Криптография – это наука, которая занимается исследованием математических методов и преобразованием информации.

Наряду с криптографией развивается криптоанализ – наука о преодолении криптографической защиты информации.

Криптография + криптоанализ = криптология.

Криптология занимается вопросами обратимого преобразования информации с целью её защиты от несанкционированного доступа, оценкой надежности систем шифрования и анализом стойкости шифров.

Принято считать, что криптография предназначена решать следующие задачи:

1. Шифрование данных с целью защиты от несанкционированного доступа
2. Проверка подлинности сообщений, а точнее проверка подлинности источника
3. Проверка целостности передаваемых данных
4. Обеспечение невозможности отказа от факта передачи как для отправителя, так и для получателя

Основные понятия и определения криптографии

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием или выработкой имитов вставки.

Имитовставка представляет собой последовательность данных фиксированной длины, которая получается по определенному правилу из открытых данных и ключа.

Шифрование – это процесс зашифрования и расшифрования данных.

Защифрование – это процес…

Расшифрование – это процесс преобразования закрытых данных с помощью шифра.

Шифр – это совокупность обратимых преобразований множества открытых данных в множество зашифрованных данных заданных алгоритмом криптографических преобразований.

Ключ – это конкретное секретное состояние некоторых параметров алгоритма криптографических преобразований, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма.

Данные, подлежащие зашифрования и расшифрованию представляют собой текст, построенные на некотором алфавите.

Алфавит – это конечное множество используемых для кодирования информации символов.

Символ — это любой знак в том числе буква, цифра или знаки препинания.

Текст – упорядоченный набор из элементов алфавита.

При выполнении лабораторных работ будет использоваться алфавит, содержащий 31 букву русского алфавита (без й и ё) и знак нижнего подчеркивания (вместо пробела).

Каждый символ алфавита будет иметь свой код: нижнее подчеркивание – 00, а – 01, … я – 31.

Двоичный код символов лабораторного алфавита будет 5 разряда.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию.

Дешифрование – это попытка получить открытый текст из шифра текста без знания ключа.

…

В настоящее время существует несколько классификаций криптоалгоритмов.

Наиболее известной является классификация, которая подразделяет криптоалгоритмы в зависимости от числа применяемых ключей.

Согласно этой классификации все криптоалгоритмы подразделяются на 3 группы:

* Бесключевые (которые не используют в вычислениях никаких ключей)
* Одноключевые, которые используют один секретный ключ как для зашифрования так и для расшифрования
* Двухключевые, которые для зашифрования и расшифрования используют 2 разных ключа: секретный и открытый.

Типы криптоалгоритмов:

К бесключевым криптоалгоритмам относится хеширование, которое представляет собой контрольное преобразование информации.

…когда из данных неограниченного размера путем криптографических преобразований вычисляется хэш – значение фиксированной длины, однозначно соответствующее исходным данным.

….

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины, при это даже в различных режимах работы одного криптоалгоритма, как пример алгоритмы DEATH.

Блоки могут шифроваться как независимо друг от друга, так и со сцеплением, когда результат шифрования текущего блока зависит либо от значения предыдущего блока, либо от результата шифрования предыдущего блока.   
В этом случае для шифрования первого блока необходима синхропосылка.

Потоковое шифрование применяется, когда информацию невозможно разбить на блоки, а каждый символ требуется зашифровать и отправить, не дожидаясь остальных данных.

В том случае, когда блоки данных зашифровываются отдельно, одинаковые блоки открытого текста переводятся в одинаковые блоки шифра текста.

Блочные шифры принято разделять на простейшие и коммерческие. К простейшим блочным шифрам относятся: шифры подстановки, шифры перестановки, шифры гаммирования.

Шифр текста зависит только от предыдущего состояния шифратора и не зависит от входного текста, поэтому каждый символ, искажённый в процессе передачи, приводит к проявлению только одного ошибочно расшифрованного символа, но потеря символа при передаче приведет к потере (срыву) синхронизации и весь текст следующий за потерянным символом будет расшифрован неправильно.

В системах с самосинхроницаией потеря символа шифра текста при передаче приведет к появлению фиксированного числа ошибок в расшифрованном тексте, после чего синхронизация будет восстановлена и текст будет расшифровываться правильно.

При конструировании блочных шифров стараются сделать так, чтобы изменение даже 1-го бита открытого текста или ключа приводило бы к изменению примерно 50% битов шифра текста.

Такого рода размножения ошибки оказывается полезным для обеспечения криптостойкости.

**Симметричные криптосистемы ( заголовок след. Лекции)**