Защита лабораторной работы №1. Шифры простой замены

Бурдина Ксения Павловна

2023 Sep 13th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №1

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

- Освоение шифров простой замены - шифр Цезаря и шифр Атбаш
- Программная реализация шифров простой замены

Теоретические сведения

Теоретические сведения

Механизмы криптографии:

- шифрование симметричными ключами
- шифрование асимметричными ключами
- хеширование

Теоретические сведения. Шифр Цезаря

Шифр Цезаря - это моноалфавитная подстановка, где каждой букве открытого текста ставится в соответствие одна буква шифртекста.

Математический вид процедуры шифрования:

$$T_m = \{T^j\}, j = 0, 1, ..., m - 1,$$

$$T^j(a) = (a + j) \bmod m,$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figure 1: Алфавит шифра Цезаря

Теоретические сведения. Шифр Атбаш

Шифр Атбаш - это шифр сдвига на всю длину алфавита.

Для алфавита, состоящего только из русских букв и пробела, таблица шифрования имеет следующий вид:

Figure 2: Алфавит шифра Атбаш

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Постановка задачи:

1. Рализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

Результат выполнения лабораторной работы. Шифр Цезаря

Алгоритм поиска новых символов и вывода полученного текста на основе принципа формирования шифра Цезаря:

```
def caesar(text: chr, key: int, abc: list):
    def caesar(text: chr, key: int):
        return abc.index(text) + key

    if text.lower() not in abc:
        return text

    new_text = abc[caesar(text.lower(), key) % len(abc)]
    if text.isupper():
        new_text = new_text.upper()
    return new_text
```

Figure 3: Функция формирования алфавита для шифра Цезаря

```
def caesar_encr(message: str, key: int, abc: list):
    a = list(map(lambda text: caesar(text, key, abc), message))
    return "".join(a)
```

Figure 4: Функция для запуска работы шифра Цезаря

Результат выполнения лабораторной работы. Шифр Цезаря

Нахождение порядковых номеров каждого символа алфавита и определение переменных для работы функций:

```
print(ord("a"), ord("z"))
print(ord("а"), ord("я"))
```

```
97 122
1072 1103
```

```
eng_c = list(map(chr, range(97, 123)))
rus_c = list(map(chr, range(1072, 1104)))
```

Figure 5: Определение переменных для работы с алфавитом

Результат выполнения лабораторной работы. Шифр Цезаря

Примеры работы функции по реализации шифра Цезаря:

```
print("Code:", caesar_encr("Secret letter", 3, eng_c))
print("Decoding:", caesar_encr("Vhfuhw ohwwhu", 23, eng_c))
```

```
Code: Vhfuhw ohwwhu
Decoding: Secret letter
```

Figure 6: Реализация шифра Цезаря на примере английского текста

```
print("Шифр:", caesar_encr("Тайное письмо", 3, rus_c))
print("Расшифровка:", caesar_encr("Хгмрси тлфяпс", 29, rus_c))
```

```
Шифр: Хгмрси тлфяпс
Расшифровка: Тайное письмо
```

Figure 7: Реализация шифра Цезаря на примере русского текста

Результат выполнения лабораторной работы. Шифр Атбаш

Принцип формирования нового алфавита для зашифровки сообщения из введенных данных:

```
def atbash(text: chr, abc: list):
    if text.lower() not in abc:
        return text
    new_text = abc[len(abc) - abc.index(text.lower()) - 1]
    if text.isupper():
        new_text = new_text.upper()
    return new_text
```

Figure 8: Функция формирования алфавита для шифра Атбаш

```
def atbash_encr(message: str, abc: list):
    a = list(map(lambda text: atbash(text, abc), message))
    return "".join(a)
```

Figure 9: Функция для запуска работы шифра Атбаш

Результат выполнения лабораторной работы. Шифр Атбаш

Примеры работы функции по реализации шифра Атбаш:

```
print("English alphabet:")
atbash_encr("abcdifghijklmnopqrstuvwxyz ", eng_a)
```

```
English alphabet:

' zyxsvutsrqponmlkjihgfedcba'
```

Figure 10: Реализация шифра Атбаш на примере английского текста

```
print("Русский алфавит:")
atbash_encr("абвгдежзийклмнопрстуфхцчшщъыьэюя ", rus_a)
```

```
Русский алфавит:

' яюэьыъщшчцхфутсрпонмлкйизжедгвба'
```

Figure 11: Реализация шифра Атбаш на примере русского текста

Выводы

Выводы

1. Изучили шифры простой замены
2. Реализовали шифр Цезаря с произвольным ключом k
3. Реализовали шифр Атбаш