1) В чем осн. идея криптографическиз преобразований на основе шифров перестановки?  
исх. текст (M) и зашифрованный текст (C) основаны на исп-нии одного и того же алфавита, а тайной явл. алгоритм перестановки (в подстановки алф мб разным)

2) Привести классиф. признаки и дать сравн. характеристику разновидностям перестан.шифров  
1) \* простой пер. (символы Mi перемещ. в новые поз)  
 - в обр. посл-сти  
 - в обр. посл-сти парами букв  
 - простой блочной перест  
 - маршрутной пер (простой, спираль, змейка, зигзаг)  
 - верт. перест  
\* сложной пер. (символы Mi перем. в новые неск раз)  
 - 2 кс, перест солбцы, потом строки  
2) блочные и поточные

3) Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языка?  
если повтор. букв в Mi длиной n символов всего сущ. n! неповтор. ключей

4) Охаректеризовать криптостойкость перестановочных и подстановочных шифров.

5) Привести примеры дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной л/р  
\* с пом решеток: 4 квадрата повор на 90\* и совмещ в 1, вырез клетки с числами 1-k2, наклад. на исх текст и поворач, продолж. вписывать

6) Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?  
лучше выбирать, чтобы длина х ширина = кол-во символов откр. текста  
чтобы длина == ширина

7) Охаректеризовать основные методы взлома перестановочных шифров  
перебор всех значений, частотный анализ по комбинациям 2-3