Глоссарий

Аппаратный шифр	Шифр, реализованный в виде электронного устройства
Атака	Попытка противника раскрыть шифр
Аутентификация	Установление подлинности источника сообщения
Блочный шифр	Шифр для зашифрования блоков данных фиксированного размера
Вероятностное шифрование	Шифрование с использованием случайных параметров
Гибкий шифр	Набор криптоалгоритмов, выбираемых в зависимости от секретного ключа
Гибридная криптосистема	Криптосистема, в которой распределение ключей осуществляется с помощью двухключевой системы, а зашифрование – с помощью одноключевой
Двухключевая криптография	Криптосистема с двумя ключами: один для зашифрования, другой для расшифрования, причем вычисление любого из этих ключей при условии, что известен другой ключ, возможно ввиду биективности отображений зашифрования/расшифрования, но представляет вычислительно трудную задачу
Зашифрование	Преобразование информации для её защиты от несанкционированного доступа
Имитозащита	Защита от навязывания ложных сообщений путем передачи небольшой дополнительной информации (контрольной суммы)
Имитовставка	Криптографическая контрольная сумма
Ключ	Секретный параметр, управляющий процессом шифрования
Криптоанализ	Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа по исходному тексту и и соответствующему шифртексту
Криптоаналитик противника	Субъект, пытающийся вычислить исходный текст по шифртексту без знания ключа или вычислить ключ по исходному тексту и соответствующему шифртексту
Криптографическое преобразование	Процедура шифрования данных или для решения других криптографических задач
Криптографический примитив	криптографическая операция (алгоритм) = составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов
Криптографический протокол	Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов
Криптосистема с закрытым ключом	Криптосистема с одним секретным ключом, известным двум или более пользователям
Криптостойкость	Способность криптосистемы выдерживать различные атаки
Лавинный эффект	Свойство криптосистемы к размножению ошибок
Лобовая атака	Криптоанализ путем перебора всех возможных ключей
Поточный шифр	Программный шифр, последовательно преобразующий биты или знаки исходного текста

Программный шифр	Шифр, реализованный в виде программы
Протокол рукопожатия	Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета
Расшифрование	Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу
Раскрытие (взлом) шифра	Нахождение решения криптографической задачи за разумное время при использовании современных вычислительных средств
Симметричная криптосистема	Криптосистема с закрытым ключом
Слепая подпись	Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению)
Стеганография	Способ скрытной передачи данных, способ формирования скрытного канала связи
Управление ключами	Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей
Управляемые операции	Операции, выбираемые в зависимости от управляющего кода
Хеширование	Вычисление значения хеш-функции
Хеш-функция	Функция, вычисляющая сжатый образ фиксированной длины для сообщения произвольной длины
Цифровая подпись	Электронная цифровая подпись
Шифр с открытым ключом	Двухключевая криптосистема
Шифр	Совокупность алгоритмов зашифрования и расшифрования
Шифрование	Преобразование информации под управлением ключа
Шифратор	Электронное устройство или программа, осуществляющие шифрование информации
Электронная цифровая подпись	Дополнительная информация, которая может быть сформирована только владельцем, обладающим некоторым секретом