Развитие полиалфавитных шифров в эпоху Возрождения.

Шифр Виженера

Работу выполнил: Боревич Андрей Алексеевич, 5.3 класс;

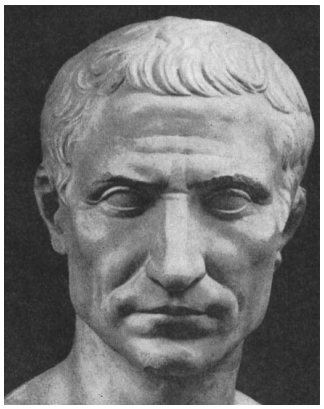
Руководители:
Боревич Алексей Альбертович,
Боревич Ирина Сергеевна,
Трофимова Светлана Николаевна

Санкт-Петербург
2014

Предмет исследования

Полиалфавитные шифры эпохи Возрождения

моноалфавитные шифры



Гай Юлий Цезарь

полиалфавитные шифры

Блез де Виженер

Цель работы

Изучение шифра Виженера, истории его создания и развития, структуры, для создания прикладной программы, реализующей его алгоритм.

История развития полиалфавитных шифров

Автор	Время	Результат	Недостатки
Леон Баттиста Альберти	1467 год	Предложил использовать два или более шифралфавита в одном сообщении.	Не было ключа. Алфавит сменялся через определённое число позиций.
Джованни Порта	1535- 1615 гг.	Усовершенствовал систему шифрования при помощи диска Альберти. Вплотную подошёл к идее взлома полиалфавитного шифра.	Не было ключа. Алфавит сменялся через определённое число позиций.
Иоганн Тритемий	1518 год	Изобрел tabula recta – первую таблицу для полиалфавитного шифрования.	Алфавиты переключались подряд, а не в определённой последовательности.

История развития полиалфавитных шифров (продолжение)

Автор	Время	Результат	Недостатки
Джованни Баттиста Беллазо	1553 год	Ввёл ключ для переключения между алфавитами.	Не смог продвинуть свою идею на государственном уровне.
Блез де Виженер	1586 год	Доработал систему и представил её королю Генриху III, а также изобрел модификации шифра.	

Шифр Виженера

Открытый текст:

если вы по коридору мчитесь

Ключ:

остер

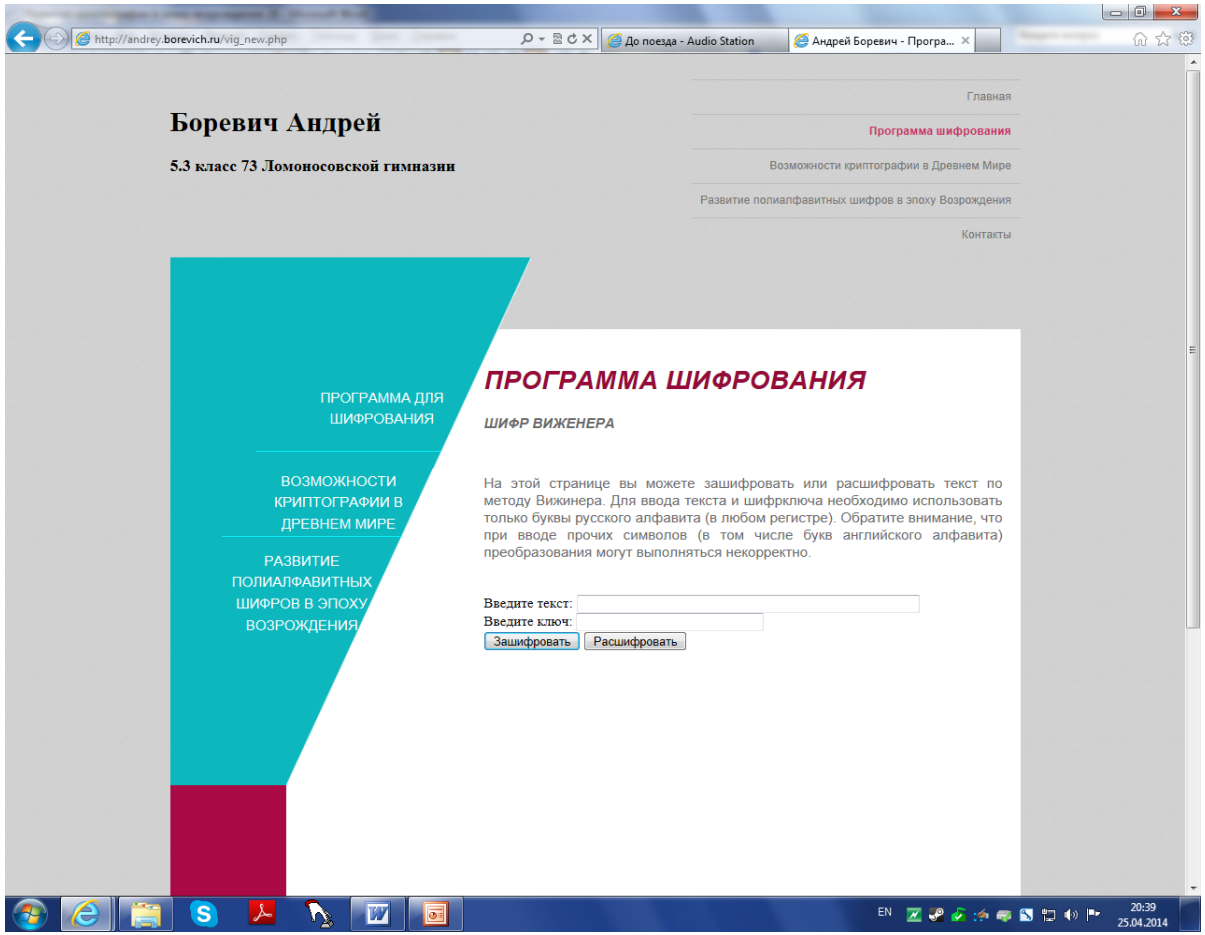
Шифртекст:

УГЮНТЙББПЯЯЪЦУБВЮЙНГУГО

Одинаковые буквы открытого текста становятся разными в шифртексте

	а	**б**	**в**	**…**	**о**	**…**	**я**
а	А	Б	В	…	О	…	Я
б	Б	В	Г	…	П	…	А
в	В	Г	Д	…	Р	…	Б
…	…	…	…	…	…	…	…
е	Е	Ё	Ж	…	У	…	Д
…	…	…	…	…	…	…	…
Я	Я	А	Б	…	Н	…	Ю

Прикладная программа (http://andrey.borevich.ru)



Взлом шифра Виженера

- На протяжении трёх веков шифр Виженера считался не взламываемым. В XIX веке, независимо друг от друга, Чарльз Беббидж и Фредерик Касиски изобрели метод взлома шифра Виженера.
- Метод основан на определении длины ключа. Если известна длина ключа, то зашифрованный текст можно разбить на фрагменты, каждый из которых кодируется с применением одного алфавита. К каждому фрагменту можно применить частотный криптоанализ.

Выводы

- Развитие метода частотного криптоанализа привело к появлению полиалфавитных шифров взамен моноалфавитных.
- Полиалфавитные шифры нельзя взломать методом частотного криптоанализа, который опирается на повторение символов, потому что в них одна и та же буква открытого текста шифруется по-разному.
- Методы взлома шифра Виженера основаны на нахождении длины ключа и были открыты в XIX веке, что позволило шифру на протяжении трёх веков считаться не взламываемым.
- Созданная программа шифрования по методу Виженера помогает шифровать быстрее и точнее, чем вручную с использованием квадрата Виженера. Все желающие могут воспользоваться ей на сайте http://andrey.borevich.ru.

Спасибо за внимание