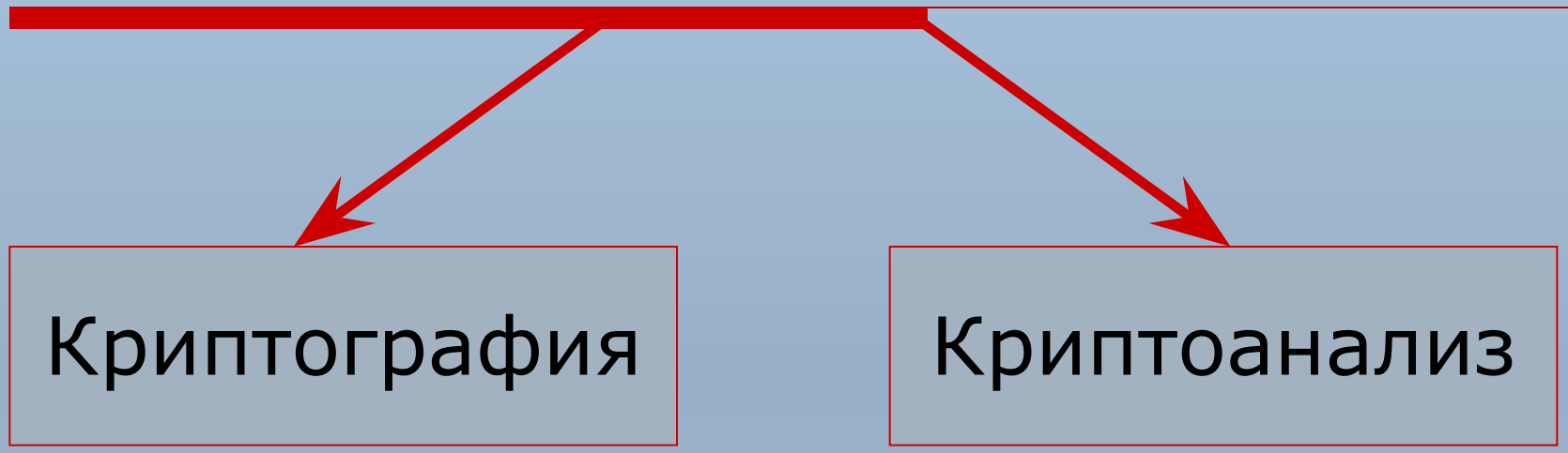
Криптография и криптоанализ

Выполнила студентка
группы И411
Суркова В.М.

Криптология



Основные термины

- Шифрование - такое преобразование информации, которое делает исходные данные нечитаемыми и трудно раскрываемыми без знания ключа.
- Ключ - секретная информация, определяющая, какое преобразование из множества возможных шифрующих преобразований выполняется в данном случае над открытым текстом.
- Вскрытие (взломом) шифра - процесс получения криптоаналитиками открытого сообщения из шифрованного сообщения без заранее известного ключа называется.

Электронная торговля

Под этим термином понимается:

- банковские операции, управление счетами и совершение покупок, а также некоторые другие действия, осуществляемые с помощью интернета (например, заказ авиабилетов, бронирование мест в гостиницах, вызов такси, перевод денег с одного счета на другой и т.д.).

защита ценной информации

защита всего сеанса связи

Сертификация

- схема, когда доверенные лица (например, центр сертификации) ручаются перед пользователями за неизвестных тем субъектов.

установление личности (идентификация)

установление подлинности (аутентификация)

Доступ к ресурсам

Повышенный уровень безопасности обеспечивают встроенные в различные продукты криптографические методы защиты дистанционного доступа.

Восстановление ключа

Технология восстановления ключа позволяет при некоторых обстоятельствах раскрыть ключ без участия его владельца

Криптоанализ

- *Атака со знанием лишь шифрованного текста (ciphertext-only attack)* – ничего не известно о содержании сообщения, есть только шифрованный текст;
- *Атака со знанием содержимого шифровки (known-plaintext attack)* – известна или угадываема часть сообщения;
- *Атака с заданным текстом (chosen-plaintext attack)* – есть возможность получения шифрованного документа для любого текста.

- *Атака с подставкой (Man-in-the-middle attack)* – направление на обмен шифрованными сообщениями;
- *Атака с помощью таймера (timing attack)* - последовательное измерение времен, затрачиваемых на выполнение операции возведения в стенень по модулю целого числа.

Спасибо за внимание!