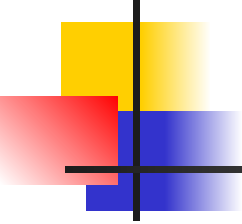


Криптографические алгоритмы

Борисов В.А.

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

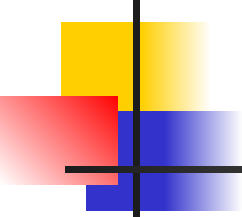


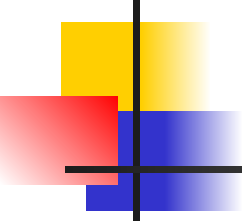
***Как выбрать хороший
криптографический
алгоритм***



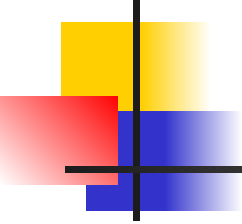
Выбор алгоритма

- воспользоваться известным алгоритмом, сравнительно давно опубликованным в специальном издании;
- довериться известной фирме, специализирующейся на продаже средств шифрования;
- обратиться к независимому эксперту;
- обратиться за поддержкой в соответствующее правительственное ведомство;
- попытаться создать собственный криптографический алгоритм.

- 
-
- Наиболее предпочтительной является использование известного алгоритма, сравнительно давно опубликованного в специальном издании по проблемам криптографии.



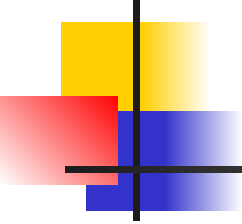
***Криптографические
алгоритмы,
предназначенные для
экспорта***

- 
-
- В настоящее время у пользователей ПК имеется возможность применять шифровальные алгоритмы, встроенные в различные программные продукты.

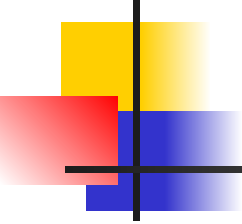


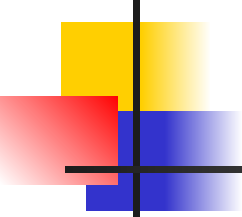
Считается, что

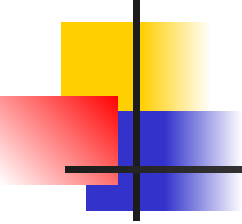
- время от времени отдельные биты ключа подмешиваются в шифртекст;
- ключ имеет длину всего 30 бит вместо официально заявляемых 100 бит;
- в начало каждого шифруемого сообщения вставляется фиксированный заголовок;
- любое шифрованное сообщение содержит отрезок случайного открытого текста вместе с соответствующим ему шифртекстом.



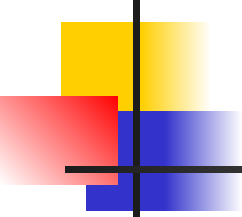
***Симметричный или
асимметричный
криптографический
алгоритм?***

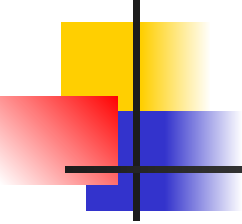
- 
-
- Симметричные криптографические алгоритмы имеют меньшую длину ключа и работают быстрее, чем асимметричные.

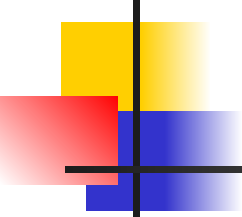
- 
-
- Симметричные криптографические алгоритмы служат для шифрования данных.
 - Асимметричные криптографические алгоритмы отвечают за работу с ключами и многочисленными криптографическими протоколами.

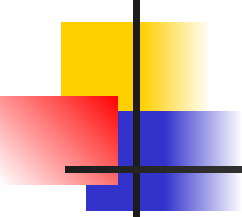


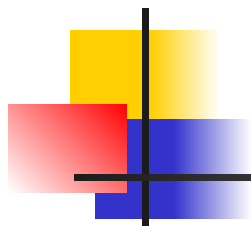
Шифрование в каналах связи компьютерной сети

- 
-
- Одной из отличительных характеристик любой компьютерной сети является ее деление на уровни, каждый из которых отвечает за соблюдение определенных условий и выполнение функций, которые необходимы для общения между собой компьютеров, связанных в сеть.

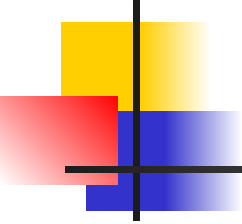
- 
-
- Примерная модель компьютерной сети - OSI.

- 
-
- OSI разносит коммуникационные функции по уровням.
 - Модель OSI выделяет семь уровней: верхние три служат для связи с конечным пользователем, а нижние четыре ориентированы на выполнение коммуникационных функций в реальном масштабе времени.

- 
-
- Если данные шифруются на нижних уровнях, шифрование называется **канальным**.
 - Если шифрование данных выполняется на верхних уровнях, то оно зовется **сквозным**.



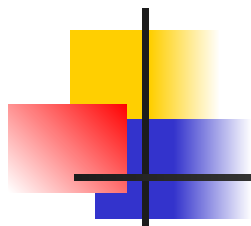
Канальное шифрование

- 
-
- При канальном шифровании шифруются абсолютно все данные, проходящие через каждый канал связи.

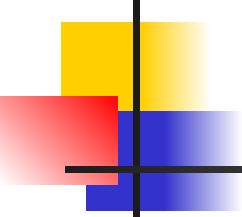
Недостатки канального шифрования



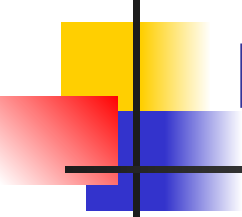
- Данные приходится шифровать при передаче по каждому физическому каналу компьютерной сети.
- Отправка информации в незашифрованном виде по какому-то из каналов ставит под угрозу обеспечение безопасности всей сети в целом.
- Стоимость реализации канального шифрования в больших сетях может оказаться чрезмерно велика.
- Необходимо защищать каждый узел компьютерной сети, через который проходят передаваемые по сети данные.



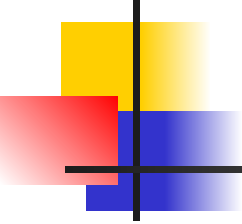
Сквозное шифрование

- 
-
- При сквозном шифровании криптографический алгоритм реализуется на одном из верхних уровней модели OSI.
 - Шифрованию подлежит только содержательная часть сообщения, которое требуется передать по сети.

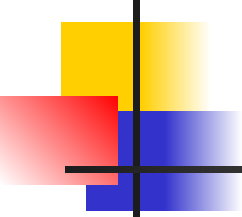
Недостатки сквозного шифрования



- Служебная информация передается по сети в незашифрованном виде.
- Более сложная работа с ключами.
- Различия в коммуникационных протоколах и интерфейсах в зависимости от типов компьютерных сетей и объединяемых в сеть компьютеров.

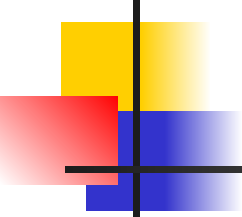


Комбинированное шифрование

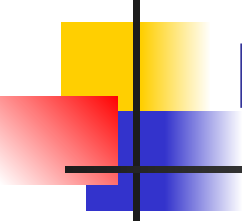
- 
-
- При комбинированном шифровании работа с ключами ведется отдельно: сетевые администраторы отвечают за ключи, используемые при канальном шифровании, а о ключах, применяемых при сквозном шифровании, заботятся сами пользователи.



Шифрование файлов

- 
-
- При шифровании файлов необходимо предусмотреть специальные механизмы для предотвращения возникновения ошибок в шифртексте.

Особенности шифрования файлов



- нередко после шифрования файла его незашифрованная копия благополучно забывается на другом магнитном диске, на другом компьютере или в виде распечатки, сделанной на принтере;
- размер блока в блочном алгоритме шифрования может значительно превышать размер отдельной порции данных в структурированном файле;

Особенности шифрования файлов

- скорость шифрования файлов должна соответствовать скоростям, на которых работают устройства ввода/вывода современных компьютеров;
- разные пользователи должны иметь доступ не только к различным файлам, но и к отдельным частям одного и того же файла.

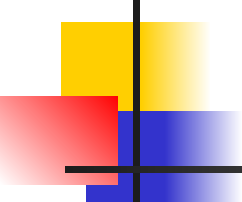


Аппаратное и программное шифрование



Аппаратное шифрование

- обладает большей скоростью;
- аппаратуру легче физически защитить от проникновения извне;
- аппаратура шифрования более проста в установке.



**Аппаратные
средства
шифрования**

самодостаточные
шифровальные
модули

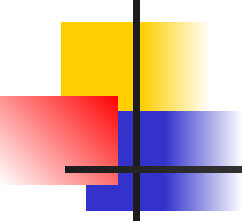
блоки шифрования
в каналах связи

шифровальные
платы расширения
для установки в ПК

Программное шифрование



- программные средства шифрования легко копируются,
- они просты в использовании,
- их нетрудно модифицировать в соответствии с конкретными потребностями.



Особенности применения встроенных средств шифрования файлов

- ни в коем случае нельзя хранить ключи на диске вместе с зашифрованными с их помощью файлами,
- незашифрованные копии файлов необходимо стереть сразу же после шифрования.



Сжатие и шифрование



Причины использования алгоритмов сжатия данных

- При вскрытии шифра криптоаналитик более всего полагается на избыточность, свойственную любому открытому тексту.
- При сжатии уменьшается длина открытого текста, и тем самым сокращается время, которое будет потрачено на его шифрование.