ХАРАКТЕР И ИСТОРИЯ КРИПТОГРАФИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ. КОМПОЗИЦИИ, МОДЕЛИ И СИНТЕЗ ШИФРОВ.

Борисов В.А.
КАСК – филиал ФГБОУ ВПО РАНХ и ГС
Красноармейск 2011 г.

криптографической деятельности

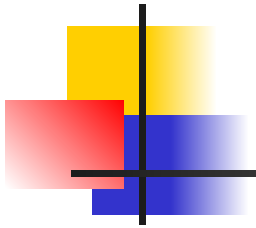
История криптографической деятельности

Криптографические методы

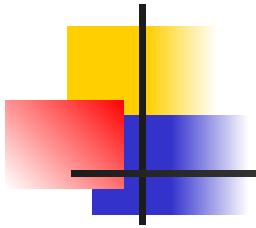
- Являются специфическим способом зашиты процессов переработки информации.

Криптология

- Наука, изучающая и разрабатывающая научно-методологические основы, способы, методы и средства криптографического преобразования информации.



Основные понятия, определения, композиции и синтез шифров



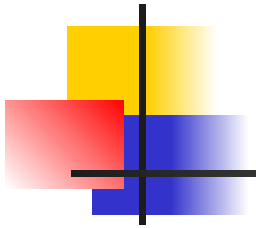
Криптология

Криптография

- Занимается поиском и исследованием математических методов преобразования информации.

Криптоанализ

- Исследует возможности расшифровывания информации без знания ключей.



Криптография

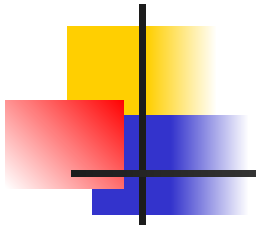
- симметричные криптосистемы
- криптосистемы с открытым ключом
- системы электронной подписи
- управление ключами

Основные направления использования криптографических методов

- передача конфиденциальной информации по каналам связи,
- установление подлинности передаваемых сообщений,
- хранение информации на носителях в зашифрованном виде.

Методы криптографического преобразования

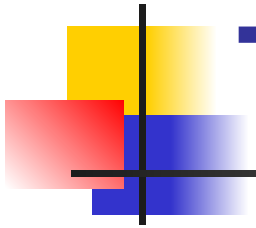
- шифрование—дешифрование;
- кодирование;
- стеганография;
- сжатие — расширение.



Основные понятия методологии криптографии

Алфавит

- Конечное множество используемых для кодирования информации знаков.



Текст

- Упорядоченный набор из элементов алфавита.

Шифрование

- Преобразовательный процесс, в ходе которого исходный текст заменяется шифрованным текстом.

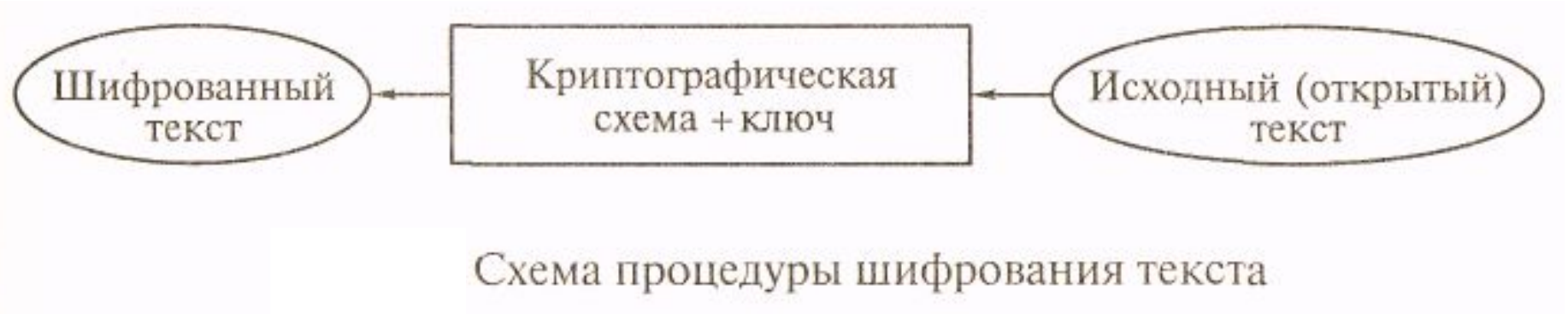


Схема процедуры шифрования текста

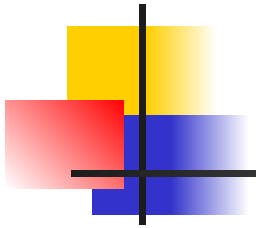
Дешифрование

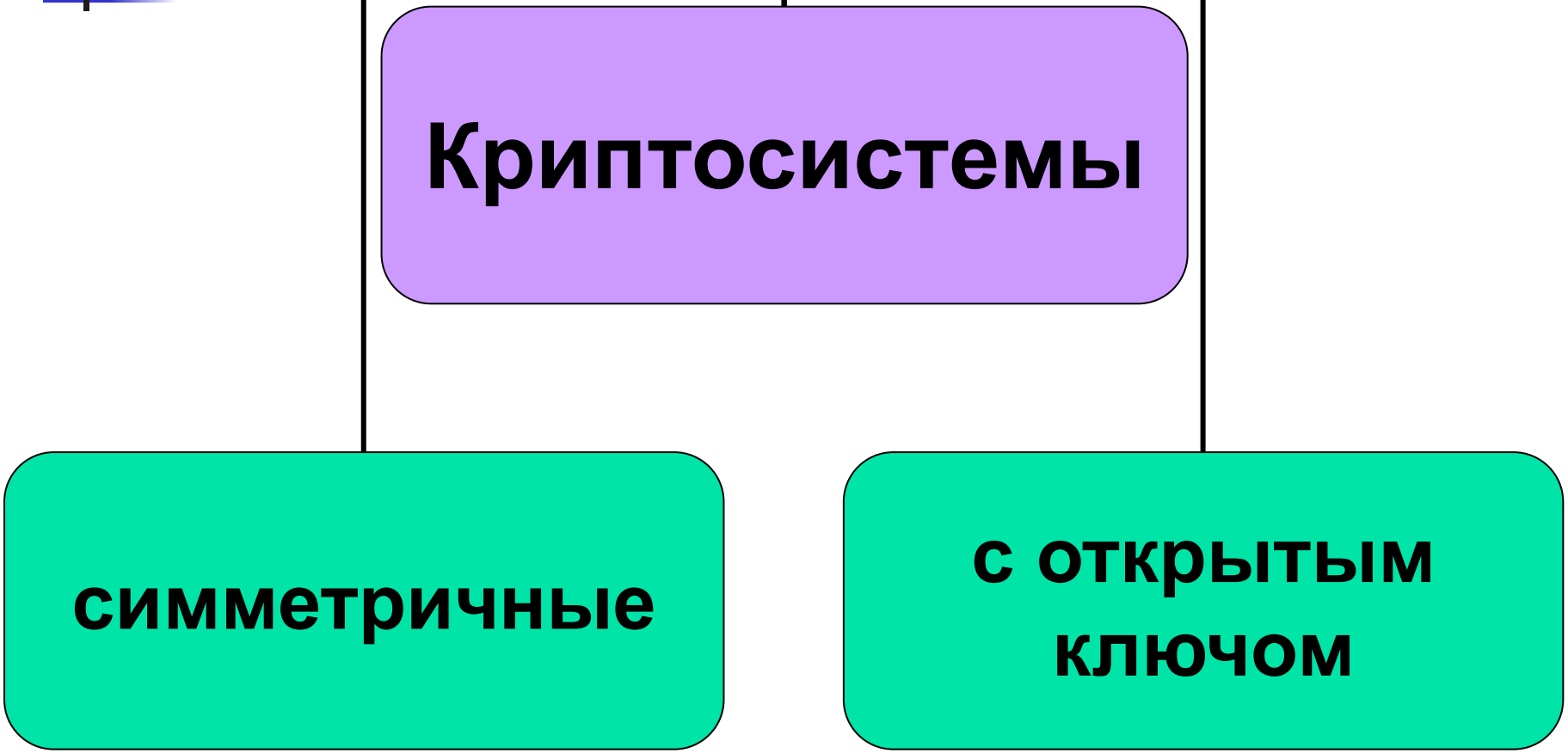
- Процесс, обратный шифрованию.
- На основе ключа шифрованный текст преобразуется в исходный.

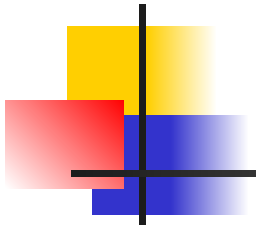
Ключ

- Информация, необходимая для беспрепятственного шифрования и дешифрирования текстов.

Криптосистемы







- В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

- В системах с открытым ключом используют два ключа — открытый и закрытый, которые математически связаны друг с другом.

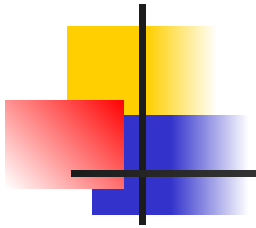
Электронная (цифровая) подпись

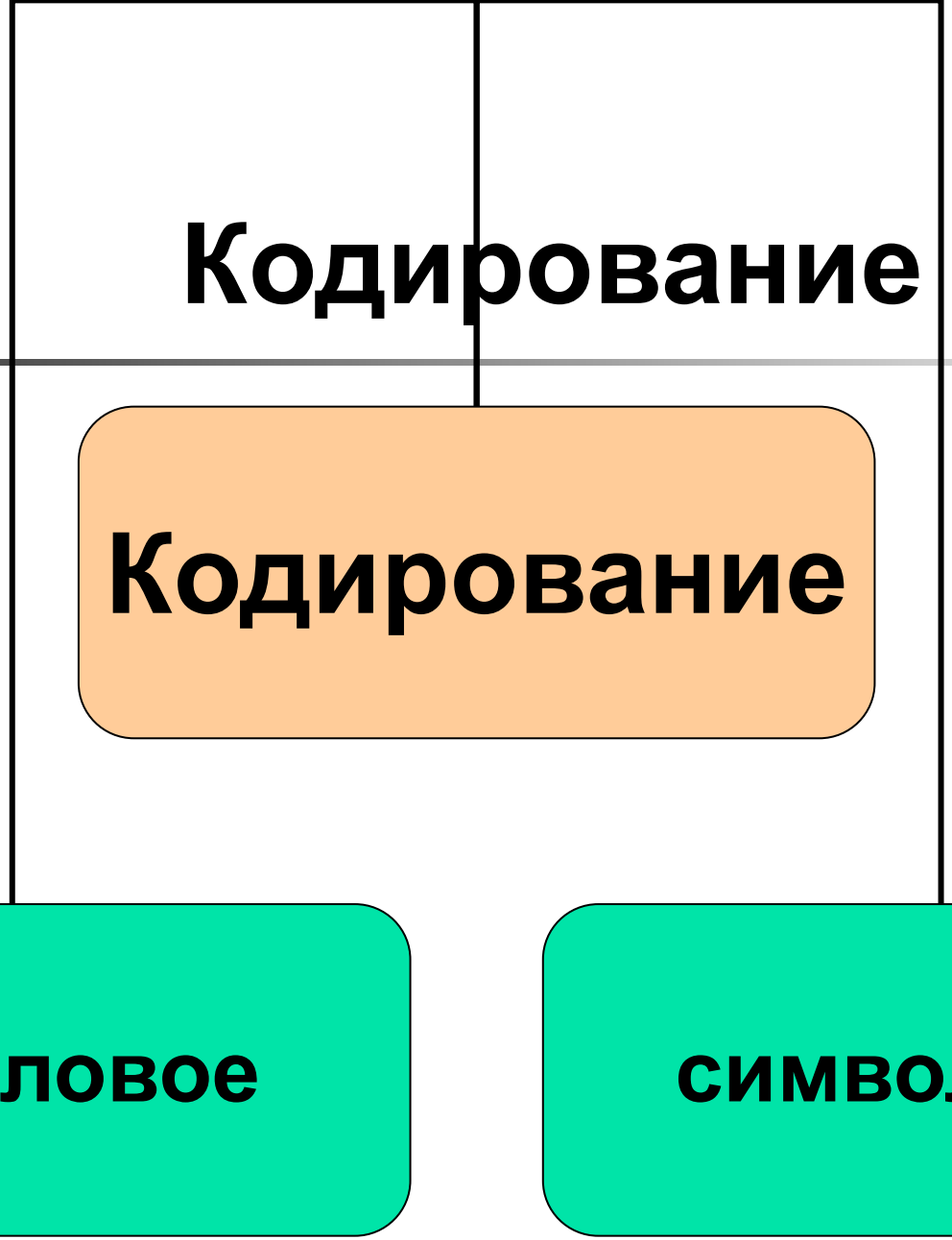
- Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

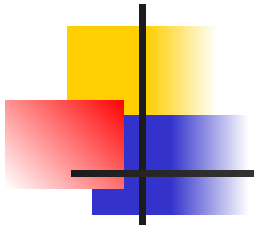
Кодирование

- Такой вид криптографического закрытия, когда некоторые элементы защищаемых данных заменяются заранее выбранными кодами.

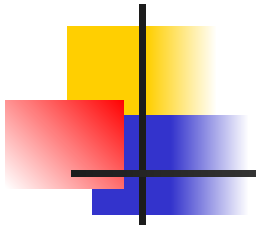
Кодирование



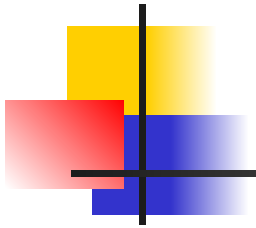




- При смысловом кодировании кодируемые элементы имеют вполне определенный смысл.



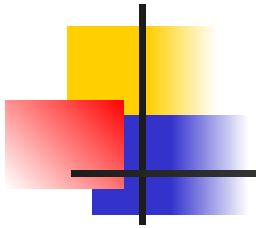
- При символьном кодировании кодируется каждый символ защищаемого сообщения.



- При кодировании замене подвергаются смысловые элементы информации.

Шифрование (дешифрование)

- Вид криптографического закрытия (раскрытия), при котором преобразованию подвергается каждый символ защищаемого сообщения.



Методы шифрования (дешифрования)

Методы шифрования (дешифрования)

с симметричным ключом

системы с открытыми ключами


подстановка (замена)
комбинированное шифрование (дешифрование)
перестановка
Способы шифрования с симметричными ключами
гаммирование
аналитическое преобразование

Метод перестановки

- Несложный метод криптографического преобразования, использующийся, как правило, в сочетании с другими методами.

Аддитивные методы (гаммирование)

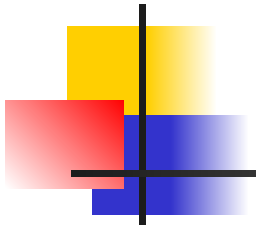
- Заключаются в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры

- Относятся к комбинированным методам и представляют собой последовательность основных методов преобразования, применяемую к блоку шифруемого текста.

Рассечение—разнесение

- Заключается в том, что массив защищаемых данных делится на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации.

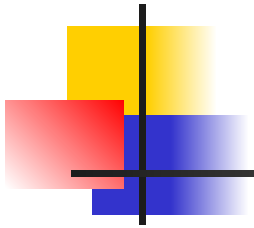


Простейшие шифры и их свойства.

Методы шифрования с симметричными ключами.

Шифрование методами замены (подстановки)

- Подразумевает, что символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов.



- Для повышения стойкости шифра используют полиалфавитные подстановки, в которых для замены символов исходного текста используются символы нескольких алфавитов.

Шифрование с симметричными ключами методами перестановки

- Подразумевает, что символы шифруемого текста внутри шифруемого блока символов переставляются по определенным правилам.

Шифрование с симметричными ключами при помощи аналитических преобразований

- Использует методы алгебры матриц, например умножение матрицы на вектор.

Шифрование аддитивными методами (гаммирование)

- Предусматривает последовательное сложение символов шифруемого текста с символами некоторой специальной последовательности, которая называется гаммой.

Комбинированные методы шифрования с симметричными ключами

- Заключаются в применении различных способов шифрования исходного текста одновременно или последовательно.

Наибольшее распространение получили

- подстановка + гаммирование;
- перестановка + гаммирование;
- гаммирование + гаммирование;
- подстановка + перестановка.

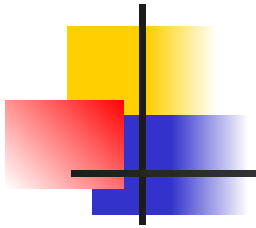
Системы с открытыми ключами

- Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу.

Структурная схема шифрования с открытым ключом

Необратимость

- Практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.



Криптосистемы с открытым ключом

Криптосистемы с открытым ключом

- разложение больших чисел на простые множители
- вычисление логарифма в конечном поле
- вычисление корней алгебраических уравнений

Алгоритмы криптосистемы СОК используются

- как самостоятельные средства защиты передаваемых и хранимых данных;
- средства для распределения ключей;
- средства аутентификации пользователей.