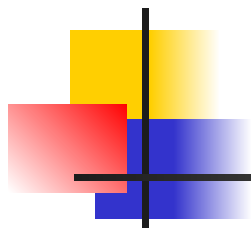


ДОКУМЕНТАЛЬНОЕ ОБЕСПЕЧЕНИЕ КРИПТОГРАФИИ

Борисов В.А.

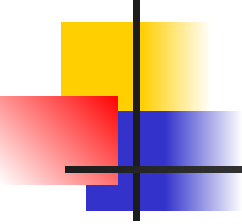
КАСК – филиал ФГБОУ ВПО РАНХ и ГС

Красноармейск 2011 г.

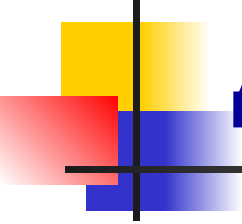


Значение документального обеспечения применения криптографии

Правила использования криптографических средств защиты

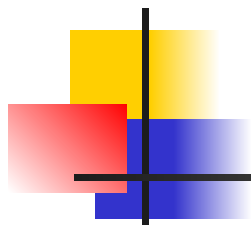


- сохранение в тайне ключей,
- исключение дублирования,
- достаточно частая смена ключей.

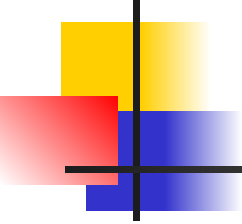


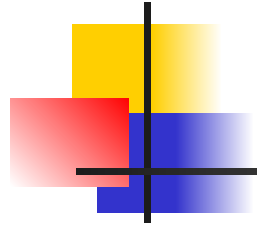
Дублирование

- Повторное шифрование одного и того же отрывка текста с использованием тех же ключей.

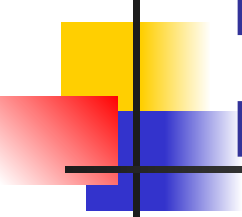


- Смена ключей по временному графику является защитной мерой против возможного их хищения, а смена после шифрования определенного объема текста — от раскрытия шифра статистическими методами.

- 
-
- Для реализации противодействия злоумышленнику применяют документальное оформление протоколов связи и распределения ключей.

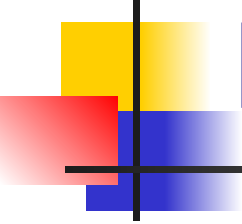


Организация протоколирования связи и распределения ключей



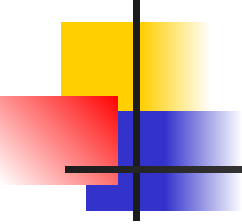
Механизм распределения ключей криптографического преобразования

- ключи должны выбираться случайно;
- ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю;
- механизм распределения ключей должен обеспечивать тайну ключей на всех этапах функционирования системы;
- должна быть предусмотрена достаточно частая смена ключей.



Протокол связи

- протокол должен защищать открытый текст и ключ от несанкционированного доступа на всех этапах передачи информации от источника к получателю сообщений;
- протокол не должен допускать выхода в линии связи лишней информации, предоставляющей криптоаналитику противника дополнительные возможности дешифрования криптограмм.

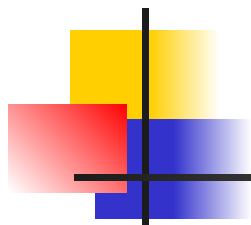


Новые направления в криптографии

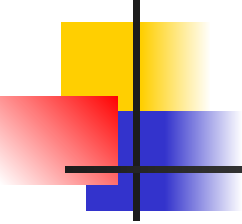
```
graph TD; A[Новые направления в криптографии] --> B[открытое распределение ключей]; A --> C[открытое шифрование];
```

открытое
распределение
ключей

открытое
шифрование



- Задача управления большим числом ключей является очень важной при использовании любого метода шифрования.



Ключи

```
graph TD; A[Ключи] --> B[для шифрования данных]; A --> C[для шифрования ключей];
```

для
шифрования
данных

для
шифрования
ключей