

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ Г. ЕКАТЕРИНБУРГА
МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 84
ЧКАЛОВСКОГО РАЙОНА Г. ЕКАТЕРИНБУРГА

«Ш И Ф Р Ы»

Предмет: математика

Исполнитель: ученик 7 «а» класса

Медведев Александр

Руководитель: Русакова

Елизавета Андреевна

Екатеринбург - 2011

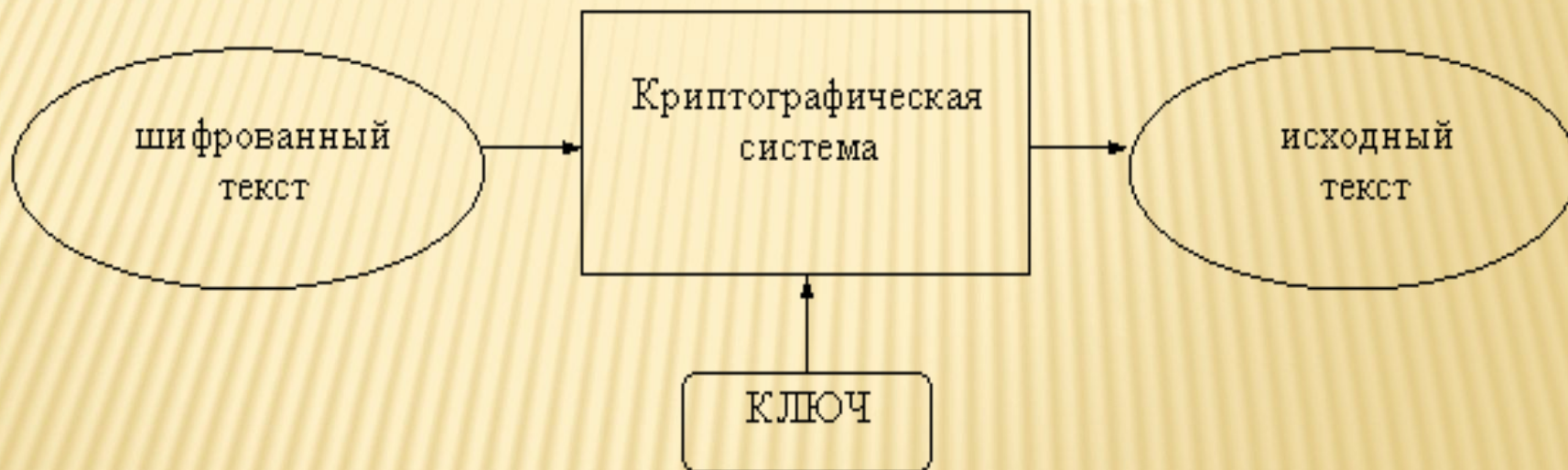
Цель: ознакомиться с различными видами шифров.

Задачи:

- научиться сохранять информацию посредством её шифрования;
- научиться приемам дешифровки.

ШИФР - СОВОКУПНОСТЬ УСЛОВНЫХ ЗНАКОВ, ПРИМЕНЯЕМЫХ ДЛЯ СЕКРЕТНОЙ ПЕРЕПИСКИ.

Процедура шифрования:



Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

ПЕРИОДЫ РАЗВИТИЯ ШИФРОВАЛЬНОГО ДЕЛА

Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

Второй период (хронологические рамки — с **IX века** на Ближнем Востоке и с **XV века** в Европе — до начала **XX века**) характеризуется тем, что на смену моноалфавитным шифрам пришли полиалфавитные шифры.

Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков.

Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии.

Однако до **1975 года** криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — **криптография с открытым ключом**.

ВИДЫ ШИФРОВ

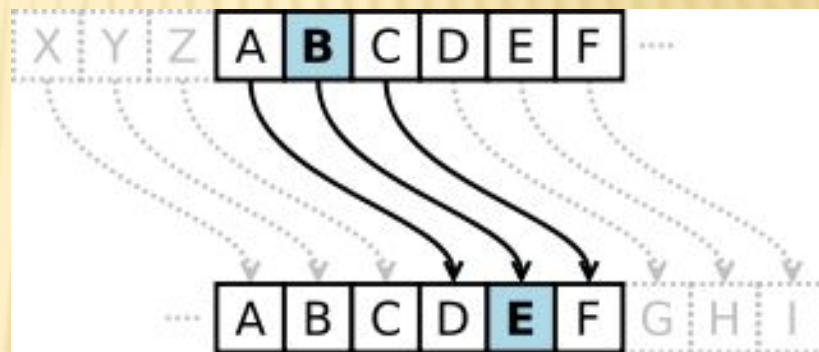
1.	Лингвистические	перестановки	Простая перестановка; Одиночная перестановка; Двойная перестановка; <u>Скитало</u> ; <u>Шифр Цезаря</u> .
		решетки	Шифр Виженера; <u>Решетка Кардано</u> .
2.	Знаковые	перестановки	<u>Тайнопись «уголки»</u> ; <u>Пляшущие человечки</u> ; <u>Шифры-полуфабрикаты</u> .
3.	Математические	перестановки	Двоичная система счисления; Матрица; <u>«Магический квадрат»</u> ; Шифр Гронсфельда; Шифрование с помощью цифр.
		решетки	<u>Квадрат Полибия</u>

ЛИНГВИСТИЧЕСКИЕ ШИФРЫ



Скитало

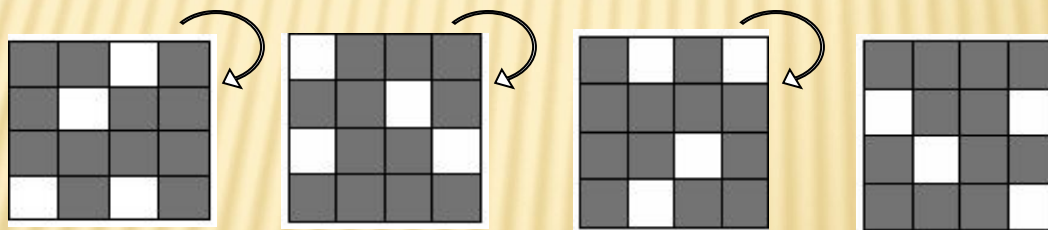
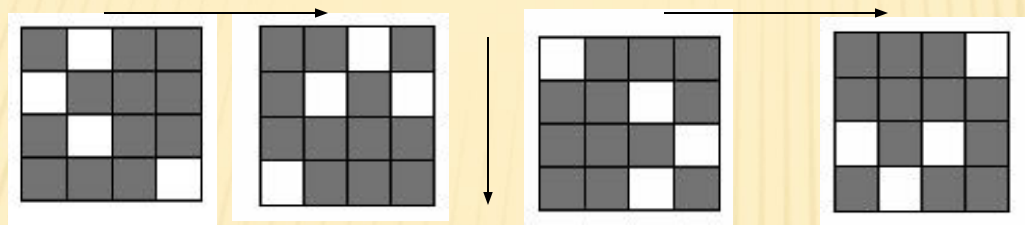
Шифр Цезаря



YHQL YLGL YLFL

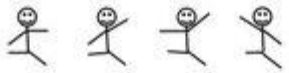
«Veni, vidi, vici» - «Пришел, увидел, победил»

Решетка Кардано



ЗНАКОВЫЕ ШИФРЫ

1. Пляшущие человечки;



А		Б		В		Г	
Д		Е		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	

2. Тайнопись «уголки»;

3. Шифры-полуфабрикаты.

МАТЕМАТИЧЕСКИЕ ШИФРЫ

«Магический квадрат»

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

Магических квадратов 4 x 4 насчитывается уже 880, а число магических квадратов размером 5 x 5 около 250000.

Приезжаю Сегодня.

.ирдзегюСжаоеянП

Квадрат Полибия

A	B	C	D	E
F	G	H	I, J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

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

13 34 22 24 44 34 15 42 22 34 43 45 32
(Cogito ergo sum)

Шифр Гронсфельда

сообщение

СОВЕРШЕННО СЕКРЕТНО

ключ

3143143143143143143

шифровка

ФПЖИСЬИОССАХИЛФИУСС

ПРАКТИЧЕСКОЕ ЗАДАНИЕ:

Дешифруйте высказывание

В.П. Ермакова используя:

- **квадрат Полибия**

«13 26 11 36 16 26 11 36 23 24 16 35 25 16 15 41 16 36 33 32
26 31 23 36 53 31 16 42 32 34 26 41 25 52 , 11 33 34 32 44 16
35 35 52 26 52 46 25 16 31 23 56»

- **шифр Гронсфельда**

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
261198261198261198261198261198261198261198261198261

«ДТБУПФВШКЛПЩНМЕФПЫСФНОТЫЮУЖХЧШОЩМЬКЧТФЧЖЫ
ЩЭТЬЩФОППА»

ИТОГИ РАБОТЫ:

1. Определены основные понятия;
2. Описаны основные периоды развития шифровального дела;
3. Рассмотрены основные виды шифров;
4. Я научился шифровать и дешифровать текст при помощи некоторых видов шифров.

Работа по данной теме была интересной и увлекательной.

ОТВЕТ НА ПРАКТИЧЕСКОЕ ЗАДАНИЕ

**«В математике следует помнить
не формулы, а процессы
мышления»**

В.П. Ермаков

ИСТОЧНИКИ ИНФОРМАЦИИ:

- ✓ <http://www.aggregateria.com/SN/shifr.html>
- ✓ <http://www.zxpress.ru/article.php?id=1832>
- ✓ <http://ru.wikipedia.org/wiki/>
- ✓ <http://www.elitarium.ru/>