера). Процесс засекречивания сообщения с помощью шифра и называется шифрованием. Не стоит путать шифр с кодированием - фиксированным преобразованием информации из одного вида в другой. В последнем отсутствует понятие ключа и в наше время кодирование практически не применяется для защиты информации.

Шифры делятся на группы:

) по количеству используемых ключей (см. выше);

) по методу шифрования сообщения:

. Блочный шифр (шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации);

. Поточный шифр (шифрует информацию и выдает шифротекст по мере поступления, таким образом имея возможность обрабатывать текст неограниченного размера);

. Подстановочный шифр (элементы исходного текста заменяются зашифрованным текстом в соответствии с некоторым правилом; элементами текста могут быть отдельные символы, пары букв, тройки букв и комбинирование этих случаев). В данной работе будут рассмотрены только подстановочные шифры.

В криптографии различают четыре типа шифра подстановки:

) Одноалфавитный шифр (шифр простой замены) - шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита (например: шифр Тритемиуса, шифр Цезаря). Отмечу, что шифр простой замены не всегда подразумевает замену буквы на другую букву. Допускается использовать замену буквы на цифру.

) Однозвучный шифр подстановки - символ открытого текста может быть заменен одним из нескольких возможных символов. Ярким примером этого вида является книжный шифр. Суть этого метода - выбор любого текста из книги, где номера слов начинающихся на определенную букву или координаты (строка, номер в строке) самих букв выступают в качестве шифра исходного сообщения. При этом одной букве может соответствовать несколько кодов.

) Полиграммный шифр подстановки - во время шифрования заменяется не один символ, а целая группа символов. Примеры: шифр Плейфера, шифр Хилла.

) Полиалфавитный шифр подстановки - шифрование состоит из нескольких шифров простой замены. Суть полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к определенному числу букв шифруемого текста.

Классическим примером симметричных шифров также являются шифры перестановки:

. Простая перестановка без ключа - самый простейший метод шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Например, нужно зашифровать фразу: Маленькая планета. Запишем ее в таблицу 5×5 (вмести с номерами строк и столбцов):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 1 | м | н | я | н |
| 2 | а | ь | п | е |
| 3 | л | к | л | т |
| 4 | е | а | а | а |

И зашифруем строки в порядке 2314:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1234 |  |  |  |  |
| 2 | а | ь | п | е |
| 3 | л | к | л | т |
| 1 | м | н | я | н |
| 4 | е | а | а | а |

Зашифрованное сообщение: алмеькнапляаетна.

Расшифровка производится обратным способом.

. Одиночная перестановка по ключу - более практичный способ шифрования, который очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы представляются по ключевому слову или фразе и переставляются в алфавитном порядке.

. Двойная перестановка - зашифрованное сообщение просто повторно зашифровывается. Доказано, что этот метод не усиливает стойкость шифрования.

Сейчас шифры перестановки применяются только в ознакомительных целях.

Также криптосистемы обладают определенной криптографической стойкостью. Криптографическая стойкость (криптостойкость) - это способность шифра противостоять криптоанализу (взлому). Стойким считается шифр, который для успешной атаки требует от взломщика недостижимых вычислительных ресурсов, недостижимого объема перехваченных открытых и зашифрованных сообщений или же огромного времени взлома, что по его истечении защищенная информация будет уже не актуальна. В большинстве случаев криптостойкость нельзя математически доказать, можно только доказать уязвимости шифра.

Криптостойкие шифры делятся на:

) Абсолютно стойкие; для каждого шифра должны выполнятся следующие условия:

. Ключ генерируется для каждого сообщения (т.е. каждый ключ используется только один раз);

. Ключ статистически надежен (т.е. вероятности появления каждого из возможных символов равны);

. Длина ключа равна или больше длины сообщения.

Единственный шифр, который обладает всеми перечисленными условиями, - это шифр Вернама.

) Достаточно стойкие; в свою очередь они делятся на:

. Практически стойкие;

. Вычислительно стойкие.

Стойкость этих шифров зависит от того, какими вычислительными возможностями обладает взломщик (правильнее криптоаналитик). Шифр Плейфера, о котором будет рассказано в данной курсовой работе, является достаточно стойким; шифр Тритемиуса, в свою очередь, гораздо уязвим для криптоаналитиков, а шифры перестановки вообще почти не имеют никакой стойкости.

Следует выделить преимущества и недостатки симметричных криптосистем:

) Преимущества:

. Простота реализации;

. Меньшая требуемая длина ключа для сопоставимой стойкости (в отличие от асимметричных криптосистем);

. Большая изученность.

) Недостатки:

. Сложность управления ключами в большой сети (это означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети; например, для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 - 499 500);

. Сложность обмена ключами.

Важным свойством симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

**2. Шифр Плейфера**

**История создания и применения шифра Плейфера**

Несмотря на то, что шифр был изобретением Чарльзов Уитстона, он стал известен как шифр Плейфера. Первое описание шифра Плейфера было зарегистрировано в документе, подписанном Уитстоном 26 марта 1854 года. Министерство иностранных дел Великобритании отклонило этот документ из-за сложности его восприятия. Когда Уитстон предложил продемонстрировать, что три из четырех мальчиков в соседней школе научаться использовать этот шифр за 15 минут, заместитель министра иностранных дел ответил: «Это очень возможно, но вы никогда не научили бы этому атташе».

Этот шифр использовался в тактических целях британскими вооруженными силами во Второй Англо-Бурской войне и в Первой мировой войне, а также австралийцами и немцами во время Второй Мировой войны. Причиной использования шифра Плейфера было то, что он достаточно быстр в применении и не требует никакого специального оборудования. Основной целью использования этой системы шифрования была защита важной, но не секретной информации во время ведения боя. К тому времени, когда вражеские криптоаналитики взламывали сообщение, информация уже была бесполезна для них.

Шифр Плейфера является достаточно стойким, но современные компьютерные технологии взламывают этот шифр за 15 минут, поэтому шифрование является нецелесообразным.

**Описание шифра**

Шифр Плейфера - ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном, но названа именем Лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в подстановки в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ.

Для русского алфавита шифр Плейфера использует матрицу 4×8, содержащую ключ (некоторую фразу). Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в русских текстах обычно опускается буква Ё). Ключевое слово в матрице записывается по строкам слева направо. Ключевое слово, дополненное алфавитом, составляет матрицу 4х8 и является ключом шифра.

Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем.

. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х», если они не несут смысла в исходном сообщении.

**Примеры**

**Задача 1.** Зашифровать с помощью шифра Плейфера сообщение: «Марс будет виден невооруженным глазом завтра в полночь».

Ключ: фраза «Шифр использует замену биграмм».

Для начала буквы ключевой фразы записываем в таблицу 4х8, отбрасывая повторяющиеся символы (см. таблицу 1).

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Ш | И | Ф | Р |
| С | П | О | Л |
| Ь | З | У | Е |
| Т | А | М | Н |
| Б | Г |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Дальше записываем в таблицу оставшиеся буквы алфавита, только без буквы «Ё». (см. табл. 2).

Таблица 2

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

Итак, ключ, по которому мы будем зашифровывать сообщение, готов. Теперь нужно разбить секретное сообщение на биграммы:

МА РС БУ ДЕ ТВ ИД ЕН НЕ ВО ОР УЖ ЕН НЫ МГ ЛА ЗО МЗ АВ ТР АВ ПО ЛН ОЧ Ь

Далее зашифровываем биграммы по отдельности:

. Ищем буквы МА в таблице. Они находятся в одной строке, поэтому «сдвигаем» каждую вправо. МА заменяем на НМ (табл. 3 а, б).

Таблица 3

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

. Ищем буквы РС в таблице. Они находятся в разных строках\столбцах, поэтому каждую букву заменяем на ту букву, которая находится на строчке, где находится соседняя буква в биграмме. То есть, букву Р мы заменяем на букву, которая находится на строчке, на которой находится буква С. Это буква Л. Тоже самое и с буквой С. Заменяем ее на Ш. Получаем ЛШ (табл. 4 а, б).

Таблица 4

|  |  |  |  |
| --- | --- | --- | --- |
| ШИФ**Р** |  |  |  |
| **С** | П | О | Л |
| **Ш** | И | Ф | Р |
| С | П | О | **Л** |

. БУ в разных строках\столбцах. Заменяем на ЬВ (табл. 5 а, б).

Таблица 5

|  |  |  |
| --- | --- | --- |
| Ь | З | **У** |
| Т | А | М |
| **Б** | Г | В |
| **Ь** | З | У |
| Т | А | М |
| Б | Г | **В** |

. Буквы биграммы ДЕ находятся в одном столбце. Каждую букву сдвигаем вниз на одну строчку. Получаем ХН (табл. 6 а, б).

Таблица 6

|  |
| --- |
| **Е** |
| Н |
| **Д** |
| Х |
| Е |
| **Н** |
| Д |
| **Х** |

Аналогично:

. ТВ на БМ.

. ИД на ГР.

. ЕН на НД.

. НЕ на ДН.

. ВО на КУ.

. ОР на ФЛ.

. УЖ на КЬ.

. ЕН на НД.

. НЫ на ЯТ.

. МГ на ВА.

. ЛА на НП.

. ЗО на ПУ.

. МЗ на УА.

. АВ на ГМ.

. ТР на НШ.

. АВ на ГМ.

. ПО на ОЛ.

. ЛН на ЕД.

. ОЧ на ЩП.

. Остался последний знак Ь. Чтобы сформировать биграмму, добавляем букву Х. Получаем биграмму ЬХ и зашифровываем. Получаем ЖЕ.

Зашифрованное сообщение:

НМЛШЬВХНБМГРНДДНКУФЛКЬНДЯТВАНППУУАГМНШГМОЛЕДЩПЖЕ.

Задача выполнена.

**Задача** 2. Расшифровать сообщение:

НМЛШЬВХНБМГРНДДНКУФЛКЬНДЯТВАНППУУАГМНШГМОЛЕДЩПЖЕ.

Ключ: Шифр использует замену биграмм.

Теперь, наоборот, надо расшифровать сообщение. Я буду расшифровывать предыдущий пример, чтобы показать, что при зашифровке и расшифровывании сообщения его смысл не меняется.

Для начала надо составить ключевую таблицу (табл. 2). Теперь надо разбить сообщение на биграммы:

НМ ЛШ ЬВ ХН БМ ГР НД ДН КУ ФЛ КЬ НД ЯТ ВА НП ПУ УА ГМ НШ ГМ ОЛ ЕД ЩП ЖЕ

После этого, в общем-то, нам надо проделать тоже самое, только сдвигать буквы будем в обратном направлении:

. Буквы биграммы НМ находятся в одной строке. Поэтому каждую букву теперь сдвигаем влево (а не вправо!) (табл. 3 а, б в обратном порядке).

. Буквы биграммы ЛШ находятся в разных строках и столбцах. Поэтому каждую букву заменяем на ту, которая находятся на одной строке с другой буквой биграммы. То есть, Л заменяем на Р, а Ш на С (табл. 4 а, б в обратном порядке).

. ЬВ в разных строках\столбцах. Заменяем на БУ (табл. 5 а, б в обратном порядке).

. Буквы биграммы ХН находятся в одном столбце. Поэтому каждую букву теперь сдвигаем вверх (а не вниз!) (табл. 6 а, б в обратном порядке).

Аналогично:

. БМ на ТВ.

. ГР на ИД

. НД на ЕН

. ДН на НЕ

. КУ на ВО.

. ФЛ на ОР.

. КЬ на УЖ.

. НД на ЕН.

. ЯТ на НЫ.

. ВА на МГ.

. НП на ЛА.

. ПУ на ЗО.

. УА на МЗ.

. ГМ на АВ.

. НШ на ТР.

. ГМ на ТВ.

. ОЛ на ПО.

. ЕД на ЛН.

. ЩП на ОЧ.

. ЖЕ на ЬХ.

Мы получаем:

МАРСБУДЕТВИДЕННЕВООРУЖЕННЫМГЛАЗОМЗАВТРАВПОЛНОЧЬХ

Восстанавливаем смысл, вставляя пробелы:

Марс будет виден невооруженным глазом завтра в полночь х.

Убираем лишние буквы «Х»:

Марс будет виден невооруженным глазом завтра в полночь.

Мы получили исходное сообщение. Задача выполнена.

**3. Шифр Тритемиуса**

**Иоганн Тритемий**

Прежде чем описывать шифр Тритемиуса, следует рассказать о ее создателе - Иоганне Тритемии.

Иоганн Тритемий (1 февраля 1462 г. - 13 декабря 1516 г.) - автор книг по истории, криптографии и оккультизму. Иоганн Хайденберг (его имя при рождении) окончил Гейдельбергский университет. Когда в 1482 году он возвращался домой, снежная буря вынудила его укрыться в бенедиктинском аббатстве Спонхайма. Он решил остаться там, и вскоре, уже в 1483 году, был избран аббатом. Он предпринял усилия к увеличению библиотеки аббатства, доведя ее с 50 до 2000 книг, и приобрел репутацию мага. Известен своими многочисленными сочинениями, среди которых «Полиграфия» (в которой и был опубликован его шифр) и «Стенография». На первый взгляд, книга посвящена магами и использованию духов для общения. Однако ключ к дешифровке книги показывает, что речь в ней идет о криптографии.

**Математическая модель**

Шифр Тритемиуса - симметричная система шифрования, разработанная Иоганном Тритемием. Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки. По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг. Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы. Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.

Уравнением зашифрования называется соотношение, описывающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Уравнение зашифрования для шифра Тритемиуса имеет следующий вид:

, где  - это номер зашифрованной буквы в алфавите,

 - номер позиции шифруемой буквы в алфавите,  - шаг смещения,  - количество букв в алфавите.

Шаг смещения может вычисляться разными уравнениями:

,



где  - ключи (их может быть сколько угодно), а

 - это позиция буквы в тексте. Таким образом, смещение зависит еще и то положения буквы в тексте. Для русского алфавита обычно применяется такая таблица положения букв (табл. 7).

Таблица 7

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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,. |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32333435 |

**Примеры**

**Задача** **1**. Зашифровать сообщение: К неевклидовым геометриям относятся сферическая и гиперболическая.

Ключ: уравнение  где ключи А = 3; В = 5.

Используя вышеперечисленные формулы, начинаем зашифровывать сообщение:

. Положение буквы К в тексте,  = 1. Вычисляем смещение:  = 3×1+5 =8

Положение буквы в алфавите,  = 11. Вычисляем позицию новой буквы:

 = (11 + 8)  36 = 19. В таблице это буква Т. Заменяем К на Т.

. Положение (пробел) в тексте,  = 2. Вычисляем смещение:  = 3×2+5=11. Положение буквы в алфавите,  = 33. Вычисляем позицию новой буквы:  = (33 + 11)  36 = 8. В таблице это буква З. Заменяем (пробел) на З.

Аналогично ((пр.) - сокращенно «пробел»):

. Н на Ы.

. Е на Х. 20. Е на (,) 36. (пр.) на В.

. Е на Ш. 21. Т на О 37. С на Щ.

. В на Ш. 22. Р на П 38. Ф на Я.

. К на Б. 23. И на К 39. Е на Т

. Л на Е. 24. Я на Б 40. Р на (,).

. И на Е. 25. М на Ф. 41. И на Ь.

. Д на Г. 26. (пробел) на З. 42. Ч на К.

. О на Р. 27. О на Ь. 43. Е на Ю.

. В на Ж. 28. Т на А 44. С на К.

. Ы на А. 29. Н на (,) 45. К на Ж.

. М на Ч. 30. О на В. 46. А на (.)

. (пр.) на К. 31. С на З. 47. Я на (,)

. Г на У. 32. Я на Ш. 48. (пр.) на В

. Е на Ш. 33. Т на О. 49. И на Р.

. О на В. 34. С на Р 50. (пр.) на З.

. М на Г. 35. Я на (,). 51. Г на Р.

. И на Щ 57. О на К. 62. С на Ь.

. П на А 58. Л на К. 63. К на Ш.

. Е на Ы 59. И на К 64. А на Р.

. Р на Ж 60. Ч на Ь. 65. Я на П.

. Б на Э 61. Е на М. 66. (.) на Х.

Зашифрованное сообщение:

ТЗЫХШШБЕЕГРЖАЧКУШВГ, ОПКБФЗЬА, ВЗШОР, ВЩЯТ, ЬКЮКЖ., ВРЗРЩАЫЖЭКККЬМЬШРПХ

Задача выполнена.

Теперь обратное задание **(задача 2)**: расшифровать текст

ТЗЫХШШБЕЕГРЖАЧКУШВГ, ОПКБФЗЬА, ВЗШОР, ВЩЯТ, ЬКЮКЖ., ВРЗРЩАЫЖЭКККЬМЬШРПХ

Ключ: уравнение  где ключи А = 3; В = 5.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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,. |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32333435 |

Для того чтобы расшифровать сообщение, нужно использовать обратную формулу:

.

**Примечание: Если разность L - k будет отрицательной, надо к этой разности прибавлять N, пока она не станет положительной.**

Используя эту формулу, расшифровываем текст:

. Позиция зашифрованной буквы Т в алфавите,  = 19. Позиция буквы в тексте,  = 1. Вычисляем смещение  = 3×1+5=8. Вычисляем позицию исходной буквы,  = 19-8  36 = 11. Это буква К. Заменяем.

. Позиция зашифрованной буквы З в алфавите,  = 8. Позиция буквы в тексте,  =2. Вычисляем смещение  = 3×2+5=11. Вычисляем позицию исходной буквы,  = 8-11  36 = -3+36 = 33. Это (пробел). Заменяем.

Аналогично:

. Ы на Н.

. Х на Е. 20. (,) на Е 36. В на (пр.).

. Ш на Е. 21. О на Т 37. Щ на С.

. Ш на В. 22. П на Р 38. Я на Ф.

. Б на К. 23. К на И 39. Т на Е

. Е на Л. 24. Б на Я 40. (,) на Р

. Е на И. 25. Ф на М. 41. Ь на И

. Г на Д. 26. З на (пр.). 42. К на Ч.

. Р на О. 27. Ь на О. 43. Ю на Е.

. Ж на В. 28. А на Т 44. К на С.

. А на Ы. 29. (,) на Н 45. Ж на К.

. Ч на М. 30. В на О. 46. (.) на А

. К на (пр.). 31. З на С. 47. (,) на Я

. У на Г. 32. Ш на Я. 48. В на (пр.)

. Ш на Е. 33. О на Т. 49. Р на И.

. В на О. 34. Р на С 50. З на (пр.).

. Г на М. 35. (,) на Я 51. Р на Г.

. Щ на И 57. К на О. 62. Ь на С.

. А на П 58. К на Л. 63. Ш на К.

. Ы на Е 59. К на И 64. Р на А.

. Ж на Р 60. Ь на Ч. 65. П на Я.

. Э на Б 61. М на Е. 66. Х на (.)

Получаем: К неевклидовым геометриям относятся сферическая и гиперболическая.

Задача выполнена.

Далее я экспериментировал с различными уравнениями (приложения 1 и 2), зашифровывая туже самую фразу, и выявил одну закономерность: в уравнении

,

где А = 7, окончания слов сфери**ческая** и гиперболи**ческая** зашифровались одинаково:

. Ч на Ч. 60. Ч на Ч.

. Е на Ч. 61. Е на Ч.

. С на (,). 62. С на (,).

. К на В. 63. К на В.

. А на П. 64. А на П.

. Я на О. 65. Я на О.

. (пр.) на (пр.) 66. (.) на (.)

и в уравнении



где А = 2; В = 4; С = 1, окончания слов сфер**ическая** и гипербол**ическая** зашифровались одинаково:

. И на З. 59. И на З.

. Ч на М. 60. Ч на М.

. Е на Ч. 61. Е на Ч.

. С на (.) 62. С на (.)

. К на Э. 63. К на Э.

. А на Ш. 64. А на Ш.

. Я на Ю 65. Я на Ю

Было несколько предположений по поводу этого:

) моя ошибка (что почти сразу было опровергнуто);

) то, что в первом уравнении не было свободного члена (из-за того, что степень была кратна 36 и число , соответственно, было кратно 36 и число  оставалось одинаковым);

) то, что во втором уравнении не была нечетного ключа, а С не играло своей роли и из-за этого число  в этом случае становилось кратным 36 и число  оставалось одинаковым;

) совпадение.

Чтобы проверить свои доводы, я зашифровал фразу, в которой все слова оканчивались с ключами, из которых первый не выполнял условие 2) а второй - условия 2) и 3) одновременно (приложения 3 и 4 соответственно).

В обоих случаях я получил, что окончания слов зашифровались по-разному, а следовательно это было совпадение.

**Заключение**

Криптография - это очень древняя наука, которая делится на две большие группы: шифрование и кодирование. В этой работе я уделил внимание шифрованию, а именно на симметричные методы шифрования. Симметричные криптосистемы - это метод шифрования, в котором используется только один ключ: для зашифровки и для расшифровки. Я отдельно разобрал все виды симметричных криптосистем, на своем примере зашифровал и расшифровал сообщение с помощью двух симметричных шифров: шифра Плейфера и шифра Тритемиуса; решил возникшие проблемы при зашифровке текста, применив один и тот же ключ к идентичному по буквенному составу тексту. Я научился отличать симметричные криптосистемы от асимметричных.

Цели моей курсовой работы достигнуты полностью.

Поставленные задачи выполнены.

**Список использованных источников**

1. Издание «Мир математики». 2 том «Криптография» и 41 том «Неразрешимые проблемы». ДеАгостини, 2014.

2. Большая Энциклопедия Кирилла и Мефодия, 2011.

. Материалы сайта www.wikipedia.org