1. Основная идея криптографических преобразований на основе шифров перестановки заключается в изменении порядка символов в сообщении без их изменения. Это достигается путем перемещения символов в тексте в соответствии с определенным ключом или правилом.

2. Классификационные признаки перестановочных шифров могут включать в себя:

- Количество и тип ключей: некоторые перестановочные шифры могут использовать один ключ, в то время как другие могут использовать несколько ключей или даже не требовать ключа вовсе.

- Способ перестановки: различные шифры могут применять разные методы перестановки символов, такие как маршрутная перестановка, столбцовая перестановка и т. д.

- Размер блока: некоторые шифры могут работать с блоками фиксированного размера, в то время как другие могут иметь переменный размер блока.

- Сложность шифрования и дешифрования: разные шифры могут иметь различные уровни сложности для шифрования и дешифрования.

3. Для алфавитов русского и белорусского языков можно составить по 32 разновидности шифров, подобных шифру Цезаря, так как оба алфавита содержат 32 буквы.

4. Перестановочные шифры могут обладать различной стойкостью к криптоанализу. Некоторые из них могут быть уязвимы к статистическим атакам из-за сохранения частоты символов, в то время как другие могут быть более стойкими, особенно если используются дополнительные методы, такие как добавление шума или использование ключей переменной длины.

5. Примеры перестановочных шифров, не рассмотренных в материалах:

- Шифр Рейндель

- Шифр Скитала

- Шифр Виженера (в том числе его вариации)

6. Выбор размеров используемой таблицы для перестановочных шифров может зависеть от конкретного алгоритма шифрования и требований к криптографической стойкости. В некоторых случаях предпочтительно использовать квадратные таблицы, а в других - прямоугольные.

7. Основные методы взлома перестановочных шифров включают в себя:

- Атаки по статистике: использование частотного анализа для определения перестановки символов.

- Атаки по известному тексту: если известен какой-то часть зашифрованного текста, можно использовать эту информацию для определения ключа или расшифровки других частей текста.

- Атаки перебором: попытка всех возможных комбинаций ключей для нахождения правильного.

- Другие методы криптоанализа, такие как анализ частот биграмм и триграмм, атаки с использованием известных уязвимостей конкретных алгоритмов и т. д.