<HTML>

<HEAD>

<BODY>

<div> ШИФРОВЩИК </div>

<SCRIPT LANGUAGE="JavaScript">

function crypter(message, key, decrypter) {

var a = "абвгдежзийклмнопрстуфхцчшщъыьэюя".split("");

message = message.split("") ;

key = ("" + key).split("") ;

return message.reduce(function(message, current) {

var i = a.indexOf(current),

b = +key.shift();

key.push(b);

decrypter ? (i -= b, i < 0 && (i += a.length)) : (i += b, i %= a.length);

return message + a[i]

}, "")

};

document.write(crypter("аааааа", 22)+"<br>")

</script>

<div> ДЕШИФРОВЩИК </div>

<SCRIPT LANGUAGE="JavaScript">

function crypter(message, key, decrypter) {

var a = "абвгдежзийклмнопрстуфхцчшщъыьэюя".split("");

message = message.split("") ;

key = ("" + key).split("") ;

return message.reduce(function(message, current) {

var i = a.indexOf(current),

b = +key.shift();

key.push(b);

decrypter ? (i -= b, i < 0 && (i += a.length)) : (i += b, i %= a.length);

return message + a[i]

}, "")

};

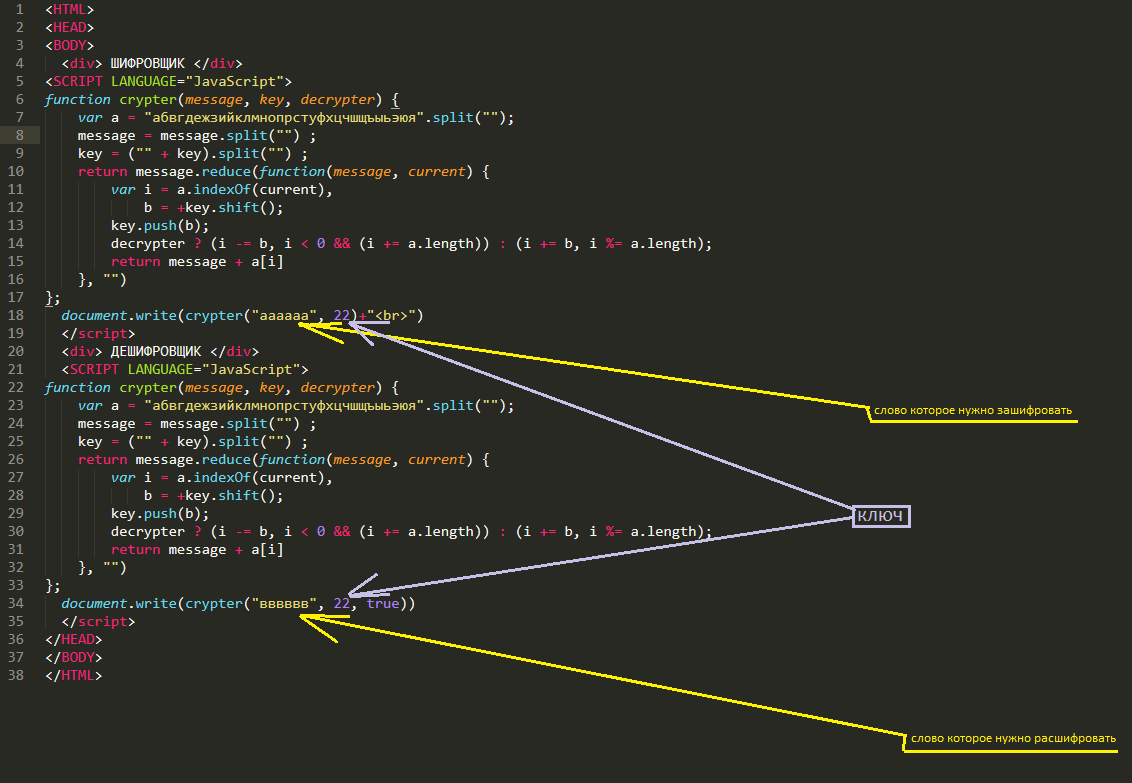
document.write(crypter("вввввв", 22, true))

</script>

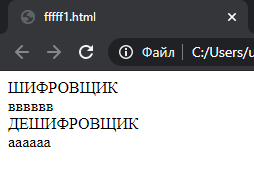
</HEAD>

</BODY>

</HTML>



Результат:



**Контрольные вопросы**

1 Что такое криптографическое преобразование информации?

Это преобразование информации основанное на определенном алгоритме, зависящего от определенного параметра, и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной

2 Что понимается под шифрованием, расшифрованием и дешифрованием данных?

Шифрование это изменение информации для того что бы сделать ее недоступной для просмотра без ключа или другого способа расшифровки.

Дешифрование это процесс расшифровки зашифрованной информации.

3 Дайте определения ключа и алгоритма шифрования?

Ключ шифрования это секретная информация, используемая для шифрования информации.

Алгоритм шифрования это инструкция или набор правил, с помощью которых шифруют и расшифровывают информацию.

4 Расскажите о криптографическом методе перестановки?

метод перестановки-это метод, шифрования при котором символы в сообщение переставляются по определенному алгоритму, чтобы смысл сообщения не был понятен

5 В чем суть криптографического метода замены?

Методы замены основан на том, что символы начального текста, которые обычно разделяют на блоки и записывают в одном алфавите, заменяются одним или несколькими символами из другого алфавита в соответствии с правилом преобразования, которое было принято ранее.

6 Какие методы шифрования Вы знаете? Назовите их достоинства и недостатки.

*Шифры замены.* Этот метод относится к классическим, и на практике дает ненадежную степень защиты сообщения. Вторым недостатком является то, что при кодировании пробелы между словами сохраняются на своих местах, что также повышает возможность взлома.

Есть рандомизированная версия, которая дает большое увеличение качества шифрования по сравнению с предыдущей версией, которая использует простой постоянный сдвиг

*Шифры перестановок* На практике, этот метод очень сложный, так как при раскодировке сообщения всегда нужно иметь набор цилиндры разных диаметров и продолжать попытки до тех пор, пока не будет получен читаемый текст.

Можно получить компьютеризованную версию, если поместить сообщение в массив одним способом, а затем переписать его другим способом.

*Шифры битовых манипуляций* Ониприменимы только к компьютерным файлам и не могут использоваться для бумажных копий зашифрованных сообщений

Из достоинств то, что они подходят для использования в компьютерной криптографии, потому что используют операции, которые легко выполняются системой. Вторая причина это полученный на выходе зашифрованный текст выглядит абсолютно нечитаемым — фактически полной бессмыслицей.

7 Назовите принципы, лежащие в основе известных Вам методах шифрования.

Основной принцип методов шифрования- это зашифровать сообщение по определенному алгоритму.  
так к примеру шифр Виженера использует тот же принцип, что и шифр Цезаря, за тем исключением, что каждая буква меняется в соответствии с кодом, а шифр перестановок основан на принципе переставления символов по определенному алгоритму.