

Шифровани е информаци

и

Автор Майоров А.В
ИСИП-11

Руководитель Косыченко Д.А

11.05.2022

PROJECTS

Содержание



1 Основные понятия

шифрования

2 Создание алгоритма

шифрования

2.2 Выявление преимуществ и недостатков

алгоритма



Основные понятия шифрования



Шифрование – математический процесс превращения информации в нечитаемый вид для защиты этой самой информации.

Шифр – алгоритм, используемый при шифровании и дешифровании. Например, Шифр цезаря или Азбука Морзе.

Ключ – инструкция к шифрованию или дешифрованию информации.

Методы шифрования



01

Симметричное

Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации

[ПОДРОБНЕЕ...](#)

02

Ассиметрично

е

В асимметричном шифровании данные шифруются одним ключом, а расшифровываются другим. Первый ключ можно держать у всех на виду, а вот второй нужно прятать.

[ПОДРОБНЕЕ...](#)

03

Хеширование

Хеширование – это математический алгоритм, который преобразовывает массив данных в строку состоящую из букв и цифр фиксированной длины

[ПОДРОБНЕЕ...](#)

Создание алгоритма шифрования

В своей программе я буду использовать шифр Цезаря – один из самых простых и наиболее известных методов шифрования. Это вид шифра, в котором каждый символ заменяется другим, находящимся на некотором позиций левее или правее него. Например, в шифре со сдвигом вправо на три, буква А была бы заменена на Г, Б на Д и так далее.



```
const abc = 'абвгдеёжзийклмнопрстуфхцчшщъьэя';  
  
var s1,s2: string;  
    l,i,k,p: integer;  
  
begin  
    write('Шифр Цезаря. Введите длину сдвига ');  
    readln(l);  
  
    write('Введите текст ');  
    readln(s1);  
  
    for i := 1 to length(s1) do  
        if s1[i] = ' ' then s2 := s2 + ' '  
        else  
            begin  
                for k := 1 to length(abc) do  
                    if s1[i] = abc[k] then  
                        begin  
                            p:= k + l;  
                            p:= p mod  
                                length(abc);  
                            s2:= s2 + abc[p];  
                            break  
                        end;  
                    end;  
                write('зашифрованный текст - ');  
                write(s2);  
                readln;  
            end;  
        end;  
end.
```

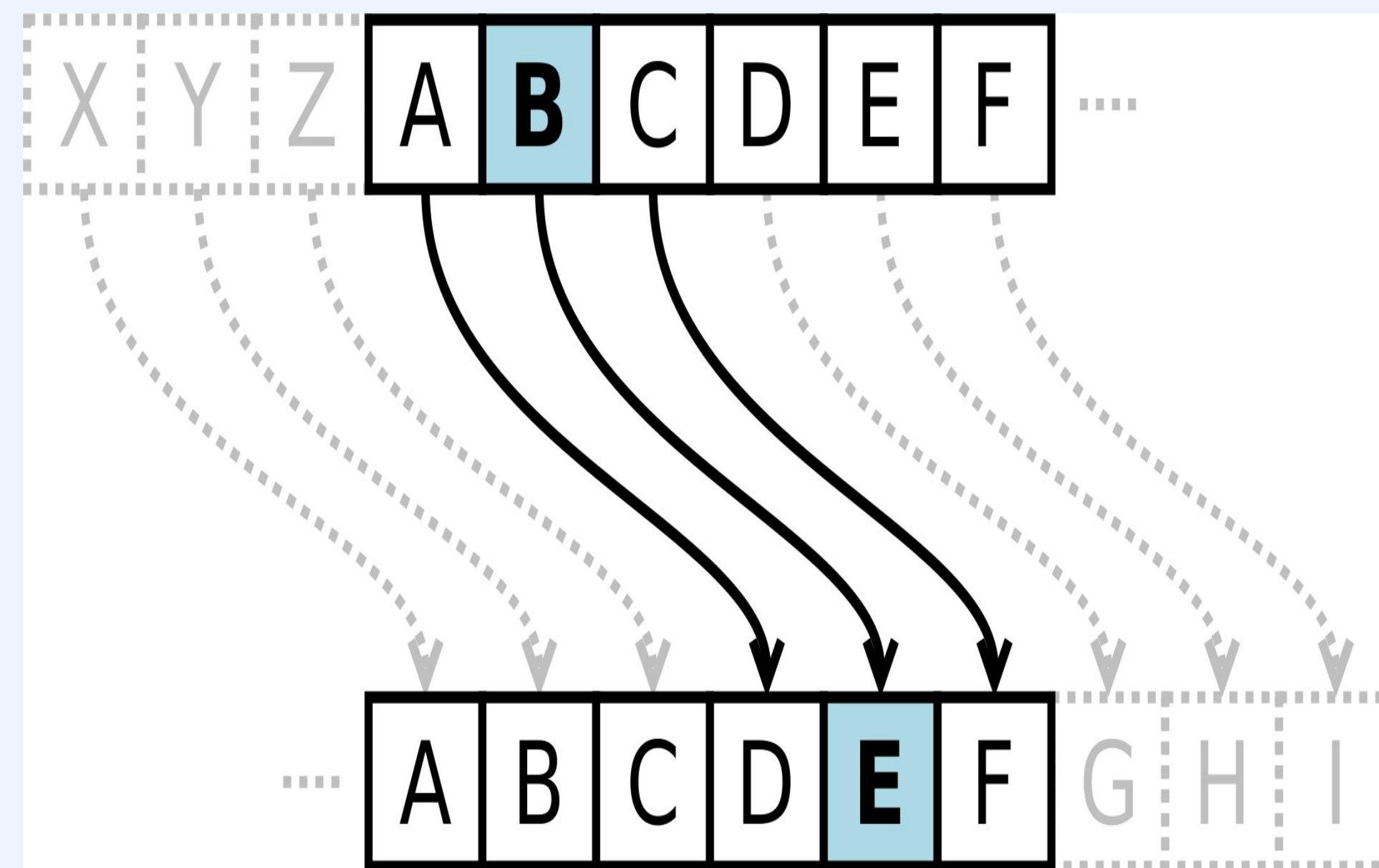
Окно вывода

```
Шифр Цезаря. Введите длину сдвига 1  
Введите текст а  
зашифрованный текст - б
```

Пример



Давайте сопоставим каждому символу алфавита его порядковый номер, начиная с нуля. Тогда, шифрование с использованием ключа $k=3$. Буква «С» сдвигается на три буквы вперед и становится буквой «Ф». Твердый знак, перемещенный на три буквы вперед, становится буквой «Э», и так далее



Выявление преимуществ и недостатков алгоритма



Понятность

Шифр Цезаря можно использовать новичкам для более полного понимания как работают шифры. Такой шифр является самым легким и понятным из известнейших классических шифров.



Коммуникабельность

Такой шифр можно использовать как способ общения или же просто передачи информации на листке бумаги.



Лёгкость дешифрования

Такой шифр может быть легко взломан даже в случае, когда взломщик знает зашифрованный текст.



Применение

В наше время, а именно в век информационного и технологического развития, такие шифры в чистом виде нигде не применяются

Спасибо за
Внимание!

КОНЕЦ.