1. Сохранит ли текст, зашифрованный с помощью метода перестановки свои статистические свойства (например, частоты повторения отдельных символов)?

**Да, так как он переставляет только буквы**

1. Приведите пример двойной табличной перестановки.

В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.



1. Можно ли выполнить сжатие информации с помощью рассмотренных методов шифрования моноалфавитной/многоалфавитной замены и перестановок?

**Нет, нельзя, количество символов сохраняется**

4. При каком свойстве исходного текста в его зашифрованном варианте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть?

При перестановке любого вида в зашифрованное сообщение будут входить те же символы, что и в открытый текст, но в другом порядке. Следовательно, статистические закономерности языка останутся без изменения. Это дает криптоаналитику возможность использовать различные методы для восстановления правильного порядка символов. Если у противника есть возможность пропускать через систему шифрования методом перестановки специально подобранные сообщения, то он сможет организовать атаку по выбранному тексту. Так, если длина блока в исходном тексте равна N символам, то для раскрытия ключа достаточно пропустить через шифровальную систему N-1 блоков исходного текста, в которых все символы, кроме одного, одинаковы. Другой вариант атаки по выбранному тексту возможен в случае, если длина блока N меньше количества символов в алфавите. В этом случае можно сформировать одно специальное сообщение из разных букв алфавита, расположив их, например, по порядку следования в алфавите. Пропустив подготовленное таким образом сообщение через шифровальную систему, специалисту по криптоанализу останется только посмотреть, на каких позициях очутились символы алфавита после шифрования, и составить схему перестановки.

[ССЫЛКА НА ХОСТИНГ С РЕАЛИЗАЦИЕЙ](https://ma4ypic4y.github.io/)