Фестиваль исследовательских и творческих работ учащихся «Портфолио»

Основные понятия криптографии

Работай с диаграммой

- Криптология
  - Криптография
    - Открытый текст
    - Криптограмма (шифртекст)
  - Криптоанализ
    - Шифр
      - Стойкость шифра
    - Ключ

Криптология

(от греч. cryptos - "тайный" и logos - "мысль")

Наука,
занимающаяся проблемами
защиты информации

Вернуться

Криптография

(от греч. cryptos - тайный, сокрытый,
и grapho - пишу, черчу, рисую)

Наука,
изучающая методы
шифрования сообщений

Вернуться

Криптоанализ

Наука,
разрабатывающая методы
раскрытия шифров.

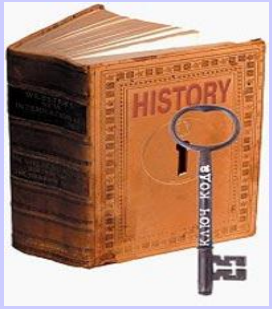
Вернуться

Шифр

(от арабского "цифра")
это определенные правила
преобразования открытых данных
в зашифрованные и обратно.

Вернуться

Ключ



Секретный элемент шифра, недоступный посторонним.

Вернуться

Открытый текст

Исходное сообщение, которое подвергается шифрованию.

Вернуться

Криптограмма

Результат, полученный применением шифра к исходному сообщению.
В дальнейшем криптограмма подлежит дешифрации.

Криптограмма (шифртекст)

Расшифрование (дешифрование)

Шифр

Ключ

Вернуться

Стойкость шифра

это способность противостоять попыткам постороннего лица восстановить открытый текст по перехваченному шифртексту.

Вернуться