ПРОЕКТ «КОДЫ СИМВОЛОВ»

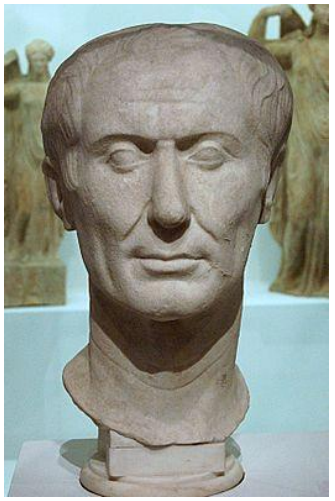
Занятие 1 - Шифры

Скитала

	Э	Т	О	Ш	И	
	Ф	Р	Д	Р	Е	
	В	Н	Е	Й	С	
	П	А	Р	Т	Ы	

- *ЭФВПТРНАОДЕРШРЙТИЕСЫ*

Шифр Цезаря



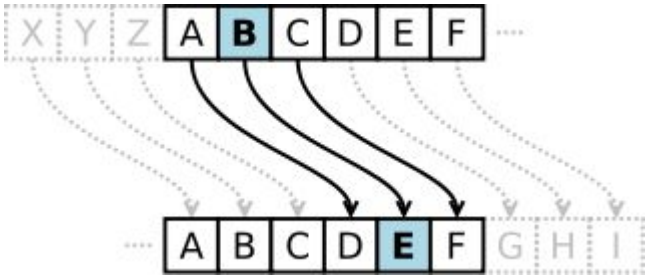
Шифр Цезаря со сдвигом на 3:

A заменяется на **D**

B заменяется на **E**

и так далее

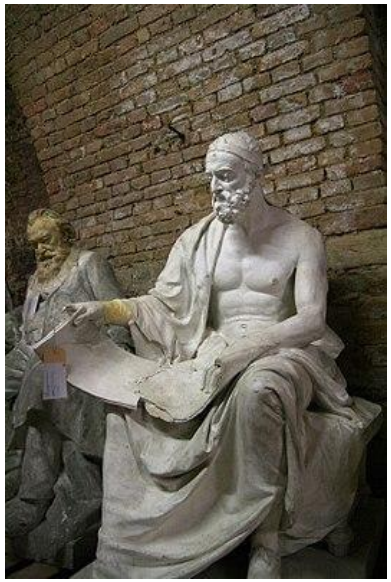
Z заменяется на **C**



Квадрат Полибия

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

До шифрования: SOMETEXT
После шифрования:
XTRKYKCY

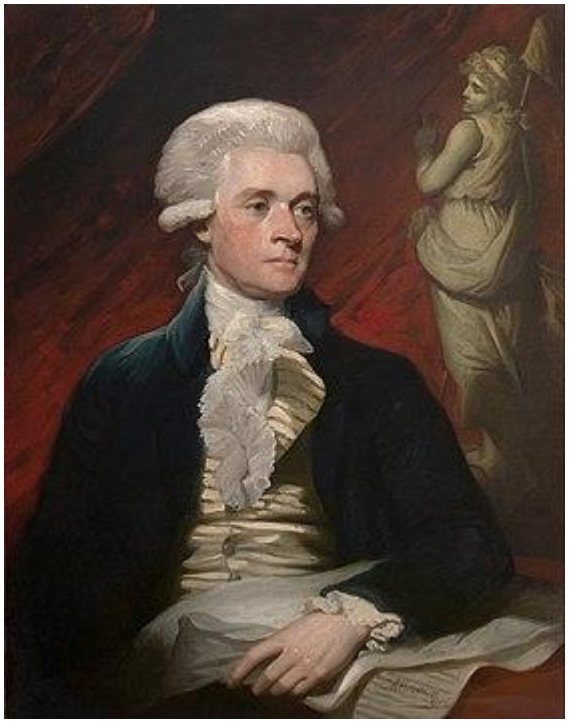


Можно составить квадрат Полибия для русского алфавита

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

До шифрования –
ПРОГРАММА
После - ?

Цилиндр Джефферсона



Шифр простой замены

Метод взлома данного шифра основан на частотном анализе. Легко заметить, что в осмысленном тексте русского языка буква «о» встречается гораздо чаще чем буква «э».

Статистика русского языка

- 0,175	О 0,090	Е 0,072	А 0,062	И 0,062	Т 0,053	Н 0,053	С 0,045
Р 0,040	В 0,038	Л 0,035	К 0,028	М 0,026	Д 0,025	П 0,023	У 0,021
Я 0,018	Ы 0,016	З 0,016	Ь,Ъ 0,014	Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006	Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002

ДОМАШНЕЕ ЗАДАНИЕ

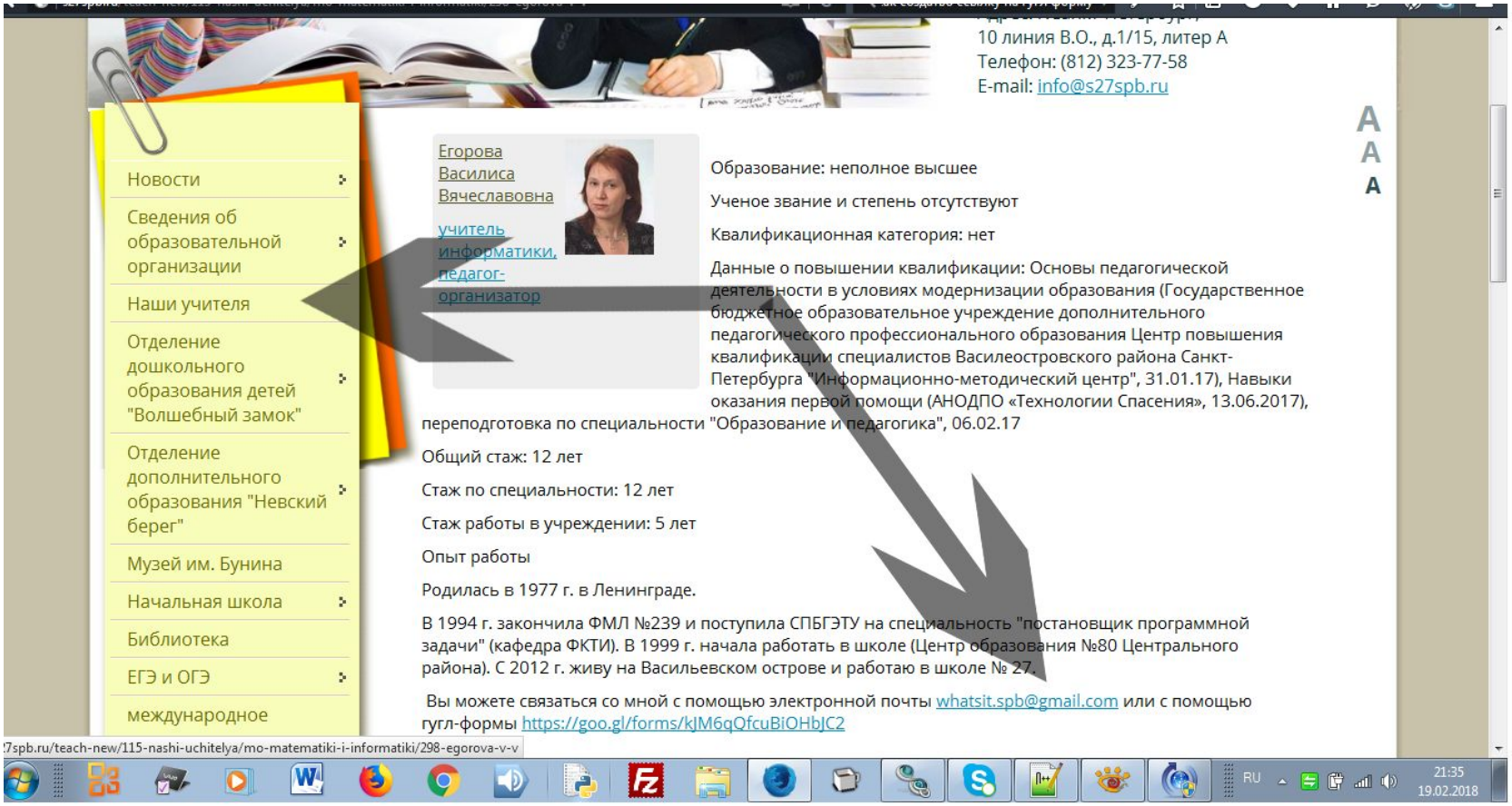
- Составьте блок-схему алгоритма: пользователь вводит с клавиатуры строку; программа выводит зашифрованную строку. Методы шифрования – на выбор: квадрат Полибия, скитала, шифр Цезаря
- Элементы блок-схем есть в учебнике на стр.25

Дополнительная литература

- Ru.wikipedia.org
- Фильм National Geografic “The Code Breakers”

- Саймон Сингх “**Книга шифров. Тайная история шифров и их расшифровки” М.: Астрель, 2007 г**

Если вы хотите задать вопрос – напишите мне письмо



Пожалуйста, оцените, насколько вам понравился урок

- 5
- 4
- 3
- 2
- 1
- 0