Тема реферата:

«Криптографическая защита информации»

Цель работы:

Раскрыть понятие криптографической системы, описать и понять принцип ее действия

Выбранная тема актуальна, так как популярность всемирной сети Интернет в последние годы способствует удваиванию информации каждый год. В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития, и монопольное обладание определенной информацией оказывается зачастую преимуществом в конкурентной борьбе. Фактически, на пороге нового тысячелетия человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит благополучие и даже выживание человечества. Однако сегодня существует опасность того, что конфиденциальная информация может быть прочитана совершенно посторонними людьми. Для защиты информации создаются различные методы. Одним из них является криптография.

Общее понятие криптографии.

Криптография – это набор методов защиты информационных взаимодействий от отклонений от их нормального, штатного протекания, вызванных злоумышленными действиями различных субъектов, методов, базирующихся на секретных алгоритмах преобразования информации.

Общее понятие криптографии.

Первая задача криптографии - защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, что нашло отражение в самом названии этой дисциплины. Эта защита используется на использовании «секретного языка», известного только лишь отправителю и получателю.

Из истории появления криптографии.

1976 год - начало эры открытой криптографии.

Открытая криптография — область криптографии, в которой алгоритмы шифрования, электронной цифровой подписи, формирования ключей, аутентификации, хеширования открыты и доступны для анализа всем желающим, и используются двухключевые алгоритмы с парой ключей — личным и публичным.

Из истории появления криптографии.

В 1976г. У.Диффи и М.Хеллманом было предложено использование односторонней криптографической функции.

W. Diffie, M. Hellman,
"New directions in cryptography"

$$f(x) = ax \pmod{p}$$

Принципы действия криптографии. Методологии.

Симметричная (секретная) методология. В этой методологии и для шифрования и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия.

Асимметричная (открытая) методология. В ней ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится втайне. Данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом.

Принципы действия криптографии. Алгоритмы.

Симметричные алгоритмы. Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей. Используют два разных ключа – один известен всем, а другой держится в тайне.

Квантовая криптография. Основное понятие.

Один из надежных способов сохранить в тайне телефонные переговоры или передаваемую по компьютерным сетям связи информацию – это использование *квантовой криптографии.*

В основе лежит идея использовать для целей защиты информации природу объектов микромира – квантов света (фотонов),

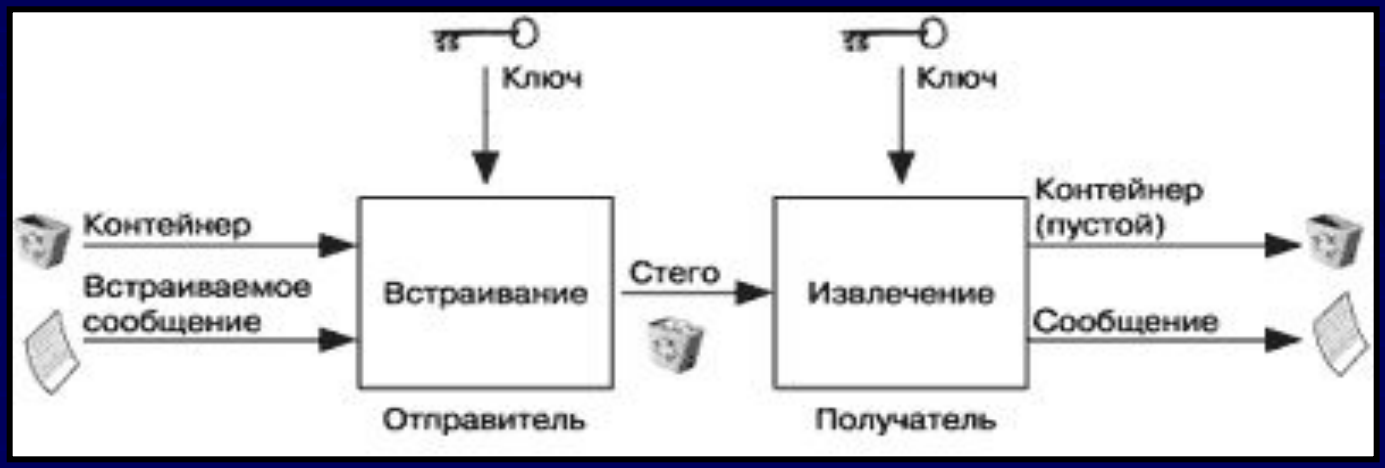
Квантовая криптография. Принципы действия.

В 1984 году Ч. Беннетт (фирма IBM) и Ж. Брассард (Монреальский университет) предложили простую схему защищенного квантового распределения ключей шифрования. Эта схема использует квантовый канал, по которому два пользователя обмениваются сообщениями, передавая их в виде

Стеганография.

Стеганография - это метод организации связи, который скрывает само наличие связи. Слово "стеганография" в переводе с греческого буквально означает "тайнопись" (steganos - секрет, тайна; graphy - запись).

Обобщенная модель стеганографии.



- ***Контейнер*** - любая информация, предназначенная для сокрытия тайных сообщений.
- ***Пустой контейнер*** - контейнер без встроенного сообщения.
- ***Заполненный контейнер или стего – контейнер —*** содержащит встроенную информацию.
- ***Встроенное (скрытое) сообщение*** -, сообщение, встраиваемое в контейнер.
- ***Стеганографический канал или просто стегоканал*** - канал передачи стего.
- ***Стегоключ или просто ключ*** - секретный ключ необходимый для сокрытия информации

Благодарю за внимание!