Научно-практическая работа

математика

«СПОСОБЫ ШИФРОВАНИЯ ТЕКСТОВ»

Выполнил:
Бейненсон Роман Александрович
учащийся 4«А» класса
МБОУ г. Иркутска СОШ №76, Россия, г. Иркутск

Руководитель:
Тузова Светлана Евгеньевна
учитель начальных классов
МБОУ г. Иркутска СОШ №76, Россия, г. Иркутск

Введение

Шифрование - это процесс преобразования сообщения в вид, нечитаемый для всех, кроме того человека или устройства, у которого имеется ключ для «расшифровки» этого сообщения обратно в читаемый вид.

Существует целая наука, изучающая системы шифрования– криптография.

Актуальность: Во все времена у людей существовала потребность спрятать текстовую информацию от посторонних глаз при её передаче или хранении. В настоящее время методы шифрования применяются не только для защиты информации от нежелательного доступа, но и лежат в основе многих новых электронных информационных технологий - электронного документооборота, электронных денег, тайного электронного голосования и др. Сейчас, когда весь мир пользуется интернетом, передавать важную информацию и скрывать ее от посторонних лиц и от мошенников является очень важной задачей.

Проблема: низкая осведомленность учащихся начальных классов о степени важности засекречивания информации в современном обществе и способах шифрования текстов.

Гипотеза: защита информации необходима в современном мире. Заниматься шифрами увлекательно и полезно. Знание и использование шифра помогает засекретить информацию, не предназначенную для посторонних.

Цель исследования: изучить основные приемы построения шифров, выявить необходимость шифрования текстов в современном обществе.

Задачи исследования: 1) изучить историю развития шифрования текстов; 2) собрать информацию о разных способах засекречивания текстовой информации; 3) провести опрос среди учеников начальной школы о том, имеют ли они представление о необходимости и способах шифрования информации; 4) на основе изученных материалов создать новый шифр.

Объект исследования – защита текстовой информации.

Предмет исследования – способы шифрования текстов.

Методы исследования: 1) теоретический – сбор информации по данной теме; 2) практический – социологический опрос, разработка шифра.

Основная часть

1. История возникновения и развития шифрования

Имеются свидетельства, что криптография как техника защиты текста возникла вместе с письменностью. Однако точное время возникновения способов обмена тайной информацией теряется в глубине веков, и установить его невозможно. Историки полагают, что первые приемы шифрования текстов появились в Древнем Египте около 4 тыс. лет назад. Египтяне для придания своим текстам загадочности и важности, видоизменяли обычные иероглифы. В Мясопотамии была найдена глиняная табличка, изготовленная в 1500 г. до нашей эры, с записанным на ней рецептом глазури для гончарных изделий.

Рис. 1. Глиняная табличка с рецептом

В тексте были намеренно перемешаны символы.

Примеры использования криптографии можно встретить в Библии. Эти методы засекречивания включали в себя перемену местами согласных и гласных букв, использование перевернутых букв и запись текста под случайными углами.

Одним из древнейших известных криптографических устройств является Скитала. Использовалось данное приспособление в войне Спарты с Афинами. Представляет собой длинную деревянную палку с наматываемой на нее полоской папируса или другим материалом для письма.

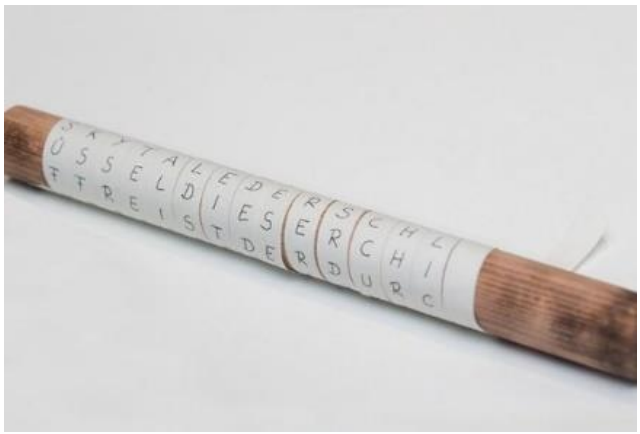
Рис. 2. Скитала

На ленту наносился текст вдоль оси Скиталы, так, что после разматывания текст становился нечитаемым. Адресату отправляли только ленту. Для восстановления текста требовалась Скитала такого же размера.

Криптография быстро развивалась в средние века, шифровками пользовались многочисленные дипломаты и купцы. Значительное влияние на развитие криптографии оказало появление телеграфа, потому что сам факт передачи данных перестал быть секретным. Это заставило отправителей сосредоточиться на шифровании данных. Активное развитие криптографии пришлось на XVI-XVIII века. Этот период времени вошел в историю криптографии как эра «черных кабинетов». «Черные кабинеты» - это специальные службы, которые занимались перехватом шифрованием и дешифровкой информации государственной важности. В них входили агенты по перехвату писем, специалисты по имитированию почерка, по подделке печатей, переводчики и многие другие. Эти люди очень высоко ценились.

Криптография оказала влияние и на литературу. Великий французский писатель-фантаст Жюль Верн в своем рассказе «Путешествие к центру Земли» 1864 года также описывает, как герои расшифровывали послание. Еще одним ярким примером служит рассказ Артура Конан Дойля «Пляшущие человечки», написанный в 1903 г., где великий сыщик Шерлок Холмс сталкивается с разновидностью шифра, в котором каждая буква заменена рисунком.

Рис. 3. Шифр замены рисунком

Во время Первой мировой войны криптография стала признанным боевым инструментом. Разгаданные сообщения противников вели к ошеломляющим результатам. Перед началом Второй мировой войны ведущие мировые державы имели электромеханические шифрующие устройства, результат работы которых считался невскрываемым.

Энигма 1 (Германия) *Коралл (СССР)*

Рис. 4. Электромеханические шифрующие устройства

Вторая мировая война послужила своеобразным катализатором развития систем шифрования.

С появлением компьютеров, криптография стала более продвинутой. Современный период развития криптографии (с конца 1970-х годов по настоящее время) знаменуется не только появлением новых технических возможностей, но и сравнительно широким распространением криптографии для использования как государством, так и частными лицами. В наш век огромного потока обмена информацией, к которой относится все больше и больше информации о нашей повседневной жизни - медицинской карты, электронные дневники школьников, переписка в различных интернет мессенджерах (viber, whatsapp и др.), банковские карты и многое другое, устойчивое и надёжное

шифрование является не просто необходимым, а жизненно важным условием безопасности.

2. Виды шифров

На сегодняшний день существует множество алгоритмов, при помощи которых шифруется информация. Важнейшее в процессе шифрования – это создание ключа, который потом позволит просматривать зашифрованные данные. Надежность шифрования данных называют криптостойкостью. Чем выше криптостойкость шифрования, тем меньше вероятность того, что стороннее лицо получит доступ к зашифрованной информации.

Все известные шифры условно можно разделить на три основные группы:

1) первая группа - шифры ***замены***. Шифром замены называется алгоритм шифрования, который производит замену каждой буквы шифруемого текста на какой-то символ. Получатель сообщения расшифровывает его путем обратной замены. Этот метод не изменяет написанный текст по последовательности.

2) вторая группа - шифры ***перестановки***. Перестановка представляет собой способ шифрования, при котором для получения шифрограммы символы исходного сообщения меняют местами.

3) третья группа - ***комбинированные*** или ***композиционные*** шифры. К этой группе относятся самые сложные способы шифрования. Они предполагают использование сразу нескольких методов шифрования (например, сначала замена символов, а затем их перестановка).

К самым известным шифрам замены относятся шифр Цезаря, шифр Полибия, Атбаш.

Шифр Цезаря

Рис. 5. Схема шифра Цезаря

Шифр цезаря состоит в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на три и более позиций. Так, если сдвигаем на девять букв вперед, то буква А становится буквой И, буква Б становится Й и так далее. Например, если исходное слово «**СОК**», то шифрограмма – «**ИЁВ**».

Шифр Полибианский квадрат

Авторство данного шифра приписывается греческому писателю Полибию, жившему в III веке до н.э. В квадрат 6х6 выписывались буквы алфавита. Каждая буква исходного текста заменялась на пару цифр – номер строки и столбца на пересечении которых стояла шифруемая буква.

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

Рис. 6. Схема шифра «Полибианский квадрат»

Например, если исходное сообщение **«ШИФР»**, то шифрограмма – **«52 24 44 36»**.

Многие из нас неосознанно используют шифр замены, например, когда создают пароль, записывая русское слово с помощью английской раскладки клавиатуры.

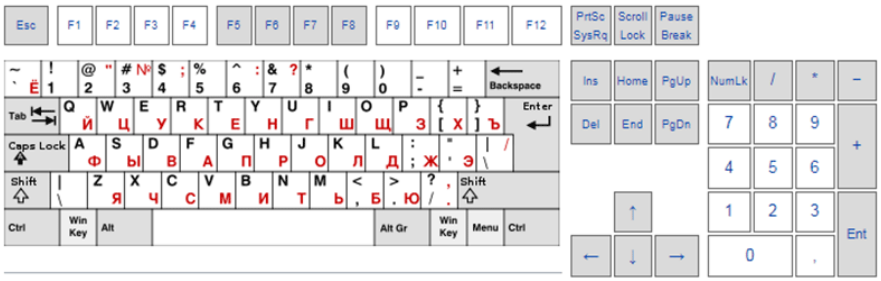

Рис. 7. Схема шифра с использованием клавиатуры

Если исходное сообщение «**Пароль»,** то шифрограмма **– «Gfhjkm».**

Самыми простыми примерами шифрования методом перестановки являются шифр простой одинарной перестановки, шифр блочной одинарной перестановки, шифр табличной маршрутной перестановки.

Шифр простой одинарной перестановки

Шифр перестановки называется простым, если элементы текста меняют свои позиции только один раз.

1	2	3	4	5	6		**П$_1$**	**А$_2$**	**Р$_3$**	**О$_4$**	**Л$_5$**	**Ь$_6$**
2	4	5	1	3	6		**А**	**О**	**Л**	**П**	**Р**	**Ь**

Рис. 8. Схема шифра простой одинарной перестановки

В первой строке данной таблицы указывается позиция символа в исходном сообщении, а во второй – его позиция в шифрограмме.

Шифр табличной маршрутной перестановки

При шифровании в таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) - по другому маршруту.

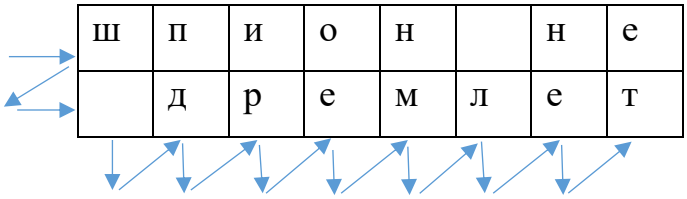

Рис. 9. Схема шифра табличной маршрутной перестановки

Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

Исходное сообщение: **«шпион не дремлет»**.

Зашифрованное сообщение: **«ш пдироенм лнеет»**.

3. Социологический опрос

Кроме изучения доступной информации о шифровании текстов, мы провели социологический опрос среди учеников моего класса. В опросе участвовало 27 человек.

Ребятам было задано 4 вопроса:

1. Знаете ли вы, что такое шифр?

2. Считаете ли вы, что шифрование имеет важное значение в современном мире?

3. Какие способы шифрования вы знаете?

4. Пробовали вы когда-нибудь зашифровать текст?

Результаты опроса представлены в таблице.

Таблица 1

Результаты социологического опроса

№ п/п	Вопрос	Ответ		Примечание
		Да	Нет	
1	Знаете ли вы, что такое шифр?	24	3	
2	Считаете ли вы, что шифрование имеет важное значение в современном мире?	10	17	
3	Какие способы шифрования вы знаете?	9	18	Слова наоборот, азбука Морзе, при помощи чернил из молока или лимона, замена букв цифрами
4	Пробовали вы когда-нибудь зашифровать текст?	7	20	

1. Большинство моих одноклассников знают, что такое шифр - 24 из 27 человек. Но только 10 ребят понимают, что шифрование имеет большое значение в современном мире. **Вывод:** существует проблема низкой осведомленность учащихся начальных классов о степени важности засекречивания информации в современном обществе.

2. По результатам опроса всего 9 человек из 27 опрошенных знают какие-либо способы шифрования. В основном это азбука Морзе, замена букв цифрами, написание слов наоборот, использование чернил из молока или лимона. Однако, лишь 7 пробовали когда-нибудь зашифровать текст. **Вывод:** у ребят моего возраста практически нет знаний в области криптографии, и в связи с этим имеется низкий интерес к применению способов шифрования.

4. Разработка шифра

Признаться, я, как и многие ребята, до проведения исследования не знал на сколько большое значение имеет криптография в повседневной жизни. Только сейчас я понял, что существует много такой информации, которой не всегда

хочется делиться с другими людьми. У меня, например, это личный дневник, в котором я пишу свои секреты и желания.

Основываясь на знаниях, полученных во время выполнения данного исследовательского проекта, мы разработали свой шифр. При его составлении были использованы изученные в ходе работы над проектом методы замены и перестановки.

Так выглядит **<u>зашифрованное сообщение</u>**:

«✈ ✱☠🕸☠💣🏳♑❄💣🏳 ✱✪❄◈✡☼❄🦶✱ 👄✈◈🏳✈❄👽⟡❒☠◈☼
✈🕷♑☼🏵🏳👄🏳 ☠❄✈❒ ✈ 🏳 🍗🗲-♑ ✱❄★🏳 ⟡◈✪✈».

Конечно, нами придуман не самый сложный шифр, но человек без специальных знаний и навыков совершенно точно не прочитает это сообщение.

<u>КЛЮЧ</u>

Буквы русского алфавита мы заменили символами.

Таблица 2

Символы для замены

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🍗			

Затем при шифровании текста был использован метод табличной маршрутной перестановки:

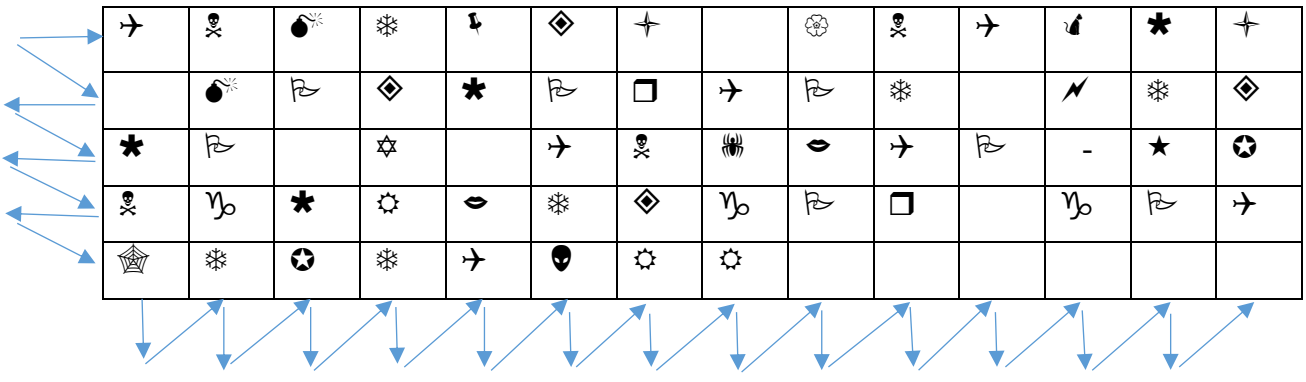

Рис. 10. Схема для дешифрования исходного сообщения

Используя данный ключ, можно без труда расшифровать текст.

Исходное сообщение: «**надеюсь занять достойное место в научно-практической конференции».**

Заключение

В результате исследования мы выяснили, что шифрование информации имеет большое значение не только для государства, но и для каждого человека в отдельности. При этом любой может скрыть важную информацию от тех, кому она не предназначена. Единственное, что для этого требуется – аккуратность и базовые знания.

Таким образом, мы подтвердили нашу гипотезу о том, что защита информации необходима в современном мире. Заниматься шифрами увлекательно и полезно. Знание и использование шифра помогает засекретить информацию, не предназначенную для посторонних.

Стоит отметить, что с развитием информационных технологий требуется создание новых, более сложных шифров, которые невозможно взломать.

Список литературы

1. Введение в криптографию/ Под ред. В.В. Ященко, 2001 г.

2. Коды, шифры, сигналы и тайная передача информации/ Фред Б. Риксон, 2011г.

3. Основы криптографии/ А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин, 2002 г.

4. Элементы криптографии (основы теории защиты информации): учебное пособие для университетов и педвузов/ Под ред. В.А. Садовничевого, 1999 г.