ПРОЕКТИРОВАНИЕ ИС ШИФРОВАНИЯ ПОЛИАЛФАВИТНОЙ ОДНОКОНТУРНОЙ ЗАМЕНОЙ ВИЖЕНЕРА.

Выполнила
Студентка 451 группы
Абрамова Дарья

ОПИСАНИЕ

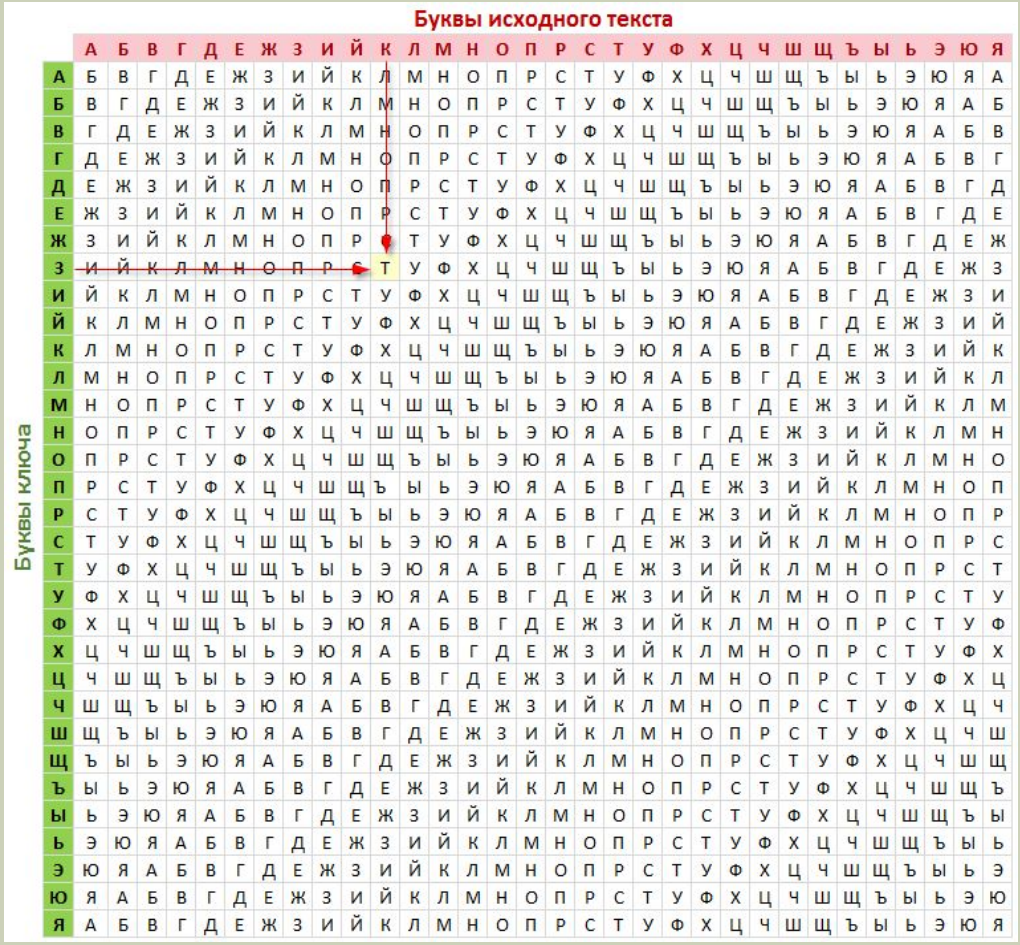
Шифр Виженера (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. *Giovan Battista Bellaso*) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата.

ИСТОРИЯ СОЗДАНИЯ

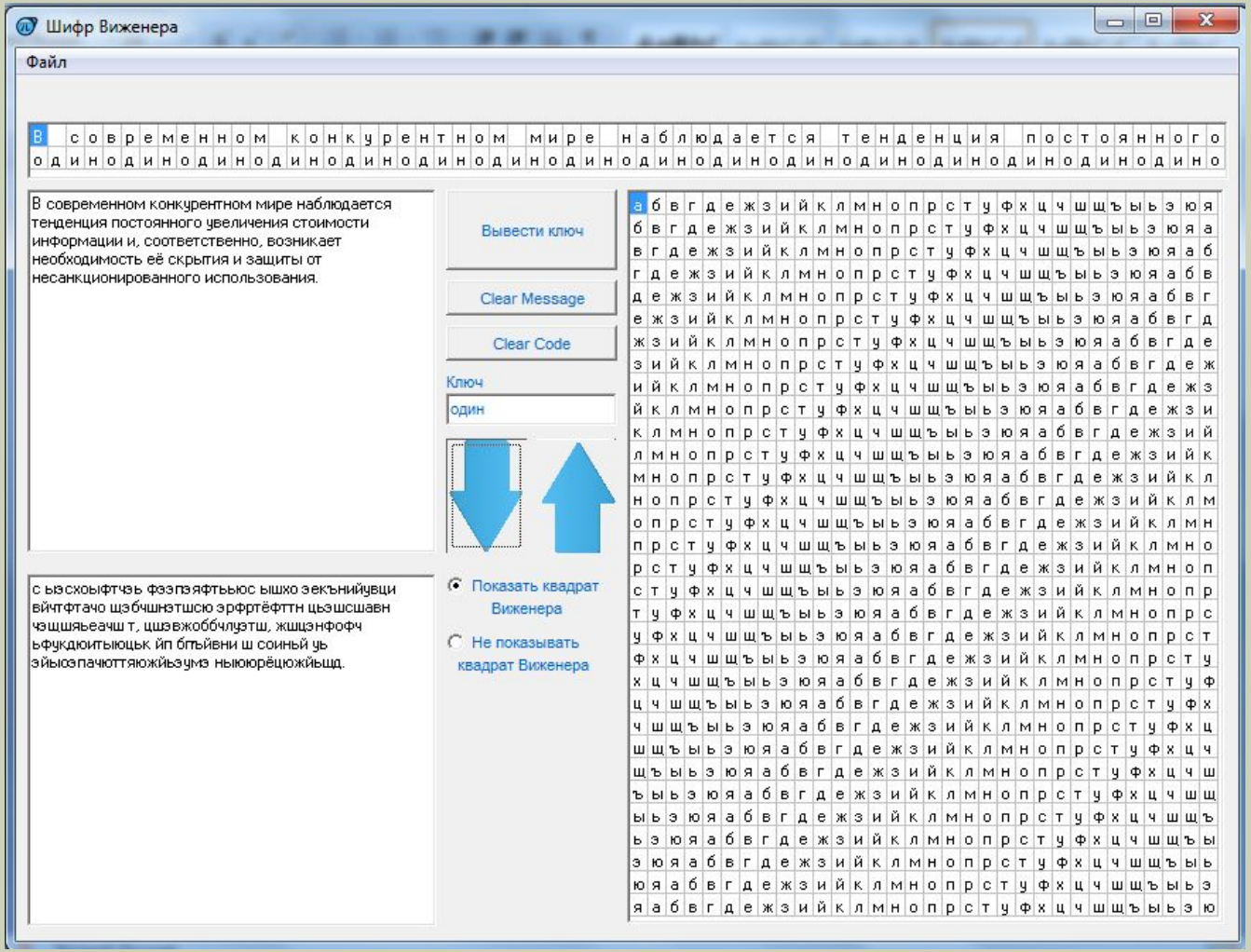
Первое точное документированное описание многоалфавитного шифра было сформулированно Леоном Баттиста АльбертиПервое точное документированное описание многоалфавитного шифра было сформулированно Леоном Баттиста Альберти в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, Иоганн Трисемус в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.

ПРИНЦИП ШИФРОВАНИЯ

1. Необходим текст, который нужно зашифровать
2. Придумывается ключевое слово, с помощью которого будет зашифрован текст
3. Буквы исходного текста берутся из горизонтального алфавита, а буквы ключевого слова из вертикального
4. На пересечении буквы исходного текста и буквы ключа находится та буква, в которую будет зашифрован исходный символ
5. Шифр повторяется циклически, пока весь исходный текст не будет зашифрован



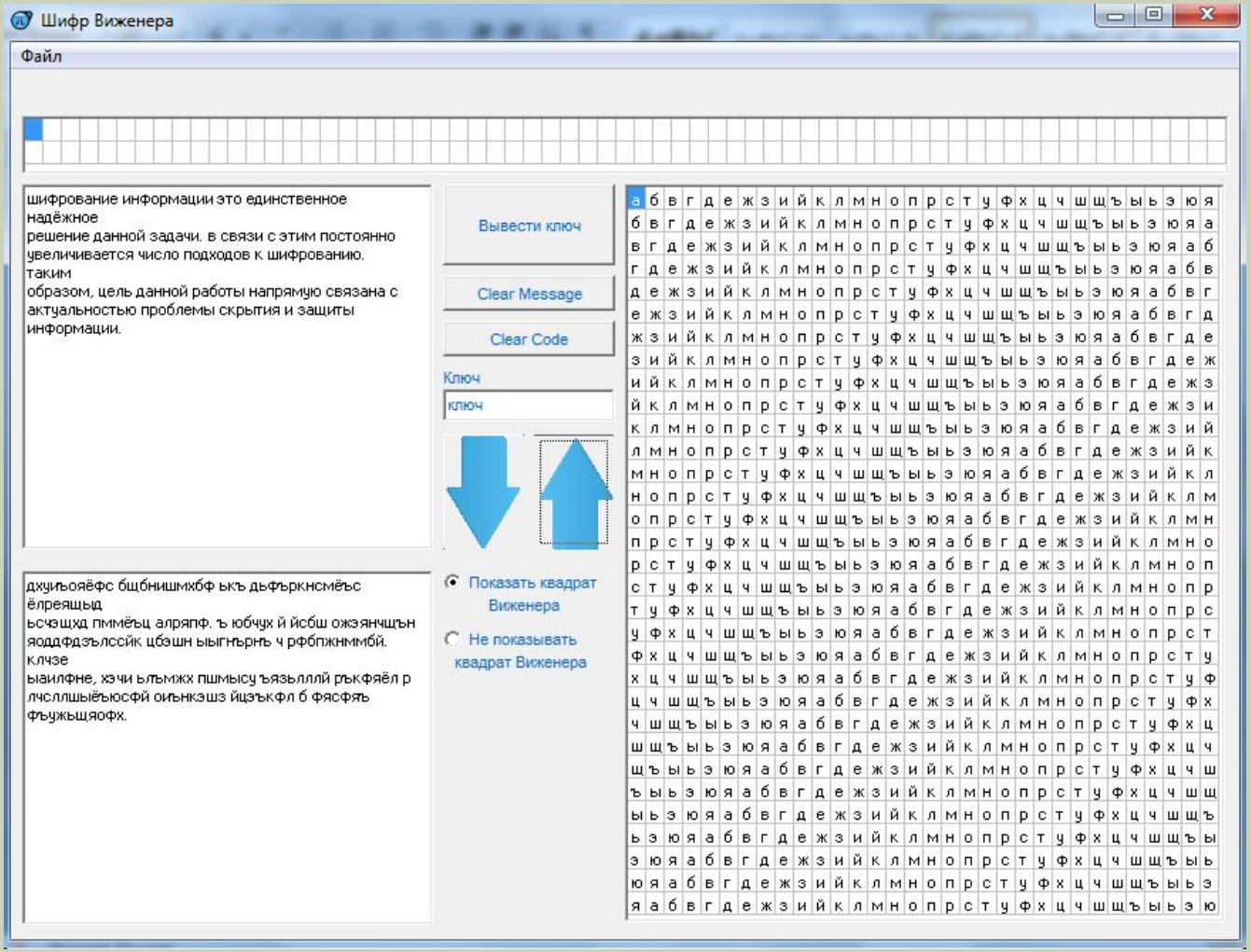
ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ШИФРОВАНИЯ



ДЕШИФРОВАНИЕ

- Расшифрование производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ДЕШИФРОВАНИЯ



Спасибо за внимание