Шифр простой замены

Бакундукизе Эжид Принц НФИмд-01-21

21 сентября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

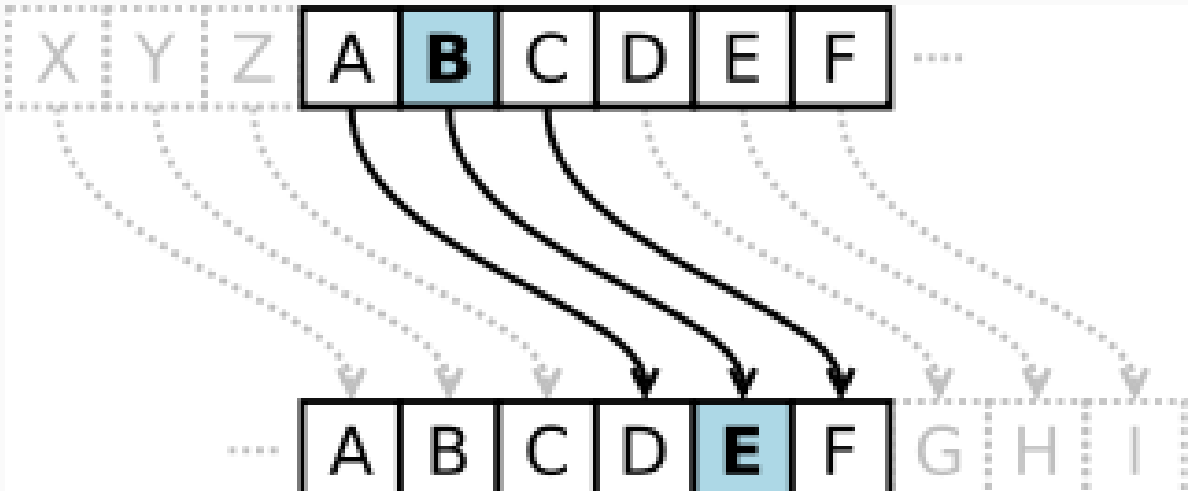
Шифрование

Шифрование - обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

С помощью шифрования обеспечиваются три состояния безопасности информации: Конфиденциальность, Целостность, Идентифицируемость.

Шифр простой замены

Шифр простой замены, простой подстановочный шифр, моноалфавитный шифр — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.



Шифр Цезаря

Шифр Цезаря — это вид шифра, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

```
y = (x + k) mod n
x = (y - k + n) mod n
```

где *x — символ открытого текста,* y — символ

Шифр Атбаш

Атбаш — простой шифр подстановки.

Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите. Также, как и Шифрование Цезаря является методом простой замены.

Работа алгоритмов

```
if __name__ == "__main__":
    main()
```

```
Шифрование Цезаря: RUDN
WZIS
Дешифрока Цезаря: WZIS
RUDN
Атбаш - шифрование: RUDN
IFWM
Атбаш - дешивровка: IFWM
RUDN
```

Figure 2: Работа алгоритмов

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы мы познакомились с алгортмами шифрования простой замены.

Рассмотрели данный вид алгоритмов на примере шифрования Цезаря и Атбаш. Выполнили программную реализацию этих двух алгоритмов.

Список литературы

Список литературы

1. [Э. Мэйволд. Безопасность сетей.]
2. [Роберт Черчхаус, “Коды и шифры. Юлий Цезарь”]
3. [Гай Светоний Транквилл. Жизнь двенадцати цезарей]
4. [Атбаш (https://www.livelib.ru/book/1001019648-atbash)]