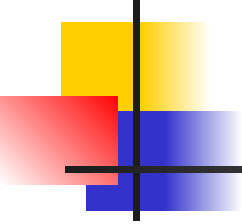


# *Методы криптоанализа*

Борисов В.А.

КАСК – филиал ФГБОУ ВПО РАНХ и ГС

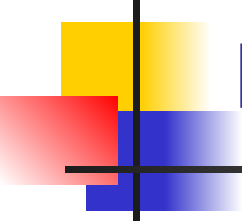
Красноармейск 2011 г.



---

# ***Дифференциальный криптоанализ***

# Дифференциальный криптоанализ



---

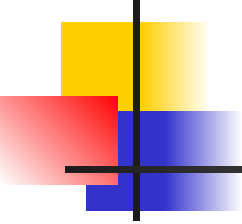
- Работает с парами шифротекстов, открытые тексты которых содержат определенные отличия.



# Характеристики

---

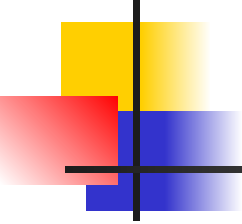
- Определенные различия получаемых шифротекстов.

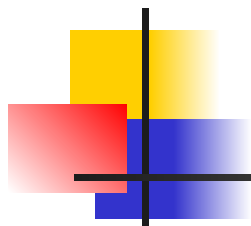
- 
- 
- Пара открытых текстов, соответствующих характеристике, называется *правильной парой*, а пара несоответствующих - *неправильной парой*.



---

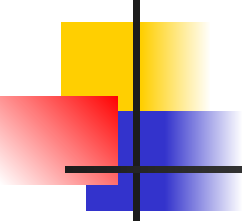
# ***Криптоанализ со связанными ключами***

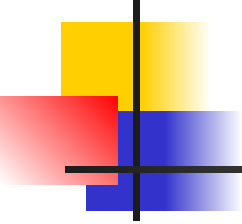
- 
- 
- Криптоанализ со связанными ключами похож на дифференциальный криптоанализ, но изучает различие между ключами.



# *Линейный криптоанализ*



- 
- 
- Криптоаналитическое вскрытие использует линейные приближения для описания работы блочного шифра.

- 
- 
- Чем больше данных, тем вернее предположение, чем больше смещение, тем быстрее вскрытие увенчается успехом.