ЗИСОПД
Лекция

Шифрование. Основные понятия и определения

Шифрование — обратимое преобразование информации в целях сокрытия от сторонних (неавторизованных) лиц, с предоставлением, в это же время, авторизованным легитимным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Криптография — наука о методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). *Традиционная криптография* образует раздел *симметричных криптосистем*, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. *Помимо* этого раздела современная криптография включает в себя *асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, квантовую криптографию*.

Открытый (исходный) текст — данные (не обязательно текстовые), передаваемые без использования криптографии.
Шифротекст — данные, полученные после применения криптосистемы.
Ключ — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра целиком определяется секретностью ключа (Принцип Керкгоффса).
Шифр, криптосистема — семейство обратимых преобразований открытого текста в шифрованный.
Шифрование — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.
Расшифровывание — процесс нормального применения криптографического преобразования шифрованного текста в открытый.
Асимметричный шифр — шифр, в котором используются два ключа, шифрующий и дешифрующий.
Криптоанализ — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
Криптоаналитик — человек, создающий и применяющий методы криптоанализа.
Криптография и криптоанализ составляют ***криптологию***, как единую науку о создании и взломе шифров.
Дешифрование — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста.
Криптографическая стойкость — способность криптографического алгоритма противостоять криптоанализу.
Центр сертификации — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.
Квантовая криптография — метод защиты коммуникаций, основанный на принципах квантовой физики. Сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи

электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определённых параметров физических объектов — переносчиков информации. А попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Методы шифрования делятся, в зависимости от структуры используемых ключей, на *симметричные методы и асимметричные методы*. Кроме того, методы шифрования могут обладать *различной криптостойкостью* и по-разному обрабатывать входные данные — *блочные* шифры и *поточные* шифры.