1. Криптографию и криптоанализ объединяют в одну науку – криптологию
2. Криптография решает следующие задачи: шифрование данных с целью защиты от несанкционированного доступа; проверка подлинности сообщений; проверка целостности передаваемых данных; обеспечение невозможности отказа.
3. Криптографические алгоритмы представляют собой алгоритмы шифрования/дешифрования, кэширования, формирования и проверки электронной цифровой подписи.
4. К криптографическим системам предьявляют следующие требования:

* зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
* знание алгоритма шифрования не должно влиять на надежность защиты;
* любой ключ из множества возможных должен обеспечивать надежную защиту информации;
* алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

1. При использовании метода перестановки сообщение делится на блоки, которые переставляют на другие позиции. А метод замены заменяет символы по алфавиты на другие.
2. При многоалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно циклически
3. Простейшим примером перестановки является перестановка с фиксированным периодом . В этом методе сообщение делится на блоки по определенному количеству символов и в каждом блоке производится одна и та же перестановка*.*
4. Метод гаммирования подразумевает создание гаммы т.е набора случайных чисел полученных различными методами гаммирования. Далее с гаммой проводятся арифметические операции.
5. При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов.
6. Важнейшим показателем надежности криптографического закрытия информации является его стойкость
7. Трудоемкость метода - определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста
8. Маршрутные перестановки основываются на некоторой геометрической фигуре. Отрезок открытого текста записывается в такую фигуру по некоторой траектории.
9. Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера 2m´2k клеток. В трафарете вырезано m´k клеток так, что при наложении его на лист чистой бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа
10. Шифры сложной замены – шифры сложной замены отличаются от шифров простой замены тем, что в них при шифровании используется много алфавитов.
11. Шифр Гронсфельда