Государственное бюджетное общеобразовательное учреждение Самарской области

средняя общеобразовательная школа № 7 имени Героя Советского Союза Ф.И. Ткачева

города Жигулевска городского округа Жигулевск Самарской области

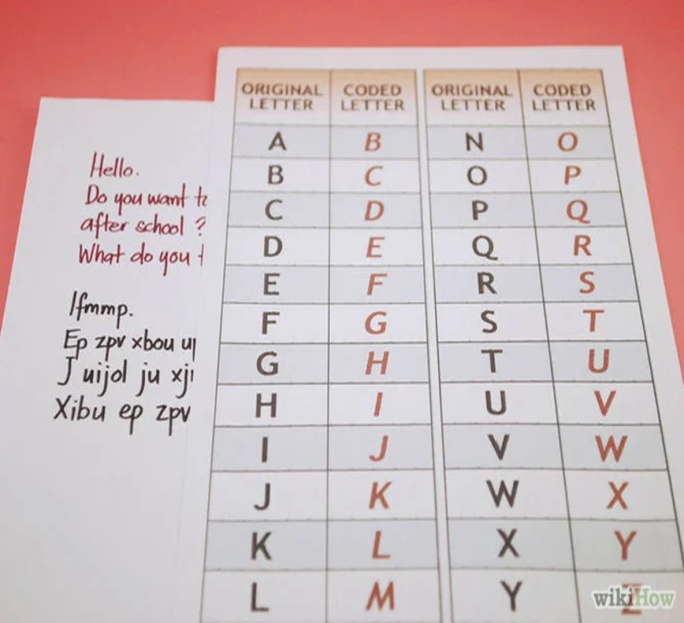
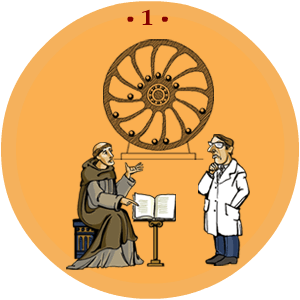
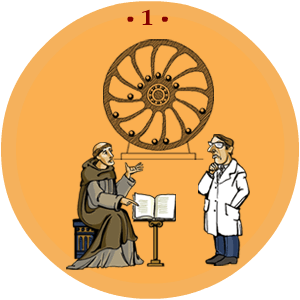
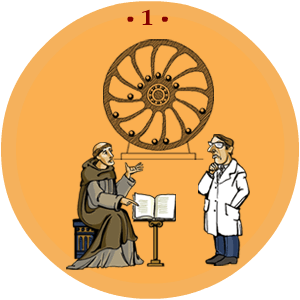
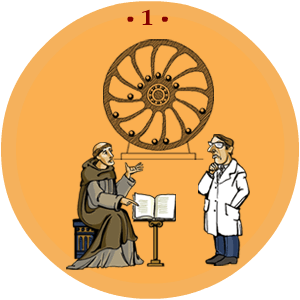
**Региональный конкурс исследовательских проектов**

**старших дошкольников и младших школьников**

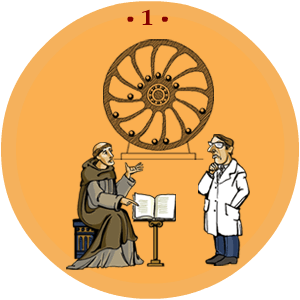
**2020/21 УЧЕБНЫЙ ГОД**

**Номинация «Математический калейдоскоп»**

**Тема «Шифры как увлекательные логические задачи»**

**Ученики 3 «А» класса:**

**Блохина Марианна, Шешиков Вениамин**

 **Преподаватель: Замотина Н.Г.**

Самара 2021 год

**Содержание**

Введение ………………………………………………………………………………..3

1.Теоретический раздел. Тайнопись. Как и когда появились шифры? Обзор простейших шифров……………………………………………………………………4

2. Практический раздел………………………………………………………………...5

Заключение……………………………………………………………………………...8

Используемая литература……………………………………………………………...8

Приложения……………………………………………………………………………..9

**Введение.** Каждый из нас смотрит и любит приключенческие фильмы, где используются зашифрованные тайные сообщения. Никого не могут оставить равнодушными и книги, в которых описываются тайные знания и умения, обычно доступные только избранным – шпионам и тайным агентам, пиратам и первооткрывателям дальних стран и, конечно же, учёным. Также мы все слышали про какие-то шифры, принимали участие в квестах или хотя бы раз в своей жизни каждый человек хотел зашифровать свои записи, сделать их понятными лишь немногим, тем более в наши дни, в век компьютеризации. А можно ли научиться шифрованию? Как это умение может пригодиться в современном мире? Ответить на этот **актуальный вопрос** мы постараемся в своей работе.

**Цель исследования:** изучить различные тайные способы передачи информации, выявить способы повышения криптостойкости простейших шифров,

научиться составлять свои шифры.

**Объект исследования:** шифры, как серьезные логические задачи

**Предмет исследования:** математические идеи и методы и их применения в шифровании.

**Гипотеза исследования**: использование математических методов способствует повышению криптостойкости шифров.

**Задачи исследования:**

1)Узнать, что такое тайнопись.

2)Выявить, какие бывают способы и средства шифрования.

3)Рассмотреть некоторые известные шифры.

4)Показать некоторые связи между математикой и шифрованием.

5)Выяснить, как использование математических методов, способствует повышению криптостойкости шифров.

6)Составить собственный шифр и показать его использование.

7)Выяснить, как шифрование используется в современном мире.

**Методы исследования:**

**1.Теоретический** (изучение научной и справочной литературы, систематизация и классификация).

**2.Экспериментальный** (наблюдение, эксперимент).

**3.Статистический** (обработка полученных данных).

**Итак, что получается?**

**1. Теоретический раздел. Тайнопись. Как и когда появились шифры? Обзор простейших шифров. Тайнопись или криптография – наука о создании, использовании и взломе шифров – одна из интереснейших и самых таинственных наук.**

Как выяснили учёные, ещё в Древней Греции прибегали к шифрованию текстов. Например, Древней Спарте было даже создано специальное устройство для шифрования текстов – сцитала. Сцитала представляла собой стержень, на который плотно наматывали ленту, а потом на ней писали текст, располагая его вдоль оси стержня. Когда ленту снимали с цилиндра, на ней оставалась цепочка букв, на первый взгляд, совершенно беспорядочная. У получателя шифровки был такой же цилиндр, на который он наматывал полученную ленту, после этого текст опять становился понятным.

В документах Древних Индии и Египта есть сведения о системах и способах составления шифрованных писем. Но самым известным из дошедших до нас древних шифров является ШИФР ЦЕЗАРЯ.

Первые шифры были не очень сложными. Например, русские дипломаты ΧV-XVI веков применяли так называемую «тарабарскую грамоту». В ней все гласные буквы оставались без изменений, а согласные заменялись одна другой по следующей схеме: в первой строке согласные идут в обычном порядке, а во второй строке – в обратном.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| б | в | г | д | ж | з | к | л | м | н |
| щ | ш | ч | ц | х | ф | т | с | р | п |

Например, вместо «Великий государь» получалось «Шеситий чолуцамь».

При шифровании должны выполняться определённые условия:

1)различные буквы должны обозначаться разными знаками: иначе получатель должен будет гадать, какую букву обозначает то или иной знак;

2) шифр должен быть трудноразгадываем;

3)операция шифрования должна быть относительно несложной.

**2. Практический раздел.**  Начать мы решили с **ROT1(Шаг вперёд)**. Этот шифр известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на Б, Б — на В, и т. д. Фраза **«Епвспё фусп» — это «Доброе утро».**

В процессе работы мы выяснили, что ROT1 — лишь один из вариантов **шифра Цезаря**. Получателю нужно просто сообщить, какой шаг использовался при шифровании: если ROT2, тогда А заменяется на В, Б на Г и т. д.

А здесь использован шифр Цезаря с шагом 5: **Иербэй йюк ёурбэй нтчйхйцтаъ энщхуж.**

Коды и шифры также делятся на подгруппы. Например, ROT1, шифр Цезаря относятся к моноалфавитной замене: каждая буква заменяется на одну и только одну букву или символ. Такие шифры очень легко расшифровываются:

1) если знаешь какое количество шагов по алфавиту нужно сделать, тогда просто делаем шаги в обратном порядке;

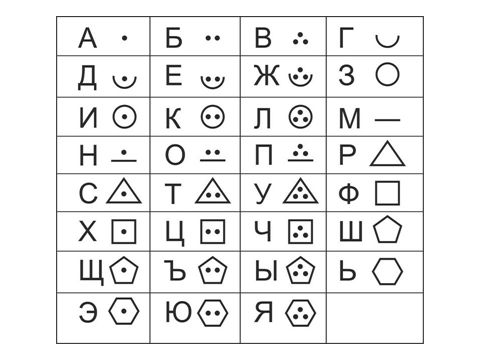
2) можно использовать метод подбора: для короткого слова **йюк** подобрать короткие слова и предлоги из русского языка;

3) очень легко расшифровываются подобные шифры с помощью **частотного анализа**.

Мы решили выяснить, как часто буквы русского алфавита встречаются в тексте. **Однако этот принцип работает только для длинных сообщений. Короткие просто не содержат в себе достаточно слов**. Для частотного анализа были использованы тексты из учебников литературного чтения, окружающего мира и хрестоматии по литературному чтению (см. Приложение 1) *Проанализировав* *полученные результаты, мы пришли к выводу: чаще всего встречается буква «О», а реже «Ъ».*

*Таким образом, в тексте, зашифрованном моноалфавитным шифром, наиболее часто встречающейся буквой будет буква, соответствующая «О».*

*Если заменить буквы на какие-либо иные символы, то секретность сообщения не изменится.*

   
Мы придумали свои шифры (см. Приложение 2)

**Эти шифры так же легко расшифровываются методом частотного анализа**.

На втором этапе мы попробовали поработать **с цифровыми шифрами**. С первого класса нам хорошо знаком способ простой подстановки, где каждая буква заменяется её порядковым номером в алфавите.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| БУКВЫ | А | Б | В | Г | Д | Е | Ё | Ж | З |
| ИХ ШИФР | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Мы решили усложнить расшифровывание и использовали **«кодовые слова».**

Например, нужно зашифровать фразу: **Мы пришли в школу. А кодовым словом будет слово из 4-х букв «утро».** Сложим порядковые номера букв из слов предложения и букв кодового слова.

М Ы П Р И Ш Л И В Ш К О Л У

14 29 17 18 10 26 13 10 3 26 12 16 13 21

+

У Т Р О У Т Р О У Т Р О У Т

21 20 18 16 21 20 18 16 21 20 18 16 21 20

=

35 49 35 34 31 46 31 26 24 46 30 32 34 41

**Б О Б А Э Л Э Ш Ц Л Ь Ю А Ж**

В результате получим зашифрованную фразу: **Бо баэлэш ц льюаж.**

***Для того, чтобы расшифровать это сообщение, обязательно нужно знать кодовое слово. И тогда нужно будет выполнить действия в обратном порядке, но уже не сложение, а вычитание.***

Обратите внимание на пробелы между словами. В предложении два коротких слова, которые можно попытаться подобрать. Многие наши одноклассники с этим заданием справились. Значит, и этот шифр достаточно легко расшифровывается (т.е. не является «криптостойким») даже без знания кодового слова. Попробуем для повышения криптостойкости нашего шифра внести следующие изменения:

1)избавимся от пробелов между словами;

2)внесём изменения в русский алфавит;

3)увеличим длину кодового слова.

Будем выполнять эти изменения по порядку.

1) Пробелу между словами дадим порядковый номер «0».

2) В русском алфавите 33 буквы. Мы добавим к буквам некоторые знаки препинания.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **А**  **1** | **Б**  **2** | **В**  **3** | **Г**  **4** | **Д**  **5** | **Е**  **6** | **Ё**  **7** | **Ж**  **8** |
| **З**  **9** | **И**  **10** | **Й**  **11** | **К**  **12** | **Л**  **13** | **М**  **14** | **Н**  **15** | **О**  **16** |
| **П**  **17** | **Р**  **18** | **С**  **19** | **Т**  **20** | **У**  **21** | **Ф**  **22** | **Х**  **23** | **Ц**  **24** |
| **Ч**  **25** | **Ш**  **26** | **Щ**  **27** | **Ъ**  **28** | **Ы**  **29** | **Ь**  **30** | **Э**  **31** | **Ю**  **32** |
| **Я**  **33** | **:**  **34** | **;**  **35** | **.**  **36** | **\***  **37** | **?**  **38** | **!**  **39** | **-**  **40** |

3) Увеличим длину кодового слова и постараемся подобрать такое слово, чтобы все буквы были разные: игрушка (7 букв, буквы не повторяются).

Посмотрим, что у нас получится при шифровании:

М Ы П Р И Ш Л И В Ш К О Л У

14 29 0 17 18 10 26 13 10 0 3 0 26 12 16 13 21

+

И Г Р У Ш К А И Г Р У Ш К А И Г Р

10 4 18 21 26 12 1 10 4 18 21 26 12 1 10 4 18

24 33 18 38 44 22 27 23 14 18 24 26 38 13 26 17 39

Ц Я Р ? Г Ф Щ Х М Р Ц Ш ? Л Ш П !

В результате получим зашифрованную фразу: **цяр?гфщхмрцш?лшп!**

***По этой шифровке невозможно определить границы слов, и следовательно, невозможно подобрать слова. Практически невозможно определить порядковый номер знаков препинания, трудно подобрать кодовое слово. А значит, нам удалось повысить криптостойкость обыкновенного цифрового шифра.*** Но с этим шифром, конечно, легко справятся профессиональные шифровальщики, воспользовавшись криптоанализом.

**Заключение** В современном мире, где практически каждый человек пользуется электронной почтой, где каждую минуту совершаются операции с электронной валютой, пересылаются личные email, подписываются электронные документы, шифры нужны как воздух. Нужны пользователям, чтобы защитить свою личную информацию и персональные данные. Нужны программистам, чтобы обеспечить безопасность проектируемых систем. Нужны специалистам по защите информации, чтобы представлять, чем и как лучше защищать корпоративные данные. Сейчас специалисты по защите информации самые востребованные специалисты на рынке труда. А значит, и к шифрам, и к шифрованию отношение остаётся самое серьёзное.

Но прошли столетия, изменились шифры и методы шифрования. В основе любого метода шифрования, по – прежнему, находятся математические методы и законы. Но об этом наше следующее исследование…

**Используемая литература**

1) Р. В. Душкин, Математика и криптография. Тайны шифров и логическое мышление – ЛитРес: <https://www.litres.ru/serii-knig/biblioteka-vunderkinda-nauchnye-skazki/>

2) Р. В. Душкин, Шифры и квесты: таинственные истории в логических загадках – ЛитРес: https://www.litres.ru/serii-knig/biblioteka-vunderkinda-3/

3) 10 популярных кодов и шифров - https://tproger.ru/translations/10-codes-and-ciphers/

Приложение 1





Приложение 2

