

*Фестиваль исследовательских и творческих работ учащихся
«Портфолио»*

Основные понятия криптографии





*Работай с
диаграммо
й*

Криптология

Криптография

Криптоанализ

*Открытый
текст*

*Криптограмма
(шифртекст)*

Шифр

Ключ

*Стойкость
шифра*



Криптология

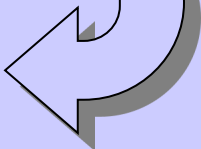


(от греч. cryptos - "тайный" и logos - "мысль")

Наука,

занимающаяся проблемами
защиты информации

Вернуться



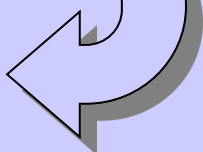
Криптография

Л Д Ч О М О М А Л Л Ф Ы З Щ Х
З У С Л Й Ц У З Ж Ь С Э Щ Е П
Ш С С Ф Ч С Ъ Х Ч Ч Ш Ц Щ С
В А К Р И П Т О Г Р А Ф И Я Э С
А К Ч С Ш Щ О К Ц Щ С М Т Р Щ
О Г А Ц Ш У Й Р Ш С У С Щ С Т
Ф Ы Х Ф Ш В Х Й В Э Ы Л В Х С

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

Наука,
изучающая методы
шифрования сообщений

Вернуться





Криптоанализ

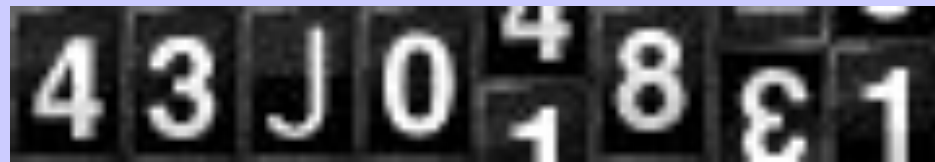
Наука,
разрабатывающая методы
раскрытия шифров.

Вернуться





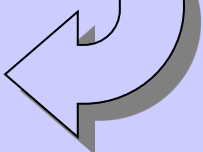
Шифр



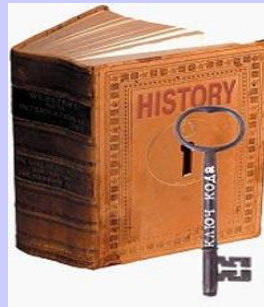
(от арабского "цифра")

**это определенные правила
преобразования открытых данных
в зашифрованные и обратно.**

Вернуться

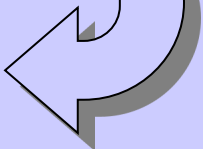


Ключ



Секретный элемент шифра,
недоступный посторонним.

Вернуться



Открытый текст

Исходное сообщение, которое подвергается шифрованию.

Открытый
текст

Шифрование

Шифр

Ключ
Ч

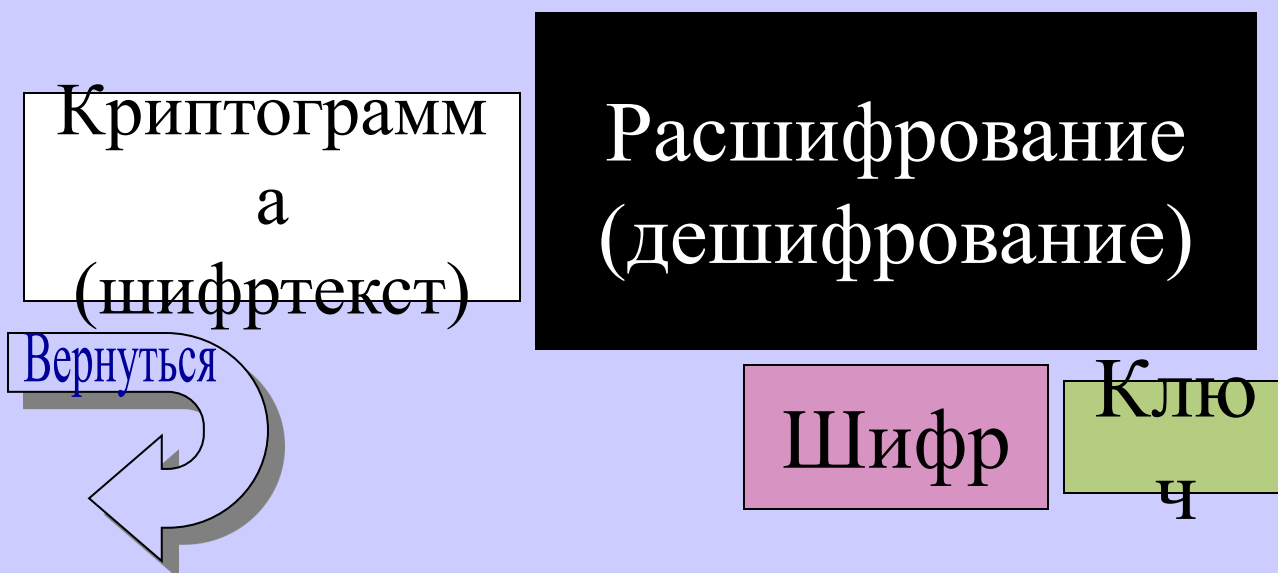
Вернуться



Криптограмма

Результат, полученный применением шифра к исходному сообщению.

В дальнейшем криптограмма подлежит дешифрации.





Стойкость шифра

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



Вернуться

