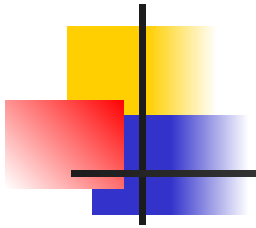
ОЦЕНКА КРИПТОСТОЙКОСТИ ШИФРОВ, ИХ ПРОГРАММНО-АППАРАТНЫХ РЕАЛИЗАЦИЙ И ТЕХНИКО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ

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



Оценка криптостойкости шифров

Криптостойкость

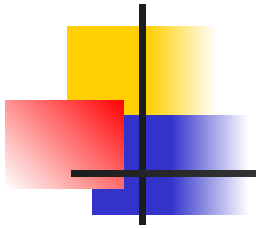
- Характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа.

Показатели криптостойкости

- число всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Криптоанализ

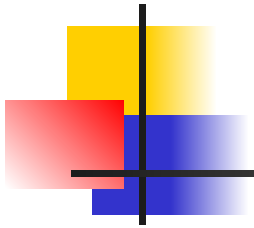
- Минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст.



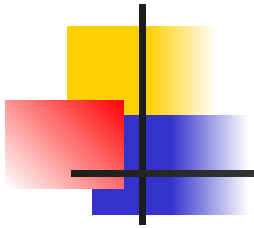
- По стойкости шифра можно определить предельно допустимый объем информации, зашифровываемый при использовании одного ключа.

Стойкость криптографического алгоритма

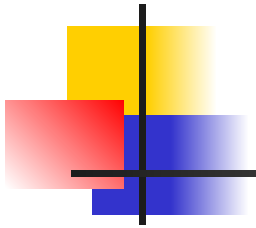
- Устойчивость к попыткам противоположной стороны его раскрыть.



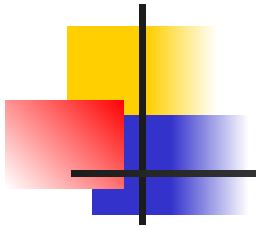
- Шифры, которые вообще невозможно раскрыть, называются абсолютно, или теоретически, стойкими.



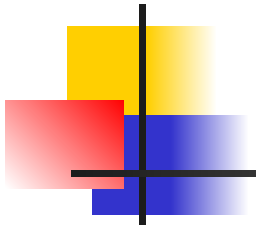
- Все современные криптосистемы построены по принципу Кирхгофа, т.е. секретность зашифрованных сообщений определяется секретностью ключа.



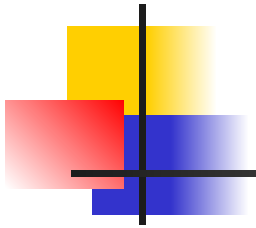
- Моноалфавитная подстановка является наименее стойким шифром, так как при ее использовании сохраняются все статистические закономерности исходного текста.



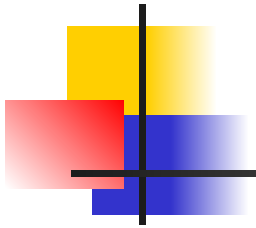
- Стойкость простой полиалфавитной подстановки оценивается значением 20^n, где n — число различных алфавитов, используемых для замены.



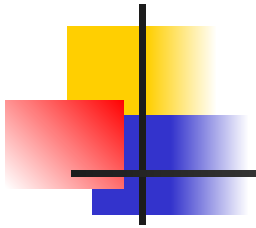
- Стойкость простой перестановки однозначно определяется размерами используемой матрицы.



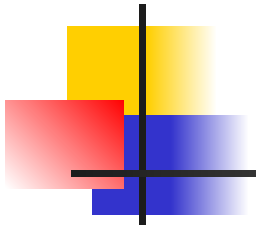
- Стойкость гаммирования однозначно определяется длиной периода гаммы.



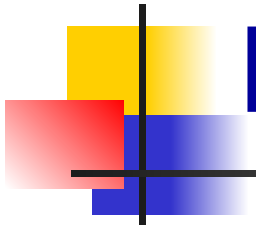
- При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов.



Оценка программно-аппаратных реализаций шифров



- По способу использования средств закрытия информации обычно различают потоковое и блочное шифрование.

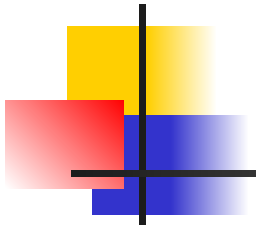


Потоковое шифрование

- Каждый символ исходного текста преобразуется независимо от других.

Блочное шифрование

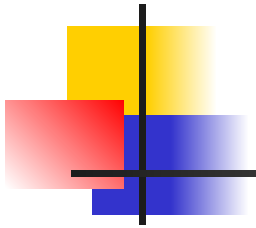
- Одновременно преобразуется некоторый блок символов закрываемого исходного текста, причем преобразование символов в пределах блока является взаимозависимым.



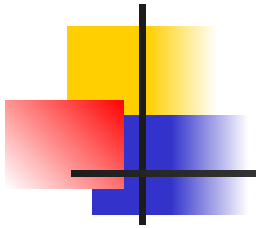
- При аппаратной реализации все процедуры шифрования и дешифрования реализуются специальными электронными схемами.

Пути улучшения криптографических свойств гаммы

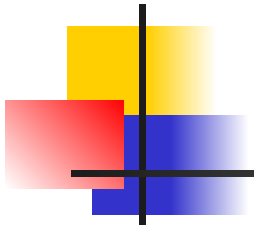
- блок управления работой регистра сдвига,
- использовании нелинейных обратных связей.



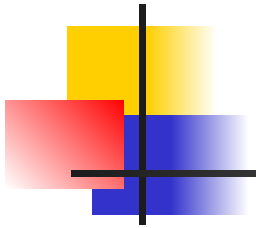
Технико-экономические показатели криптографических методов защиты



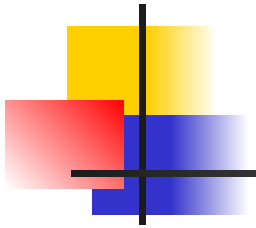
- Основным достоинством программных методов реализации криптографической защиты является их гибкость, т.е. возможность быстрого изменения алгоритма шифрования.



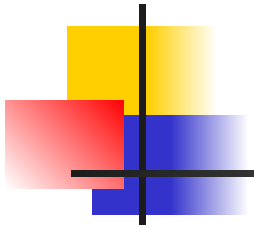
- Основным недостатком программной реализации криптографических методов является существенно меньшее быстродействие.



- Программные методы могут быть реализованы только при наличии в составе аппаратуры мощного процессора.



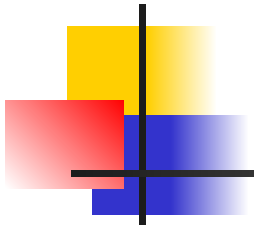
- Расходы на программную реализацию криптографических методов защиты определяются сложностью алгоритмов прямого и обратного преобразований.



- Расходы на аппаратную реализацию могут быть оценены приближенно стоимостью шифрующей аппаратуры.

Трудоемкость метода шифрования

- Число элементарных операций, необходимых для шифрования одного символа исходного текста.



- Таким образом, наиболее трудоемкими являются аналитические преобразования, затем по мере снижения трудоемкости следует гаммирование, перестановки и замены.