Региональная научно-практическая конференция учащихся  
«Мир - глазами детей»

Начальное общее образование 2 класс

Название работы  
«Шифрование»

Автор:  
Горшенин Николай Иванович, 2 «Б» класс, «Технический Лицей» города Обнинска

Научный руководитель:  
Солодухо Маргарита Владиславовна, заместитель директора по учебно-воспитательной работе (начальные классы), «Технический Лицей» города Обнинска

г. Обнинск 2018г

**План**

1. Что такое шифрование.
2. Почему я выбрал эту тему.
3. Как это работает.
4. Что такое алфавит.
5. Что такое ключ.
6. Перестановочный шифр. Теория.
7. Перестановочный шифр. Практика.
8. Диск Альберти.



* Это преобразование информации в другую форму или код таким образом, что доступ к ней сможет получить только тот пользователь, у которого есть секретный ключ.



* В свободное от уроков время, я читал книгу «Девочка с земли», автор Кир Булычёв. В этом рассказе, во время взлёта на коробле «Пегас», главные герои передавали сообщения диспетчеру в зашифрованном виде, чтобы их не перехватили космические захватчики. Мне стало интересно, что это такое «зашифрованный вид».



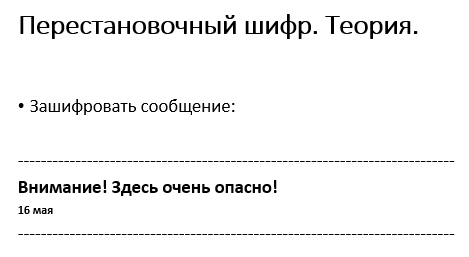
* Я узнал самый простой способ шифрования – перестановка букв. Этот способ использовали люди ещё 2 000 лет назад.
* Его главная идея состоит в том, что каждая буква из обычного алфавита заменяется другой буквой, из шифр-алфавита.



Что необходимо для того, чтобы использовать этот метод для шифрования сообщений:

1. Знать алфавит. Особенно порядок его букв!
2. Ключ.

* Алфавит это набор букв. Буквы в алфавите строго упорядоченны!
* Ключ - это самое важное в шифровании! Ключ помогает отправителю зашифровывать сообщения, а получателю правильно его расшифровать. Отправитель и получатель должны договориться заранее, что они будут использовать в качестве ключа.



* Для начала я расскажу Вам как это работает.
* Представим себе, что нам необходимо зашифровать следующее сообщение:

-------------------------------------------------------------

**Внимание! Здесь очень опасно!**

**16 мая**

-------------------------------------------------------------

Обратите внимание на дату в конце сообщения. Это будет наш ключ!

* Первое, что нам необходимо, это придумать шифр-алфавит. Ключом к созданию шифр-алфавита у нас будет ДАТА, которая указана в сообщение:

-----------------

16 мая

----------------

* Напишем её прописью:

----------------

шестнадцатое мая

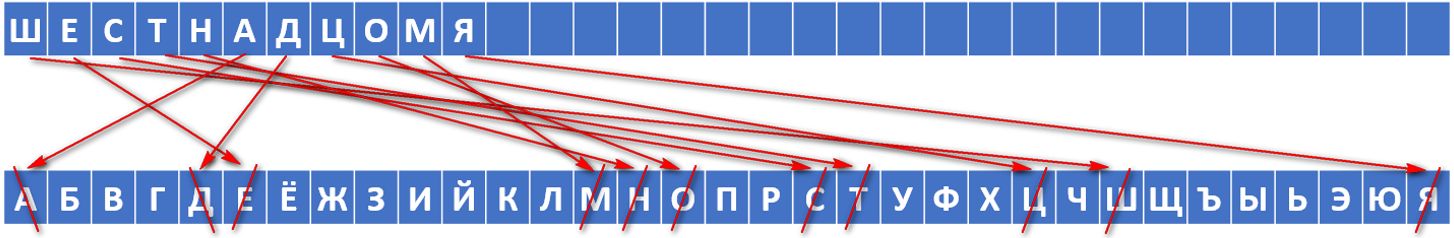
----------------



* Так как в буквы в алфавите не должны повторяться, нам необходимо вычеркнуть все повторяющиеся буквы из этого предложения!
* Начало нашего шифр-алфавита:



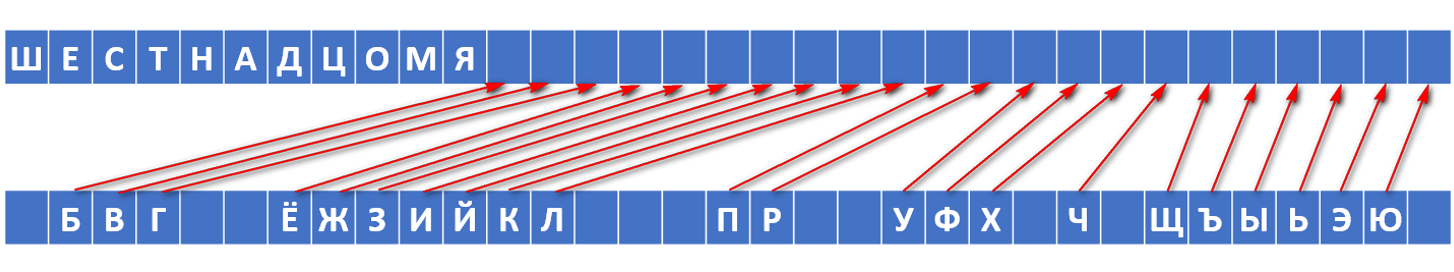
* Далее мы, уже найденные буквы, вычёркиваем из стандартного алфавита (ведь буквы не должны повторяться!):



* Вот что мы получим на этом этапе:



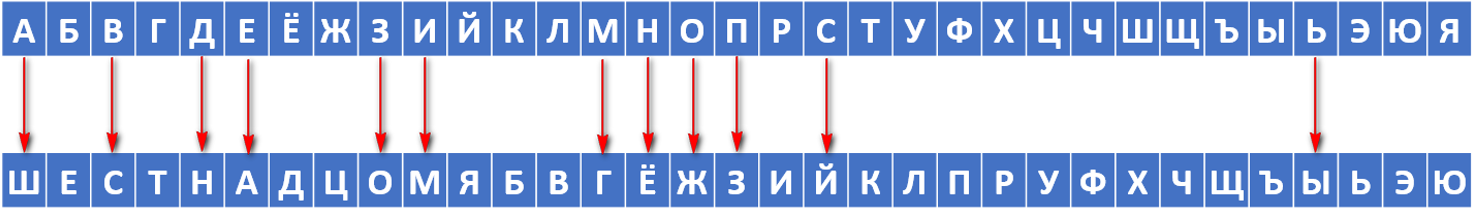
* И последнее, наш шифр-алфавит заполняется последовательно оставшимися буквами из стандартоного алфавита:



* В итоге, мы создали шифр-алфавит, на основе ключа: «16 мая»:



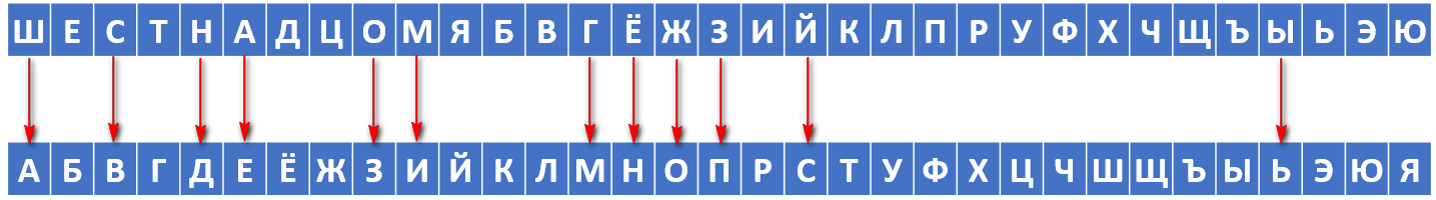
* УРА!!! Теперь мы можем зашифровать наше сообещние!
* Чтобы зашифровать сообщение: **Внимание! Здесь очень опасно!**  нам необходимо сопоставить буквы из стандартого алфавита с шифр-алфавитом:



* И наконец теперь, наше сообщение будет выглядень следующим образом:



* Его-то мы и отправим получателю!
* Помните, что для того, чтобы получатель смог расшифровать сообщение, ему обязательно необходимо передать дату! Ведь дата в нашем случае это ключ к расшифровыванию сообщения!
* По этой дате, получатель составит шифр-алфавит и сопоставит буквы из него с настоящим алфавитом:



* Зашифрованное сообщение было:

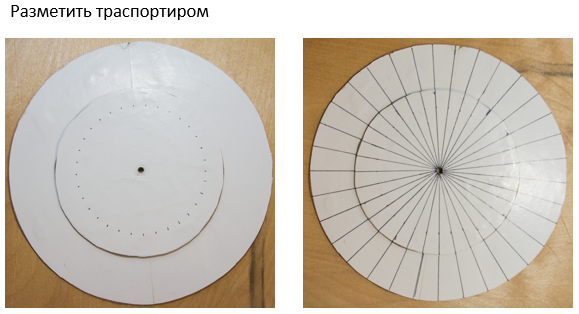
**ВНИМАНИЕ ЗДЕСЬ ОПАСНО**



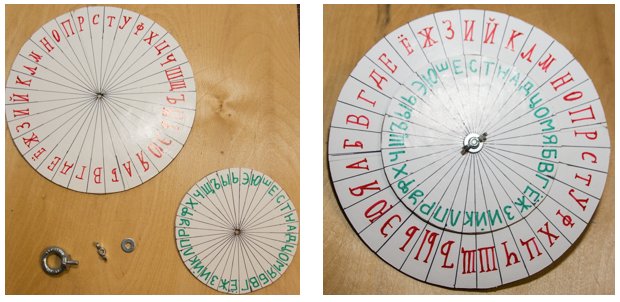
* Мы с папой смастерили прибор, который позволяет зашифровывать и расшифровывать сообщения очень быстро.
* Его придумал архитектор из Италии по фамилии Альберти почти 500 лет назад. Этот прибор так и называется – диск Альберти.



* Диск Альберти состоит из двух вращающихся дисков.
* Большой круг содержит стандартный алфавит.
* Малый круг содержит шифр-алфавит.



* Диски размечены транспортиром
* Круг содержит 360 градусов
* 360 поделить на 33, разчерить, вписать буквы.



**Заключение.**