

# **Инструкция пользователя**

## **приложением программной реализации шифра Бэкона в режиме отрицаемого шифрования (двухлитерное кодирование)**

Выполнил: Студент группы М22-512 Ветушинский И.С.





Преподаватель: Иванов М.А.

### **Оглавление**

Запуск	2
Зашифрование сообщения	2
Расшифрование сообщения	4
Получение ложного сообщения	5

## Запуск

Для запуска приложения с пользовательским интерфейсом дважды кликнуть на ярлык под названием “Run\_Bacon.bat”:

 bacon.py	17.01.2023 0:25	Python File	4 КБ
 bacon_qt.py	17.01.2023 0:13	Python File	17 КБ
 Run_Bacon.bat	16.01.2023 0:07	Пакетный файл ...	1 КБ
 words.txt	15.01.2023 19:57	Текстовый докум...	5 205 КБ

Откроется окно с приложением:

Программная реализация шифра Бэкона в режиме отрицаемого шифрования

	BinCode	Key		BinCode	Key
A	<input type="text"/>	<input type="text"/>	N	<input type="text"/>	<input type="text"/>
B	<input type="text"/>	<input type="text"/>	O	<input type="text"/>	<input type="text"/>
C	<input type="text"/>	<input type="text"/>	P	<input type="text"/>	<input type="text"/>
D	<input type="text"/>	<input type="text"/>	Q	<input type="text"/>	<input type="text"/>
E	<input type="text"/>	<input type="text"/>	R	<input type="text"/>	<input type="text"/>
F	<input type="text"/>	<input type="text"/>	S	<input type="text"/>	<input type="text"/>
G	<input type="text"/>	<input type="text"/>	T	<input type="text"/>	<input type="text"/>
H	<input type="text"/>	<input type="text"/>	U	<input type="text"/>	<input type="text"/>
I	<input type="text"/>	<input type="text"/>	V	<input type="text"/>	<input type="text"/>
J	<input type="text"/>	<input type="text"/>	W	<input type="text"/>	<input type="text"/>
K	<input type="text"/>	<input type="text"/>	X	<input type="text"/>	<input type="text"/>
L	<input type="text"/>	<input type="text"/>	Y	<input type="text"/>	<input type="text"/>
M	<input type="text"/>	<input type="text"/>	Z	<input type="text"/>	<input type="text"/>

Исх. текст

Шифртекст

Шифртекст

Исх. текст

Лож. текст

Лож. шифр

Шифртекст

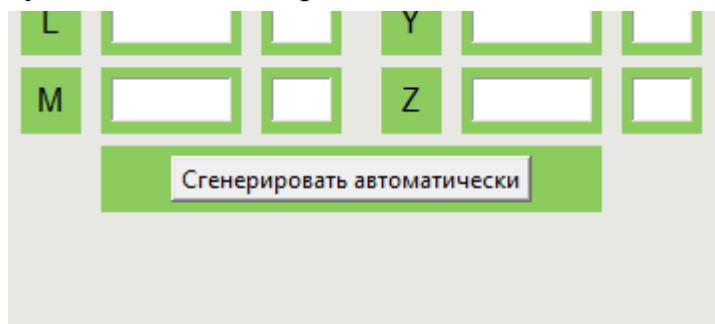
	FK		FK
A	<input type="text"/>	N	<input type="text"/>
B	<input type="text"/>	O	<input type="text"/>
C	<input type="text"/>	P	<input type="text"/>
D	<input type="text"/>	Q	<input type="text"/>
E	<input type="text"/>	R	<input type="text"/>
F	<input type="text"/>	S	<input type="text"/>
G	<input type="text"/>	T	<input type="text"/>
H	<input type="text"/>	U	<input type="text"/>
I	<input type="text"/>	V	<input type="text"/>
J	<input type="text"/>	W	<input type="text"/>
K	<input type="text"/>	X	<input type="text"/>
L	<input type="text"/>	Y	<input type="text"/>
M	<input type="text"/>	Z	<input type="text"/>

## Зашифрование сообщения

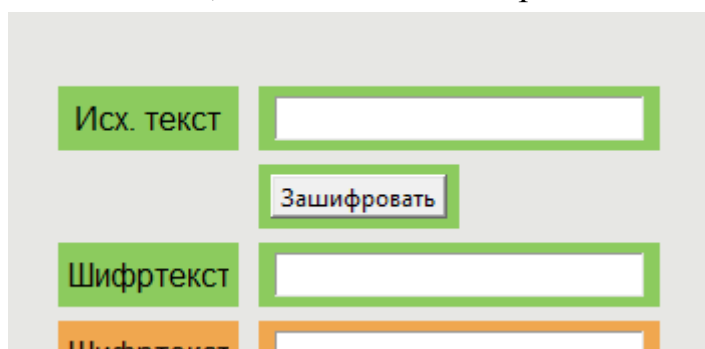
Для того, чтобы зашифровать сообщение, необходимо задать ключевую информацию. Для этого нужно заполнить ячейки, находящиеся слева, зеленого цвета. В первом столбце задается ключ для первого шага зашифрования как двухлитерный пятиразрядный код (например 01011) для символов A-M английского алфавита, во втором столбце для тех же символов задается ключ, необходимый для второго шага зашифрования, в

виде двухсимвольного двухлитерного кода (0 или 1). В третьем и четвертом столбцах все аналогично, но только для символов N-Z.

Чтобы сгенерировать ключевую информацию псевдослучайно и автоматически, нужно нажать на кнопку “Сгенерировать автоматически”, находящуюся внизу под этими четырьмя столбцами:



После того, как ключевая информация заполнена, необходимо заполнить поля зеленого цвета, находящиеся посередине окна сверху:



В поле “Исх. текст” нужно вставить текст, который нужно зашифровать. Формат текста - заглавные английские буквы без пробелов и знаков препинания.

После того как все готово, нажать кнопку “Зашифровать”.

В поле “Шифртекст” будет выведен зашифрованный исходный текст.

Окно с приложением будет выглядеть похожим образом:

Программная реализация шифра Бэкона в режиме отрицательного шифрования

	BinCode	Key		BinCode	Key
A	10111	0	N	00111	1
B	01001	0	O	01100	1
C	01111	0	P	11000	1
D	10110	0	Q	01010	1
E	11001	0	R	00100	1
F	00000	0	S	10001	1
G	00011	0	T	10100	1
H	00110	0	U	01110	1
I	00001	0	V	10000	1
J	01101	0	W	00010	1
K	10011	0	X	01011	1
L	10101	0	Y	10010	1
M	01000	0	Z	00101	1

Сгенерировать автоматически

Исх. текст:

Зашифровать

Шифртекст:

Шифртекст:

Расшифровать

Исх. текст:

Сгенерировать ложный текст

Лож. текст:

Лож. шифр:

Шифртекст:

	FK		FK
A		N	
B		O	
C		P	
D		Q	
E		R	
F		S	
G		T	
H		U	
I		V	
J		W	
K		X	
L		Y	
M		Z	

## Расшифрование сообщения

Для расшифрования сообщения, необходимо также выполнить действия по заполнению полей с ключевой информацией.

После этого ввести зашифрованное сообщение в поле “Шифртекст” оранжевого цвета в формате, что допускаются только английские буквы в верхнем регистре без пробелов и знаков препинания. Текст должен быть длиной, кратной 5.

После выполнения этих действий нужно нажать на кнопку “Расшифровать”. В поле “Исх. текст” будет выведен расшифрованный текст.

Программная реализация шифра Бэкона в режиме отрицаемого шифрования

	BinCode	Key		BinCode	Key
A	10111	0	N	00111	1
B	01001	0	O	01100	1
C	01111	0	P	11000	1
D	10110	0	Q	01010	1
E	11001	0	R	00100	1
F	00000	0	S	10001	1
G	00011	0	T	10100	1
H	00110	0	U	01110	1
I	00001	0	V	10000	1
J	01101	0	W	00010	1
K	10011	0	X	01011	1
L	10101	0	Y	10010	1
M	01000	0	Z	00101	1

Исх. текст: WATER

Зашифровать

Шифртекст: JDAWBYCPZXSBUQBQ

Шифртекст: JDAWBYCPZXSBUQBQ

Расшифровать

Исх. текст: WATER

Сгенерировать ложный текст

Лож. текст:

Лож. шифр:

Шифртекст:

Сгенерировать автоматически

	FK		FK
A		N	
B		O	
C		P	
D		Q	
E		R	
F		S	
G		T	
H		U	
I		V	
J		W	
K		X	
L		Y	
M		Z	

## Получение ложного сообщения

Для получения ложного сообщения путем использования отрицаемого шифрования предусмотрено два способа:

### Способ 1)

Для наглядности зашифровать какое-нибудь сообщение с исходной ключевой информацией.

Затем ввести новый ключ для создания ложного сообщения, заранее известный пользователю, во 2 и 4 столбцы, как это рассматривалось ранее.

В поле для расшифрования (оранжевого цвета) ввести зашифрованное сообщение и нажать кнопку “Расшифровать”. Полученное в оранжевом поле “Исх. текст” сообщение будет являться ложным текстом для заданного ранее нового ключа.

В данном способе необходимо, чтобы ключ из 2 и 4 столбцов не приводил к ситуации несоответствия ключу из 1 и 3 столбцов, когда при переводе шифртекста в двухлитерный код не получались 5-разрядные последовательности, по модулю большие 25.

Программная реализация шифра Бэкона в режиме отрицательного шифрования

	BinCode	Key		BinCode	Key
A	10111	1	N	00111	0
B	01001	0	O	01100	1
C	01111	0	P	11000	1
D	10110	0	Q	01010	1
E	11001	0	R	00100	1
F	00000	0	S	10001	1
G	00011	0	T	10100	1
H	00110	1	U	01110	0
I	00001	0	V	10000	1
J	01101	0	W	00010	1
K	10011	0	X	01011	1
L	10101	0	Y	10010	1
M	01000	0	Z	00101	1

Исх. текст: WATER

Зашифровать

Шифртекст: JDAWBYCPZXSBUQBQ1

Шифртекст: JDAWBYCPZXSBUQBQ1

Расшифровать

Исх. текст: HAVEH

Сгенерировать ложный текст

Лож. текст:

Лож. шифр:

Шифртекст:

Сгенерировать автоматически

	FK		FK
A		N	
B		O	
C		P	
D		Q	
E		R	
F		S	
G		T	
H		U	
I		V	
J		W	
K		X	
L		Y	
M		Z	

## Способ 2)

В отличие от способа 1 пользователю не нужно иметь ключа для получения ложного сообщения. Приложение произведет поиск слова и выведет соответствующий ему ключ.

Для начала ключевая информация слева также должна быть заполнена.

Далее нужно зашифровать какое-нибудь сообщение и получить его шифртекст.

После этого достаточно нажать на кнопку “Сгенерировать ложный текст” красного цвета.

В поле “Лож. текст” появится осмысленный ложный текст, соответствующий исходному шифртексту и исходному тексту.

В столбцах справа появится соответствующий ложному тексту сгенерированный ключ.

В поле “Лож. шифр” появится результат первого шага расшифрования исходного шифртекста для исходного сообщения (двухлитерный код), чтобы при желании проверить полученный результат.

В поле “Шифртекст” появится исходный шифртекст, который теперь соответствует и ложному тексту.

	BinCode	Key		BinCode	Key
A	10001	0	N	00111	1
B	10010	0	O	10101	1
C	00001	0	P	01000	1
D	10011	0	Q	01001	1
E	01101	0	R	01100	1
F	00010	0	S	00101	1
G	11001	0	T	00100	1
H	10100	0	U	00011	1
I	10111	0	V	01010	1
J	01110	0	W	01011	1
K	10110	0	X	00110	1
L	01111	0	Y	00000	1
M	11000	0	Z	10000	1

Сгенерировать автоматически

Исх. текст: RABBIT

Зашифровать

Шифртекст: IYNHFZIGKOOHCTCYKD

Шифртекст:

Расшифровать

Исх. текст:

Сгенерировать ложный текст

Лож. текст: LAMBDA

Лож. шифр: 01111100011100010010

Шифртекст: IYNHFZIGKOOHCTCYKD

	FK		FK
A	0	N	1
B	1	O	1
C	1	P	0
D	1	Q	0
E	1	R	0
F	1	S	1
G	0	T	0
H	0	U	1
I	1	V	1
J	0	W	0
K	0	X	1
L	0	Y	1
M	1	Z	1

При повторном нажатии на кнопку “Сгенерировать ложный текст” будет получен новый ложный текст для исходного шифртекста и соответствующий ему ключ:

	BinCode	Key		BinCode	Key
A	10001	0	N	00111	1
B	10010	0	O	10101	1
C	00001	0	P	01000	1
D	10011	0	Q	01001	1
E	01101	0	R	01100	1
F	00010	0	S	00101	1
G	11001	0	T	00100	1
H	10100	0	U	00011	1
I	10111	0	V	01010	1
J	01110	0	W	01011	1
K	10110	0	X	00110	1
L	01111	0	Y	00000	1
M	11000	0	Z	10000	1

Сгенерировать автоматически

Исх. текст: RABBIT

Зашифровать

Шифртекст: IYNHFZIGKOOHCTCYKD

Шифртекст:

Расшифровать

Исх. текст:

Сгенерировать ложный текст

Лож. текст: SCOFFS

Лож. шифр: 00101000011010100010

Шифртекст: IYNHFZIGKOOHCTCYKD

	FK		FK
A	0	N	0
B	0	O	1
C	1	P	0
D	0	Q	1
E	1	R	0
F	0	S	0
G	0	T	0
H	0	U	0
I	1	V	0
J	1	W	0
K	0	X	1
L	0	Y	1
M	1	Z	0