**Тема Симметричные криптосистемы**

1. Раздел науки, объединяющий криптографию и криптоанализ называется криптологией
2. Защита конфиденциальности, проверка целостности и подлинности, обеспечение отказоустойчивости.
3. Криптографический алгоритм – алгоритм, по которому шифруется и дешифруется сообщение.
4. Надежность шифрования, приемлемая стоимость, не возможность подобрать ключ, не ограниченность по количеству и типу символов, минимальная избыточность при шифровке.
5. Метод замены меняет один символ на другой, а метод перестановки меняет символы местами.
6. Последовательная замена символов на символы из алфавита.
7. Перестановка символов и групп символов между собой в файле
8. Символы файла последовательно складываются с символами определённой последовательноси, называемой гаммой.
9. Гораздо эффективнее шифровать сообщение комбинируя метода шифрования. Таким образом выявление криптографического алгоритма и подбор ключа становятся практически не возможными.
10. Важнейшим показателем надежности криптографического закрытия является не возможность дешифровки файла без ключа.
11. Трудоёмкость определяется по числу операций при шифровании сообщения.
12. Перестановка, когда файл записывается по одной траектории, а считывается по другой.
13. Вид ключа для метода перестановки. При применении его к массиву с символами, после поворота символы извлекаемые из массива меняются.
14. –
15. Шифры простой замены используют один алфавит, или же ключ, а в сложных используется несколько.
16. Метод Альбеди, метод Виженера, шифр Тритемия, Шифр Гронсфельда,