Тема: Шифры сложной замены

Введение

Шифры сложной замены – шифры сложной замены отличаются от шифров простой замены тем, что в них при шифровании используется много алфавитов. Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты. Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита ***A*** может быть преобразован в несколько различных символов шифровальных алфавитов ***B***.

Шифр Гронсфельда

Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву, как это делается в шифре Цезаря, а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа.

Пример:

1) Зашифруем сообщение: ***совершенносекретно***;
2) Возьмём ключ: *314*;
3) Шифротекст: ***фпжисыиосстйнсйхот***;

Сообщение	С	О	В	Е	Р	Ш	Е	Н	Н	О	С	Е	К	Р	Е	Т	Н	О
Ключ	3	1	4	3	1	4	3	1	4	3	1	4	3	1	4	3	1	4
Шифротекст	Ф	П	Ж	И	С	Ы	И	О	С	С	Т	Й	Н	С	Й	Х	О	Т

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

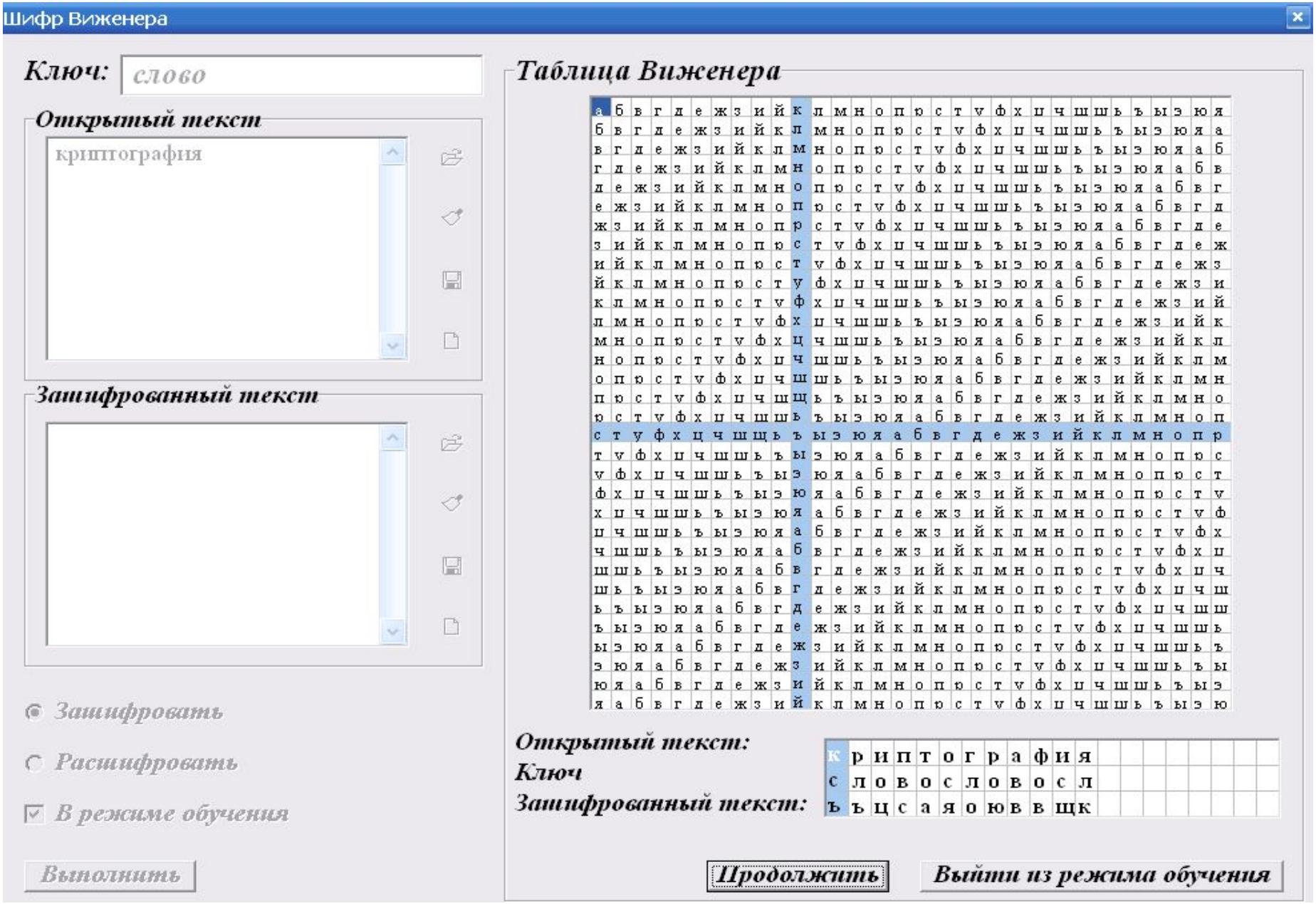
Шифр Виженера

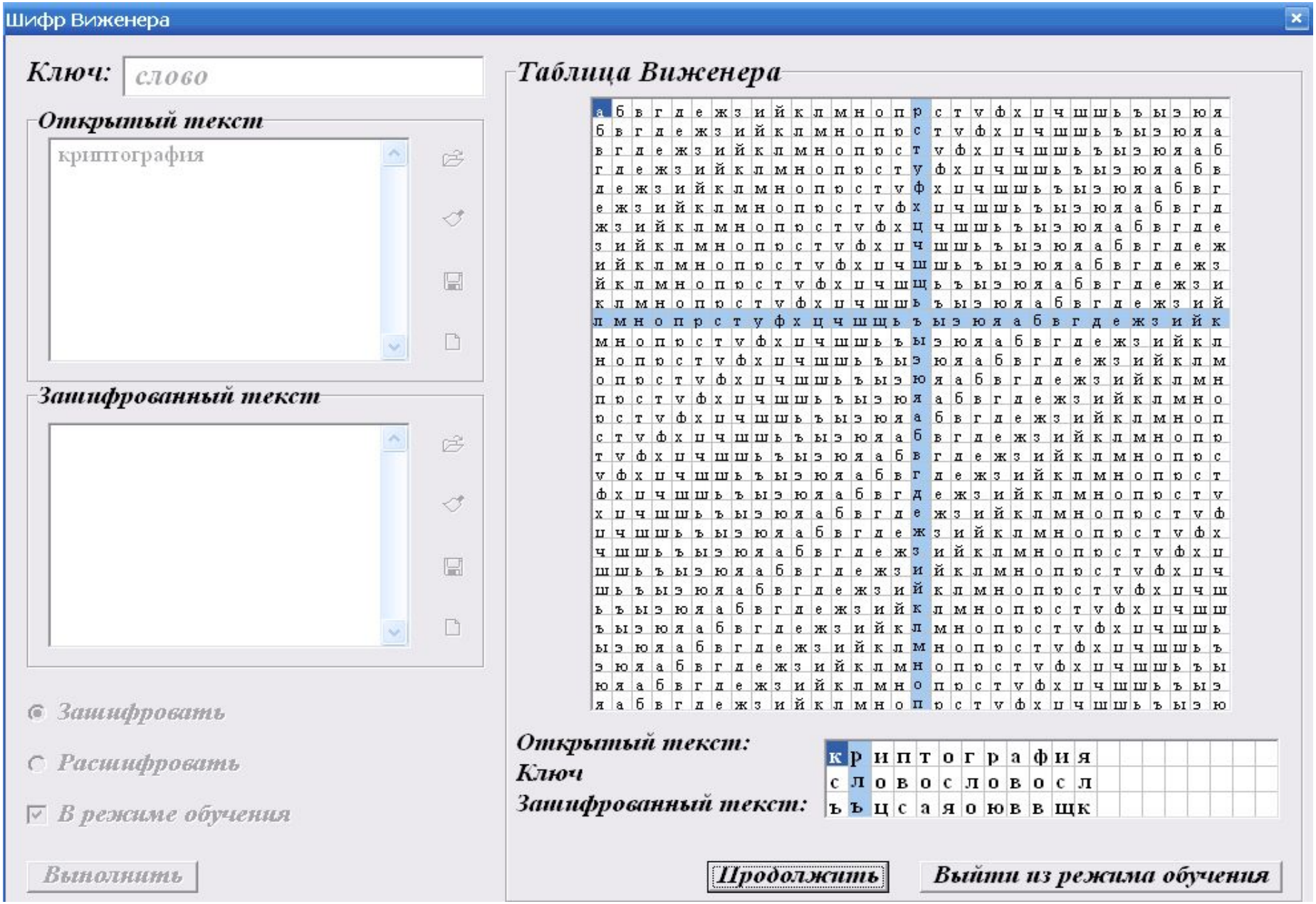
Система Виженера в первые была опубликована в 1586 году и является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI века Блеза Виженера, который развивал и совершенствовал криптографические системы. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая квадрат (таблица) Виженера. Применительно к русскому алфавиту таблица Виженера составляется из строк по 32 символа, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 32 различных шифра Цезаря. На разных этапах шифр Виженера использует различные алфавиты из этой таблицы. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

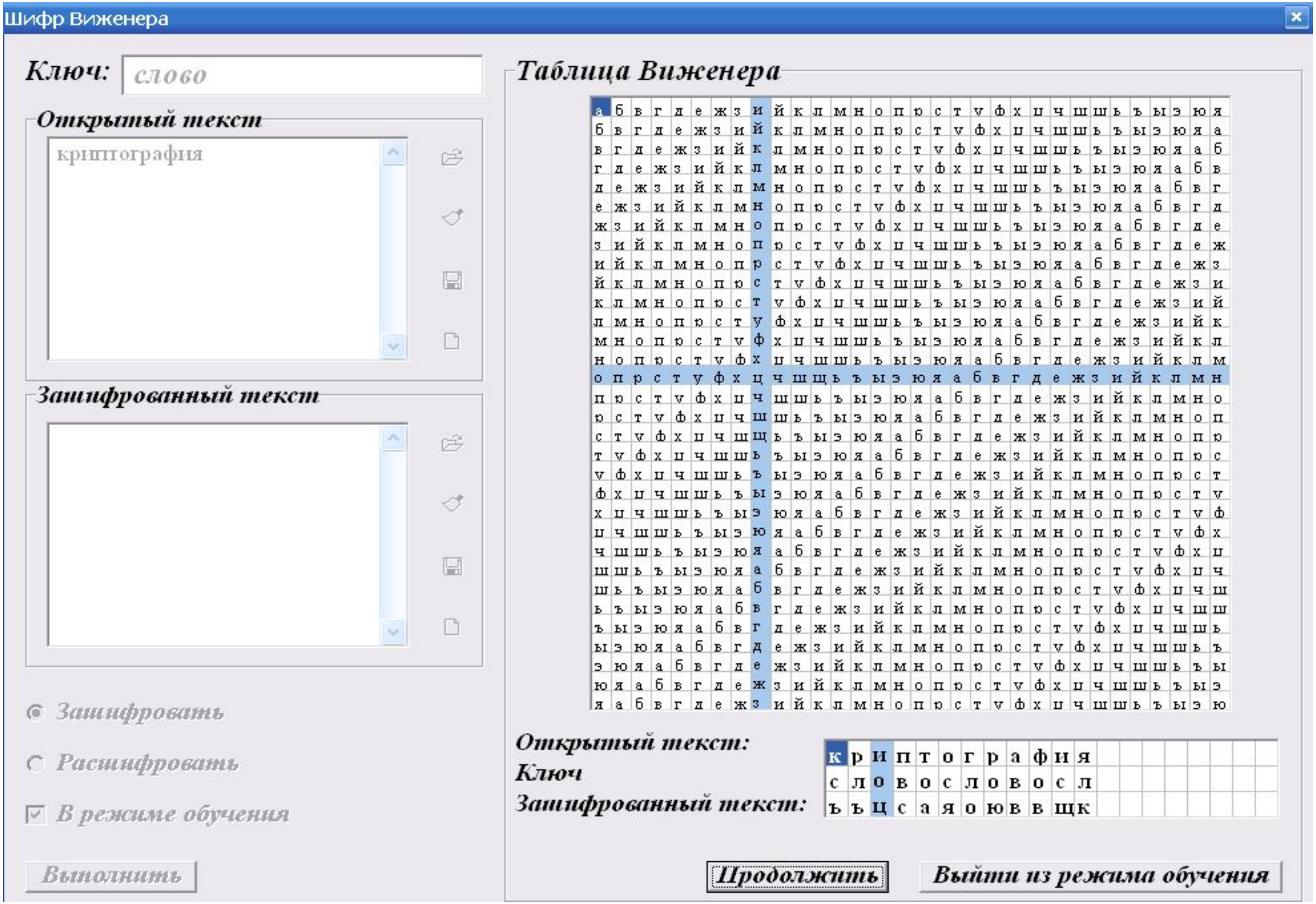
При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифротекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой буквой ключа.

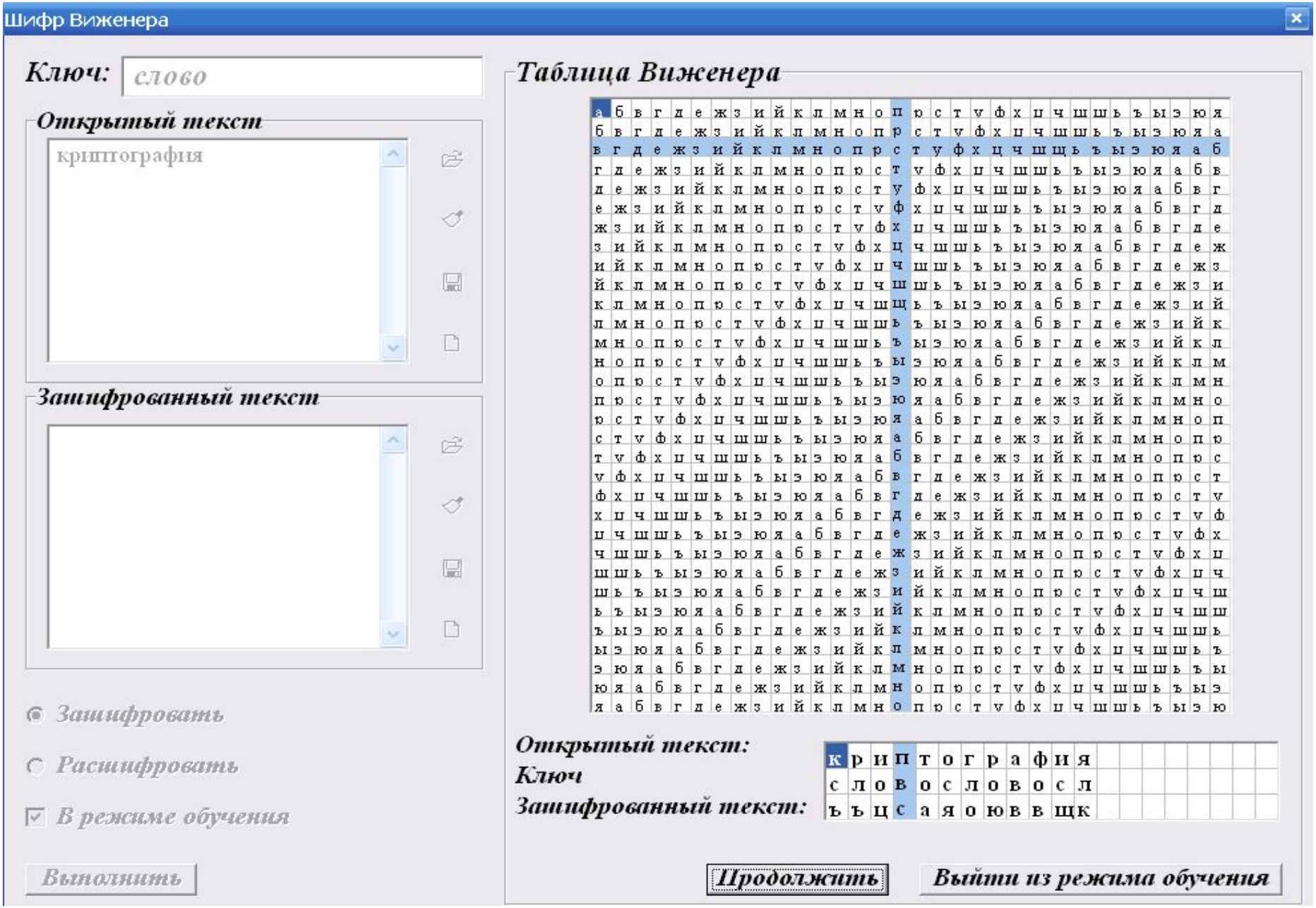
Пример:

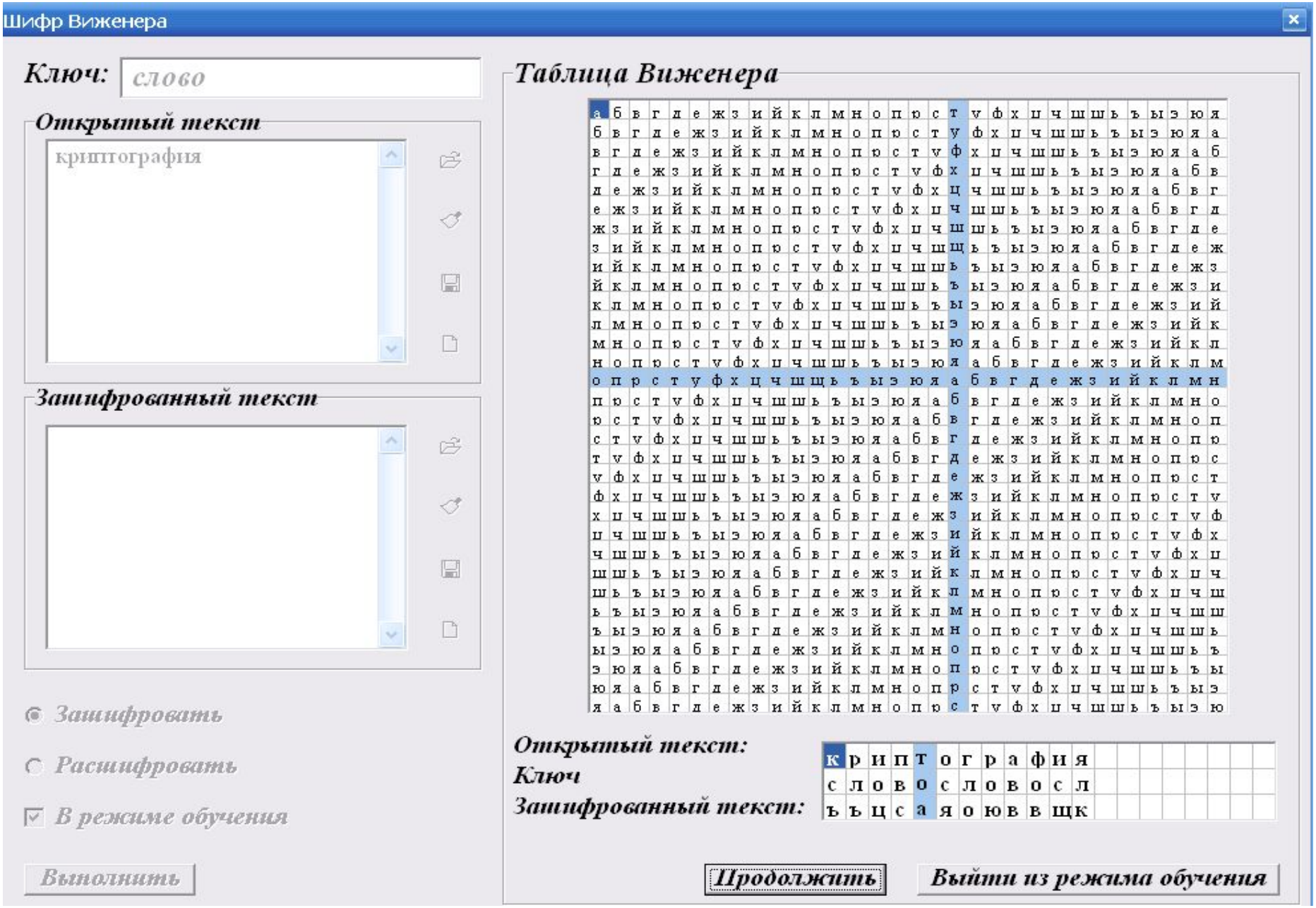
1) Зашифруем слово: ***криптография***;
2) Ключ: ***слово***;
3) Шифротекст: ***ъъцсаяоюввщк***.

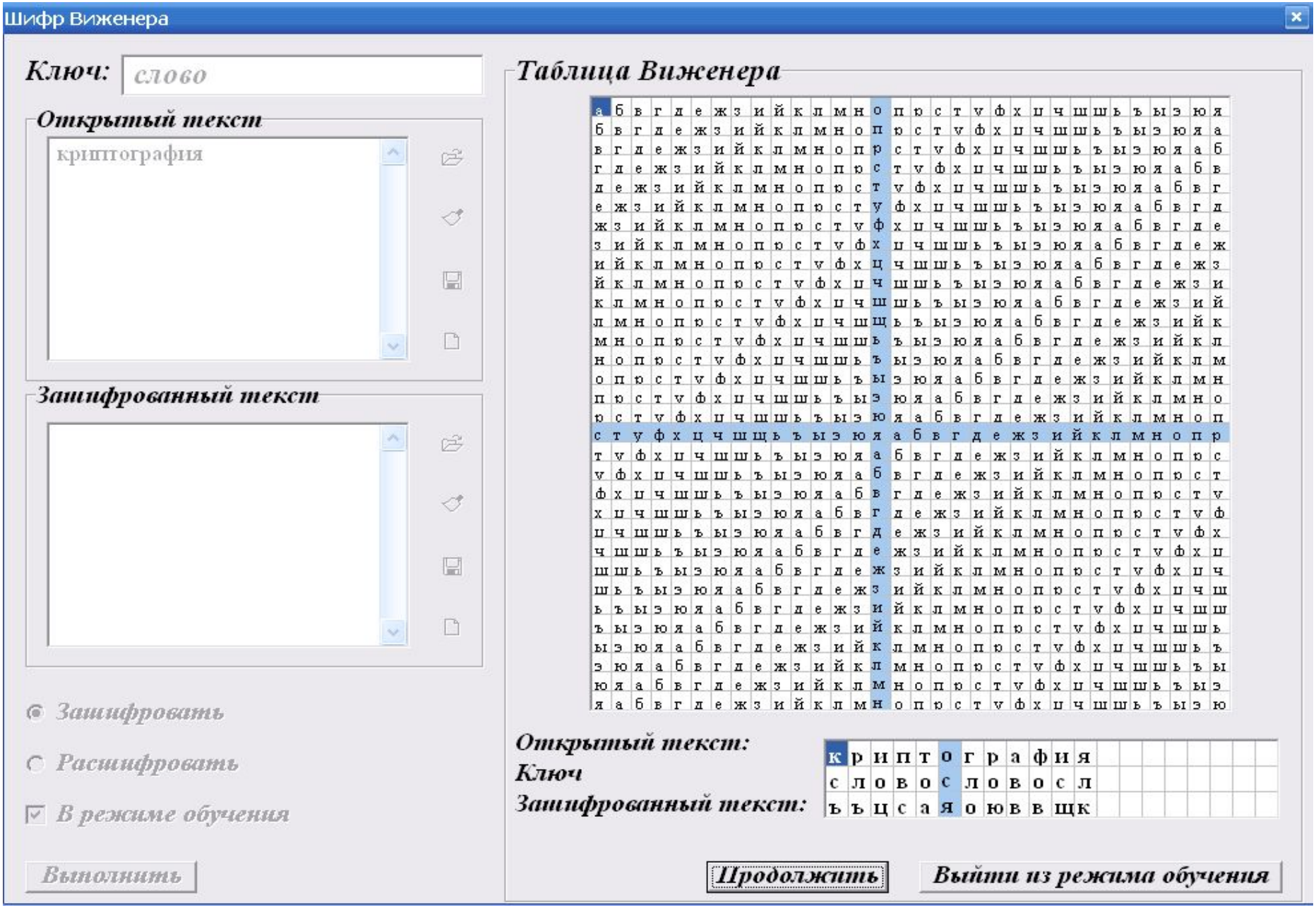

Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
криптография
словословосл
ъъцсаяоюввщк
Продолжить
Выйти из режима обучения


Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
к р и п т о г р а ф и я
с л о в о с л о в о с л
ъ ъ ц с а я о ю в в щ к
Продолжить
Выйти из режима обучения


Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
к р и п т о г р а ф и я
с л о в о с л о в о с л
ъ ъ ц с а я о ю в в щ к
Продолжить
Выйти из режима обучения


Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
к р и п т о г р а ф и я
с л о в о с л о в о с л
ъ ъ ц с а я о ю в в щ к
Продолжить
Выйти из режима обучения


Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
к р и п т о г р а ф и я
с л о в о с л о в о с л
ъ ъ ц с а я о ю в в щ к
Продолжить
Выйти из режима обучения


Шифр Виженера
Ключ:
слово
Открытый текст
криптография
Зашифрованный текст
Зашифровать
Расшифровать
В режиме обучения
Выполнить
Таблица Виженера
Открытый текст:
Ключ
Зашифрованный текст:
к р и п т о г р а ф и я
с л о в о с л о в о с л
ъ ъ ц с а я о ю в в щ к
Продолжить
Выйти из режима обучения

Одноразовая система шифрования «Одноразовый блокнот»

Почти все применяемые на практике шифры характеризуются как условно надежные, поскольку они могут быть в принципе раскрыты при наличии неограниченных вычислительных возможностей. Абсолютно надежные шифры нельзя разрушить даже при использовании неограниченных вычислительных возможностей. Существует единственный такой шифр, применяемый на практике, - одноразовая система шифрования «Одноразовый блокнот». Характерной особенностью одноразовой системы шифрования является одноразовое использование ключевой последовательности.

Одноразовая система шифрования «Одноразовый блокнот»

Одноразовая система изобретена в 1917 году американцами Дж. Моборном и Г. Вернамом. Для реализации этой системы подстановки иногда используют одноразовый блокнот. Этот блокнот составлен из Отрывных страниц, на каждой из которых напечатана таблица со Случайными числами (ключами) ***Ki***. Блокнот выполняется в двух экземплярах: один используется отправителем, а другой – получателем. Для каждого символа ***Xi*** сообщения используется свой Ключ ***Ki*** из таблицы только один раз. После того как таблица использована, она должна быть удалена из блокнота и уничтожена. Шифрование нового сообщения начинается с новой страницы. *Этот шифр абсолютно надежен*.

Недостатки одноразовой системы шифрования «Одноразовый блокнот»:

1) Последовательность должна быть действительно случайной. В противном случае у криптоаналитика есть материал для атаки.
2) Ключ может использоваться только один раз, и он должен быть такой же длинны, как и открытый текст.
3) Ключ должен передаваться заранее по секретному каналу.

Пример:

1) Зашифруем сообщение: ***совершенносекретно***.
2) Сформируем ключ случайным образом сами, либо с помощью генератора случайных чисел. Каждой букве будет соответствовать число от [1, 31];

Ключ: 11,2,28,6,19,12,18,29,21,15,1,3,27,13,3,1,30,25.

3) Шифротекст: ***ьрюлгдчквэтиеэиулз***.

Сообщение	С	О	В	Е	Р	Ш	Е	Н	Н	О	С	Е	К	Р	Е	Т	Н	О
Ключ	**11**	**2**	**28**	**6**	**19**	**12**	**18**	**29**	**21**	**15**	**1**	**3**	**27**	**13**	**3**	**1**	**30**	**25**
Шифротекст	Ь	Р	Ю	Л	Г	Д	Ч	К	В	Э	Т	И	Е	Э	И	У	Л	З

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
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**

Недостатки одноразовой системы шифрования «Одноразовый блокнот»:

1) Последовательность должна быть действительно случайной. В противном случае у криптоаналитика есть материал для атаки.
2) Ключ может использоваться только один раз, и он должен быть такой же длинны, как и открытый текст.
3) Ключ должен передаваться заранее по секретному каналу.