Государственное бюджетное общеобразовательное учреждение
«Инженерно-технологическая школа № 777»
Санкт-Петербурга

НАУЧНО-ТЕХНИЧЕСКИЙ ПРОЕКТ
«Создание прибора для шифрования»

Техническое направление «Прототипирование, конструирование»

Автор (ФИО полностью, дата рождения)
Михлина Станислава Андреевна, 26.09.2012

Класс 2.7

Научный руководитель/консультант (ФИО полностью, должность)
Бик Алевтина Фёдоровна, учитель начальных классов

Образовательное учреждение
Государственное бюджетное образовательное учреждение «Инженерно-технологическая школа №777», г. Санкт-Петербурга, Лыжный пер., 4/2, строение 1, school777spb@yandex.ru, +7 (812) 246-35-80

Санкт-Петербург, 2020 год

Введение

Шифрование известно с древних времён. Его использовали правители и полководцы, чтобы защитить важную для себя информацию от посторонних. Потом зашифрованные сообщения стали использовать при дипломатических переписках, без них не могли обойтись шпионы и разведчики.

В современном мире шифрование используют во многих сферах жизни: при оплате покупок по банковским картам, при создании паролей, в переписке по почте и телефону. Современное шифрование тесно связано со сложными разделами математики: алгеброй, комбинаторикой, теорией вероятности и другими.

Я тоже люблю делать секретные записи: могу написать для друзей невидимыми чернилами из сока лимона или молока и зашифровать сообщения для брата, ещё люблю расшифровывать сообщения, адресованные мне. Делаю это, чтобы сохранить важную для себя информацию в секрете.

Гипотезы:

- ✓ Знание и использование шифра помогает защитить информацию от посторонних;
- ✓ Если знаешь ключ шифра, то можно расшифровать сообщение.

Цель проекта: изучение шифров и изготовление прибора для шифрования своими руками.

Объект исследования: шифры.

Предмет исследования: прибор для шифрования.

В ходе проекта я планирую решить **задачи:**

- ✓ Изучить, что такое шифрование и шифры;
- ✓ Научиться использовать разные шифры на практике;
- ✓ Изготовить прибор для шифрования своими руками.

Для достижения цели буду использовать теоретические методы, такие как сбор материала и анализ предметной области, и экспериментальный, - сконструирую прибор для шифрования и зашифрую с его помощью слово.

1. ГЛАВА 1. Что такое шифрование?

1.1. Шифрование, шифр и ключ шифра.

В современном мире люди обмениваются друг с другом огромным количеством информации. Чтобы информация не попала в чужие руки используют шифрование. Информация – это передаваемое сообщение, которое надо скрыть от посторонних. Шифрование – это изменение сообщения так, чтобы оно стало понятным для своих и непонятным для посторонних. Способ изменения сообщения называется шифром. У шифра обычно есть ключ. Ключ –это дополнительная информация, которая помогает прочитать секретные сообщения. Прибор для шифрования секретных сообщений называется шифровальной машиной.

Шифры можно разделить на две группы: шифры перестановки и шифры замены. В шифрах перестановки буквы в сообщении просто меняются местами. Пример шифра – решетка Кардано. Ключ к разгадке шифра – шифровальная решётка. В шифрах замены каждая буква заменяется на другую букву. Ключ к разгадке шифра – правило, по которому меняется буква. Пример шифра замены – Шифр Цезаря.

1.2. Шифр перестановки: решетка Кардано

Решетка Кардано – квадрат из 6*6, 8*8 клеток (и т.д.), некоторые из которых вырезаны. Клетки должны иметь такой размер, чтобы в каждую помещалась ровно одна буква. Для облегчения создания решёток Кардано можно воспользоваться конструктором решёток.

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Рисунок 1.

Например, для создания решётки 8*8 (см. рисунок 1) нужно разделить квадрат 8*8 на четыре квадрата размером 4*4 и пронумеровать клетки внутри каждого малого квадрата от 1 до 16. Затем вырезать строго одну из четырёх клеток с номером 1, строго одну из четырёх клеток с номером 2 и т.д. Чтобы зашифровать сообщение,

нужно разместить решётку на бумаге и вписать часть текста в вырезанные клетки, затем повернуть решётку на 90° и вписать следующую часть и т. д. Если останутся пустые места на бумаге, то нужно вписать произвольные буквы.

1.3. Шифр замены: шифр Цезаря

В шифре Цезаря каждая буква сдвигается по алфавиту вправо на одно и то же число. Этот шифр изобрел римский правитель Юлий Цезарь, который использовал его со сдвигом 3, чтобы защищать военные сообщения.

Рассмотрим пример шифрования с использованием ключа «сдвиг на 3 буквы» (см. рисунок 2). Буква «А» «сдвигается» на три буквы и заменяется на букву «Г», буква «Б» заменяется на букву «Д», буква «В» - на букву «Е».

Алфавит	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
Шифр	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	А	Б	В

Рисунок 2.

Буква «Э», перемещённая на три буквы вперёд, становится буквой «А», а буква «Я», перемещённая на три буквы вперёд, становится буквой «В».

Если сопоставить каждой букве алфавита её порядковый номер (начиная с 0), то с точки зрения математики шифр Цезаря можно записать так:

$y = x + k$ – сдвиг вправо – шифрование,

$x = y – k$ – сдвиг влево – дешифрование,

где x - буква исходного текста, y - буква шифра, k – ключ.

2. ГЛАВА 2. Использование шифров на практике.

2.1. Зашифруем тему моего проекта

Тема моего проекта «Я – разведчик секреты шифрования». В названии темы 27 букв. Я решила использовать решётку 6*6, в которой всего 36 клеток.

27 клеток из 36 пойдут для названия темы, а в оставшиеся 9 клеток я впишу свою фамилию «Михлина С.». Для облегчения создания решётки я сделала конструктор размером 6*6 клеток. Решётку 6*6 (см. рисунок 3) нужно разделить на четыре квадрата размером 3*3 и пронумеровать клетки внутри каждого малого квадрата от 1 до 9. Затем вырезать 9 клеток в произвольном порядке, но строго только одну из четырёх клеток с номером 1, строго только одну из четырёх клеток с номером 2 и т. д. Получилась вот такая решетка (см. рисунок 4).

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Рисунок 3.

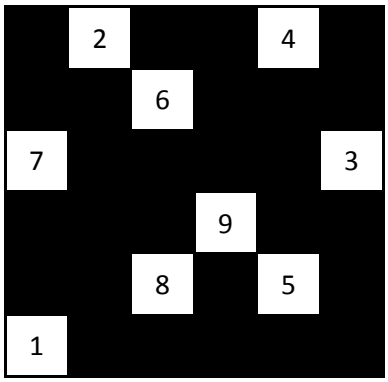

Рисунок 4.

К	Я	М	С	Р	И
И	Ф	А	Р	Х	Е
З	К	О	Л	Р	В
В	И	Е	Е	Н	А
А	Т	Д	Н	Ч	Ы
И	И	С	Ш	Я	.

Рисунок 5.

Потом я разместила решётку на бумаге и вписала часть темы в вырезанные клетки, затем повернула решётку на 90° вправо и вписала следующую часть и т. д. В последние пустые клетки на бумаге, я вписала свою фамилию (см. рисунок 5). Получился интересный шифр, ключом к нему служит шифровальная решётка с вырезанными клетками (см. ПРИЛОЖЕНИЕ 1).

2.2. Где зарыт клад?

В шифре Цезаря каждая буква исходного текста заменяются следующей после неё буквой в алфавите со сдвигом на некоторое число. При этом можно использовать разные величины сдвига.

Зашифруем сообщение «ГДЕ ЗАРЫТ КЛАД?» шифром Цезаря с ключом «сдвиг на 1 букву» (см. рисунок 6). В этом случае в зашифрованном сообщении буква «А» «сдвигается» вправо на одну букву и заменяется на букву «Б», буква «Б» заменяется на букву «В», буква «В» - на букву «Г» и т.д.

Алфавит	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
Шифр	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	А

Рисунок 6.

Тогда зашифрованное сообщение будет выглядеть так (см. рисунок 7).

СДВИГ НА 1 БУКВУ												
Сообщение	г	д	е	з	а	р	ы	т	к	л	а	д
Шифр	Д	Е	Ё	И	Б	С	ь	У	Л	М	Б	Е

Рисунок 7.

Отправим его нашему другу разведчику. При этом мы знаем, что другой разведчик использует ключ «сдвиг на 3 буквы» (см. рисунок 8).

Алфавит	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
Шифр	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	А	Б	В

Рисунок 8.

Когда в ответ мы получим зашифрованное сообщение (см. рисунок 9), то сможем расшифровать, выполнив обратное преобразование: буква «Н» «сдвигается» влево на 3 буквы и заменяется на букву «К», буква «О» - на букву «Л» и т.д. (см. рисунок 10). Теперь мы знаем, что «КЛАД ЗАРЫТ В САДУ».

Сообщение														
Шифр	Н	О	Г	Ж	К	Г	У	Ю	Х	Е	Ф	Г	Ж	Ц

Рисунок 9.

СДВИГ НА 3 БУКВЫ														
Сообщение	к	л	а	д	з	а	р	ы	т	в	с	а	д	у
Шифр	Н	О	Г	Ж	К	Г	У	Ю	Х	Е	Ф	Г	Ж	Ц

Рисунок 10.

Сделаем вывод: кроме шифра важно знать - какой ключ использовался!

3. ГЛАВА 3. Прибор для шифрования

3.1. Основные детали прибора

Мне понравился шифр Цезаря. Но запоминать алфавиты со сдвигом сложно, можно запутаться. Я решила сделать прибор, чтобы пользоваться этим шифром. Я люблю собирать из LEGO, поэтому собирала прибор из него.

Основные детали прибора – диск для задания ключа, ротор, зубчатое колесо, коническое колесо, маркер, два алфавита, цепь и направляющие для цепи. Всё сделано из LEGO. Внешний вид основных деталей, узлов и самого прибора для шифрования представлен в ПРИЛОЖЕНИИ 2.

3.2. Чертежи основных узлов

Для того чтобы, вращая диск для задания ключа, двигать алфавит шифра, мне потребовалось узнать про зубчатые передачи. Зубчатая передача передает вращение с одного колеса на другое. Я изучила внешние виды и чертежи зубчатых передач и выбрала две:

1) реечная зубчатая передача служит для перемещения цепи с алфавитом шифра (см. рисунок 11);
2) коническая зубчатая передача связывает ротор с диском и реечной передачей (см. рисунок 12).

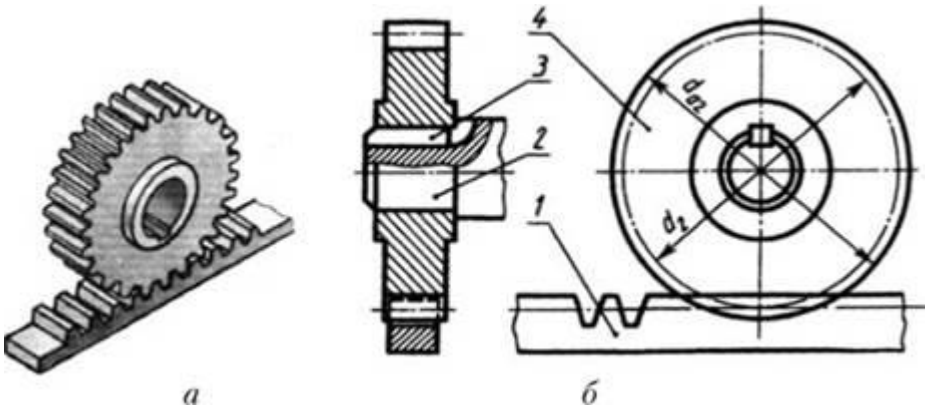

Рисунок 11. Реечная зубчатая передача: а) внешний вид, б) чертеж.

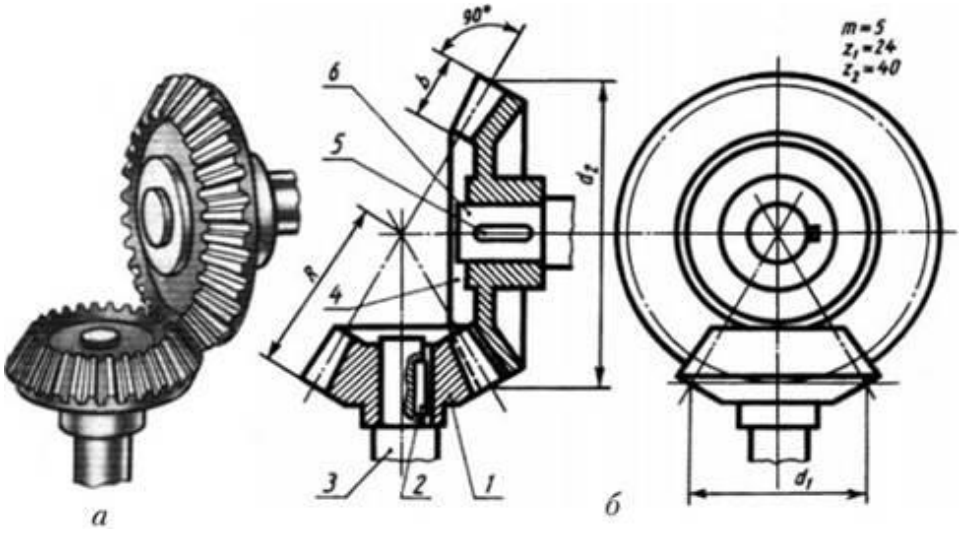

Рисунок 12. Коническая зубчатая передача: а) внешний вид, б) чертеж.

3.3. Этапы создания прибора

1 ЭТАП – создание конической зубчатой передачи: соединение зубчатого и конического колеса, чтобы они крутились вместе.

2 ЭТАП – сборка палочки-ротора с диском, соединенной с зубчатой передачей.

3 ЭТАП – создание цепи, сборка основания прибора и соединение зубчатой передачи и реечной передачи с цепью, установка конструкции на основание.

4 ЭТАП – нанесение исходного алфавита и алфавита шифра на подвижную и неподвижную части прибора.

5 ЭТАП – разметка диска и установка башни с указателем.

3.4. Как работает прибор

Чтобы показать, как работает мой прибор, зашифруем слово «ЗАГАДКА» по шифру Цезаря со сдвигом на 3 буквы. Выставим на диске: ключ = 3. Смотрим на прибор буква «З» заменяется на букву «К», буква «А» заменяется на букву «Г», буква «Г» - на букву «Ё». Получили зашифрованное сообщение (см. рисунок 13). Недостаток этого шифра в том, что три одинаковые буквы «А» превращаются в три одинаковые буквы «Г». И шифр легко разгадать.

С помощью моего прибора можно сделать хитрее. Зададим ключ = 2609 – день моего рождения. Запишем слово «ЗАГАДКА» и под каждой буквой разместим цифру ключа. Выставим на диске ключ для первой буквы: ключ = 2. Находим на приборе, что буква «З» заменяется на букву «Й». Для второй буквы ключ = 6. Выставляем на приборе, тогда буква «А» заменяется на букву «Ё» и т.д. Так получим всё зашифрованное слово (см. рисунок 14).

Сообщение	З	А	Г	А	Д	К	А
КЛЮЧ	3	3	3	3	3	3	3
Шифр	К	Г	Ё	Г	Ж	Н	Г

Рисунок 13.

Сообщение	З	А	Г	А	Д	К	А	
КЛЮЧ	2	6	0	9	2	6	0	9
Шифр	Й	Ё	Г	И	Ё	Р	А	

Рисунок 14.

Мой прибор может шифровать сообщение, в котором каждая буква сдвигается по алфавиту на разное число от 0 до 9, получается буква «А» заменяется буквой «Ё», буква «А» - буквой «И», буква «А» остается буквой «А». Сделаем вывод: такой шифр разгадать сложнее! Такой шифр называется шифром Виженера.

3.5. Ограничение конструкции прототипа

В зубчатой передаче использованы одно коническое колесо и одно обычное, вместо двух конических колес, поэтому сцепление между ними оказывается хуже и быстро диск крутить нельзя. Это ограничение связано с тем, что у Lego нет больших конических колес.

3.6. Перспективы развития

Прототип можно улучшить двумя способами:

1) усложнить конструкцию, чтобы шифровать несколько букв сразу или слово целиком;

2) установить двигатель для автоматического вращения диска, например, используя детали конструктора LEGO Mindstorm. В этом случае ключ может быть не из цифр, а из цветов (красный, синий, жёлтый и т.д).

Заключение

В современном мире шифрование вошло в нашу повседневную жизнь. Задача изменить информацию так, чтобы посторонние люди не смогли её понять и воспользоваться – не только очень увлекательна, но и полезна.

По результатам проекта, я сделала такие выводы:

- ✓ Каждый шифр – это логическая задача. Даже если школьники начальных классов ещё не знакомы со сложными разделами математики, у них решение задач по шифрованию развивает логику и изобретательность, что очень важно для юных инженеров.
- ✓ Из LEGO можно делать настоящие устройства. Я думаю, что такое конструирование в форме познавательной игры хороший способ развития технического и конструкторского мышления. Мой прибор работает!
- ✓ Самые важные составляющие шифра – правило, по которому изменяется исходное сообщение, и ключ. Важно знать не только шифр, но и ключ от шифра. С ключом разгадать шифр быстрее и проще.
- ✓ Все ключи и пароли необходимо хранить в секрете.

Я подтвердила гипотезы и выполнила задачи. Мне понравилось, что в своей работе получилось изучить тему, а потом применить полученные знания на практике: сделать макет шифровальной решётки и собрать действующий прототип прибора для шифрования.

Литература

1. Решетка Кардано. Шифр Цезаря. Шифр Виженера. Википедия – электронная энциклопедия.
2. История шифров. Виктория Журавлева. Издательство «Настя и Никита», 2020.
3. Криптография и взлом шифров на PYTHON: Глава: Шифр Цезаря. Эл Свейгарт. Издательство «Диалектика», 2020 г.
4. Статья «Криптография». Журнал «Наука и жизнь» №7, 2020 г.
5. Математика и криптография. Роман Душкин. Издательство «АСТ», 2017 г.
6. Naked science: история криптографии. Https://naked-science.ru/article/sci/ot-manuskriptov-do-shifrovalnyh
7. Конические передачи. https://studme.org/35950/tovarovedenie/konicheskie_peredachi
8. Планета Excel. Защита ячеек шифром Виженера. https://www.planetaexcel.ru/techniques/5/212/

ПРИЛОЖЕНИЕ 1. Макет шифровальной решётки

Рисунок 1. Зашифрованное сообщение. Рисунок 2. Шифровальная решётка.

1)

2)

3)

4)

Рисунок 3. Этапы дешифрования сообщения.

ПРИЛОЖЕНИЕ 2. Прототип: шифровальный прибор

Рисунок 1. Основные детали прибора.

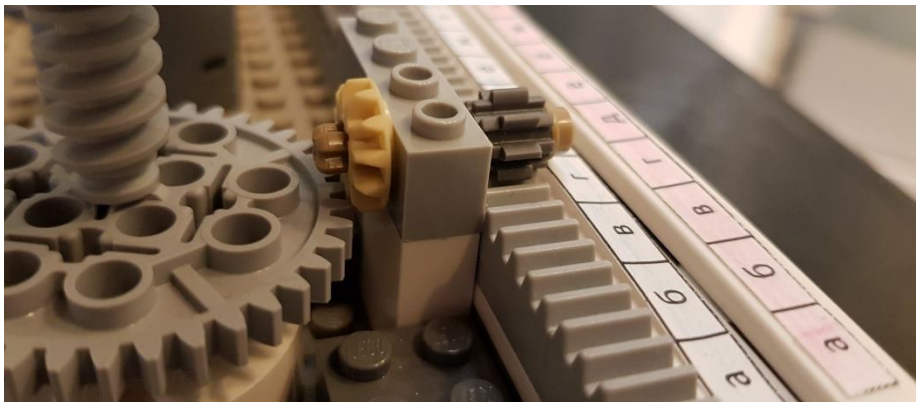

Рисунок 2. Внешний вид зубчатой и реечной передач.

Рисунок 3. Внешний вид прибора для шифрования.