Фестиваль исследовательских и творческих работ учащихся «Портфолио»

Методы шифрования

Работай с диаграммой

Методы шифрования

- Метод замены
- Метод перестановки
- Аддитивный метод
- Комбинированный метод

назад

Это метод,
при котором позиции букв
в шифровке остаются теми же,
что и у открытого текста,
но символы открытого текста
заменяются символами
другого алфавита.

Например:

**Если по забывчивости не переключить
на клавиатуре ЭВМ регистр
с латиницы на кириллицу,**

**то вместо букв русского алфавита
при вводе текста будут печататься буквы
латинского алфавита.**

В результате:

криптография → rhbgnjuhfabz

Вернуться

Это метод,
при котором все буквы открытого текста остаются без изменений,
но перемещаются

с их исходных позиций на другие места

Например:

- **Методом перестановки**

  двух соседних букв в слове

- **можно получить простейшую шифровку**

к	р	и	п	т	о	г	р	а	ф	и	я

Это метод,

в котором буквы алфавита вначале заменяются числами,

к которым затем добавляются числа секретной псевдослучайной числовой последовательности (гаммы).

- **Состав гаммы меняется в зависимости от использованного ключа.**
- **Обычно для шифрования используется логическая операция «Исключающее ИЛИ».**

- **При дешифровании та же гамма накладывается на зашифрованные данные.**

- **Метод гаммирования широко используется в военных криптографических системах.**

Вернуться

Это метод,

при котором для шифрования сообщения используются сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

Вернуться