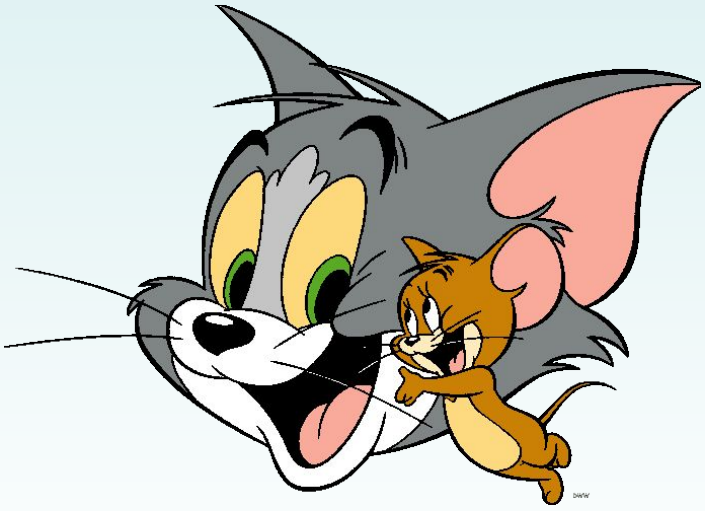
Тема урока:



Зашифрованная переписка

Особенности шифрования информации Второй мировой войны

Во времена Второй мировой войны шифрование посланий стало ключевым заданием.

Перед началом Второй мировой войны ведущие мировые державы имели электромеханические шифрующие устройства, результат работы которых считался невскрываемым.

Особенности шифрования информации Второй мировой войны

Эти устройства делились на два типа — роторные машины и машины на цевочных дисках. К первому типу относят «Энигму», использовавшуюся сухопутными войсками Германии и её союзников, второго типа — американская М-209.

В СССР производились оба типа машин.

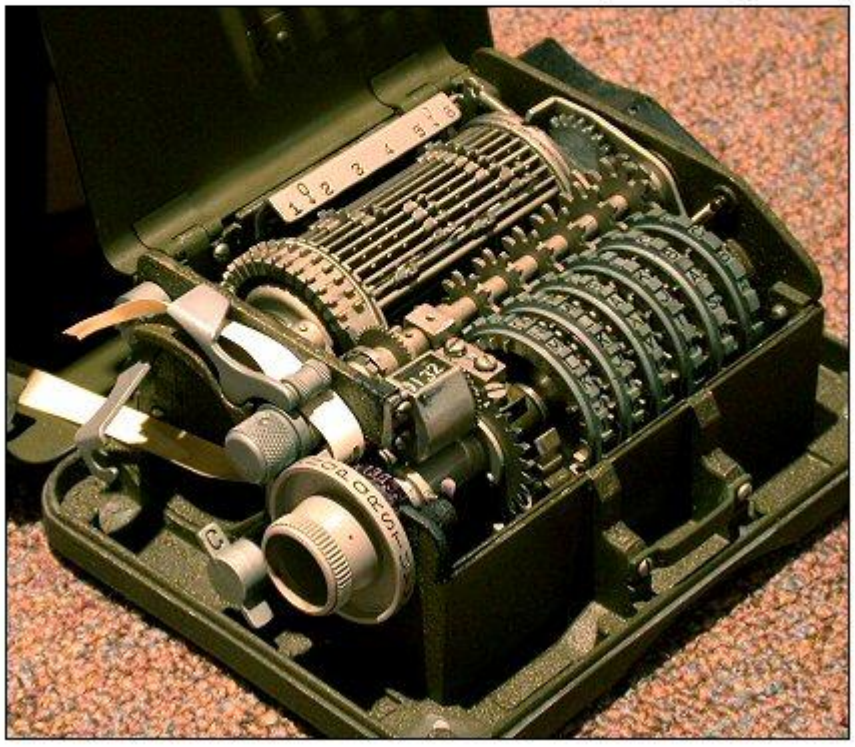
Самая яркая шифровальная машина, которая внесла значительный вклад в историю - Эни́гма

Это портативная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений.

Энигма представляла собой как бы динамический шифр Цезаря. Т.е. изначально на барабаных выставлялось некое начальное значение (этакий random seed), которое и являлось ключом. Далее, при наборе букв, каждая буква шифровалась шифром цезаря, а потом, этот шифр менялся на другой.

Американская шифровальная машина М-209

HAGELIN M-209 CIPHER MACHINE (GVG / PD)



Машина состояла из 6 колёс, комбинация выступов которых давала значение сдвига для буквы текста. Хотя машина не могла использоваться для шифрования серьёзного трафика.

М-209

была популярна в армии из-за малого веса, размера и лёгкости в обучении.

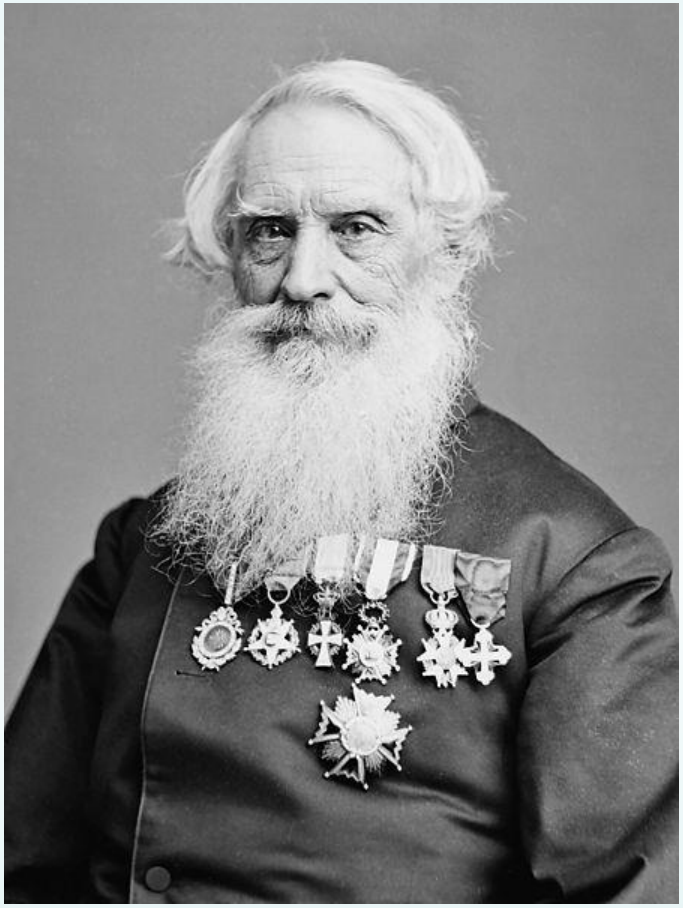
Азбука Морзе

Все мы слышали об Азбуке Морзе, которую более века использовали военные и гражданские специалисты в области связи. Изобрел ее американец Сэмюэл Финли Бриз Морзе в 1838 году.

«Морзя́нка» — способ знакового кодирования, представление букв алфавита, цифр, знаков препинания и других символов последовательностью сигналов: длинных («тире») и коротких («точек»)).

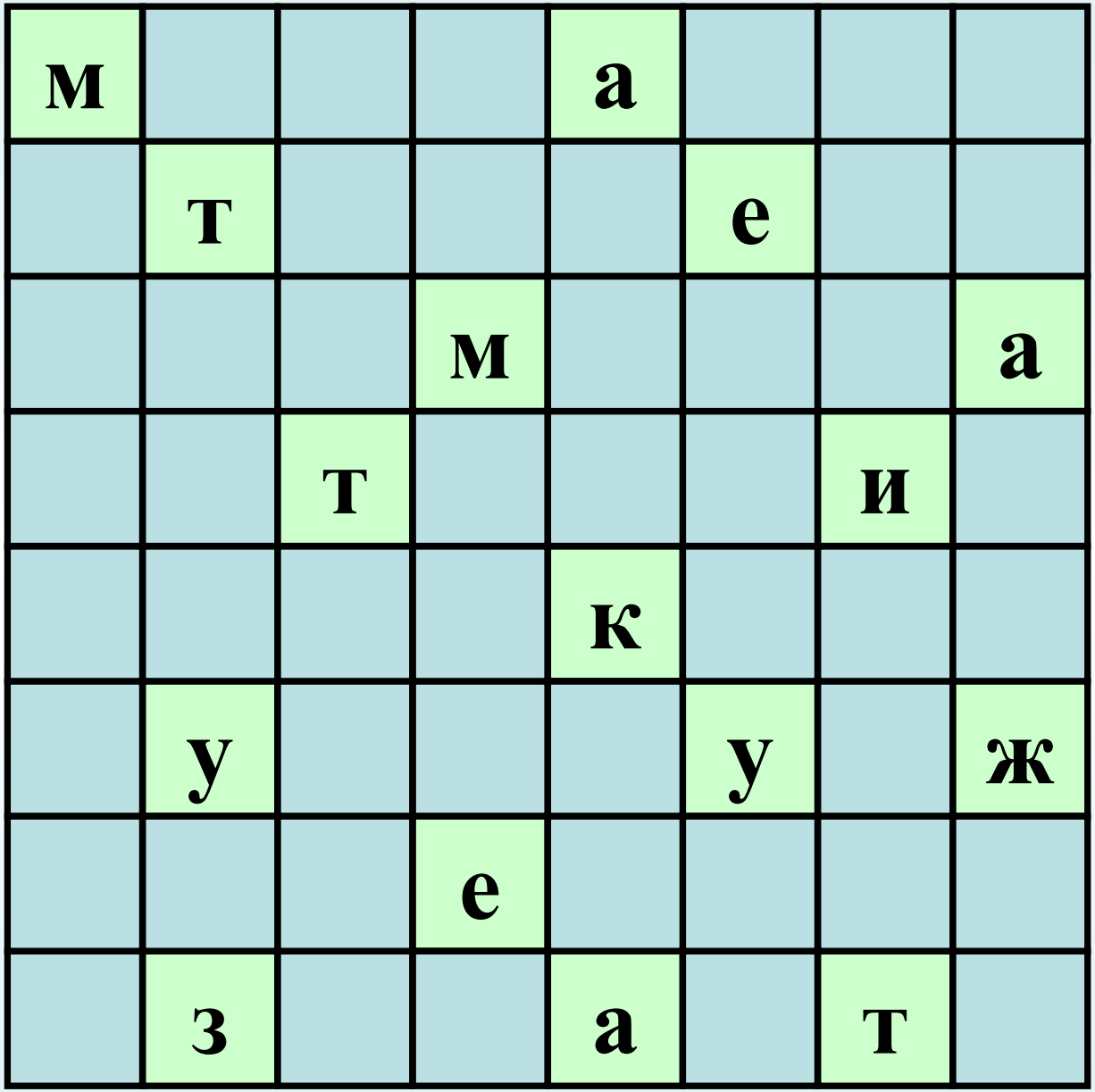
Азбука Морзе

А	·—	Й	·——	Т	—	Ы	—·—	5	·····
Б	—···	К	—·—	У	··—	Ь	—··	6	—····
В	·——	Л	·—··	Ф	··—·	Э	··—··	7	——···
Г	——·	М	——	Х	····	Ю	··——	8	———··
Д	—··	Н	—·	Ц	—·—·	Я	·—·—	9	————·
Е, Ё	·	О	———	Ч	———	1	·————	0	—————
Ж	···—	П	·——·	Ш	————	2	··———	!	——·——
З	——··	Р	·—·	Щ	——·—	3	···——	.	····——
И	··	С	···	Ъ	——·——	4	····—	,	·—·—·—



Задание :

Расшифруйте высказывание первого русского ученого.


м а
т е
м а
т и
к
у у ж
е
з а т

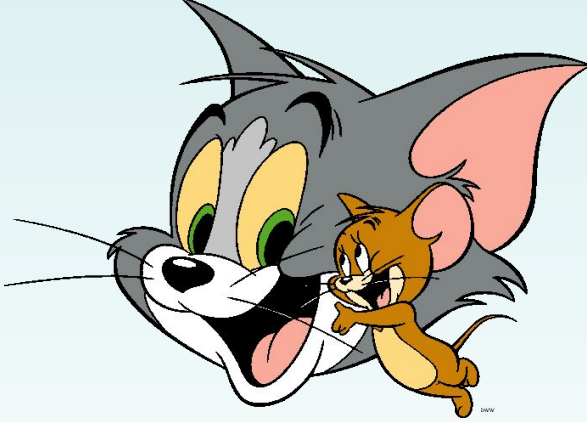
Михаил Васильевич Ломоносов

1711 – 1765

Первый русский ученый-естествоиспытатель мирового значения, поэт, заложивший основы современного русского литературного языка, художник, историк, поборник развития отечественного просвещения, науки и экономики.

Математику уже затем учить надо,
что она ум в порядок приводит.

Алгоритм шифрования:



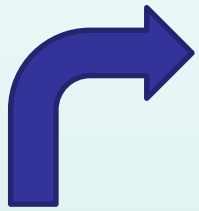
1. Наложить решетку на бумагу, писать сообщение в окошечках решетки
2. Сначала помещается 16 букв сообщения
3. Поворот решетки по часовой стрелке на 90º
4. Следующие 16 букв сообщения
5. Ещё 2 поворота и текст вписан
6. Если остаются неиспользованные клетки, их заполняют буквами(а,б,в,г и тд.),чтобы не было пробелов

Задание : Зашифровать фразу:
Если ты будешь любознательным, то будешь много знающим.

Алгоритм шифрования:

1. Наложить решетку на бумагу, писать сообщение в окошечках решетки
2. Сначала помещается 16 букв сообщения
3. Поворот решетки по часовой стрелке на 90º
4. Следующие 16 букв сообщения
5. Ещё 2 поворота и текст вписан
6. Если остаются неиспользованные клетки, их заполняют буквами(а,б,в,г и тд.),чтобы не было пробелов

е							
			с				л
и			т			ы	
		б					
у				д		е	
		ш				ь	
	л						ю
			б		о		



Поворот –

геометрическое преобразование фигуры, при котором свойства фигуры не меняются, может измениться лишь положение фигуры, так как каждая его точка повернется вокруг некоторой точки на угол поворота