

Шифры Цезаря и Атбаш

Gagik T. Papikyan

RUDN University, Moscow, Russian Federation

Теоретические сведения

Шифр Цезаря

- ▶ Прimitивный алгоритм шифрования.
- ▶ Отсутствие практического применения.
- ▶ Смещение каждого символа входящего сообщения на K шагов в рассматриваемом алфавите.

Пример:

Алфавит: а, б, в, г, д

Входящее сообщение: “авд”

K : 1

Зашифрованное: “бга”

Шифр Атбаш

- ▶ Примитивный алгоритм шифрования.
- ▶ Отсутствие практического применения.
- ▶ ‘Симметричное отражение’ символа входящего сообщения относительно центра рассматриваемого алфавита.

Пример:

Алфавит: а, б, в, г, д

Входящее сообщение: “ав”

Зашифрованное: “дв”

Пример реализации Шифра Цезаря

```
const alphabet = `! abcdefghijklmnopqrstuvwxyzABCDEFGGHIJKLMNOPQRSTUVWXYZ`
```

```
function CaesarEncode( msg, k = 1){  
  let res = ''  
  for(let char of msg){  
    let code = alphabet.indexOf(char)  
    res += alphabet[ (code+k)%alphabet.length ]  
  }  
  return res  
}
```