

Математические основы защиты информации и информационной безопасности. Лабораторная работа №1

Шифры простой замены

Студент: Лесков Данила Валерьевич НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
3.1	Шифр Цезаря	7
3.2	Шифр Атбаш	7
4	Выполнение лабораторной работы	8
4.1	Листинг кода	9
4.2	Результаты и анализ выполнения	11
5	Выводы	13
	Список литературы	14

List of Figures

4.1	Таблица ASCII	8
4.2	Шифр Цезаря	11
4.3	Шифр Атбаш	12

List of Tables

1 Цель работы

Ознакомиться с шифрами простой замены на примере шифра Цезаря и Атбаш.

2 Задание

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

3 Теоретическое введение

3.1 Шифр Цезаря

Данный шифр замены позволяет зашифровать сообщение путем сдвига каждого символа сообщения на произвольный ключ j . Таким образом, можно вывести соотношение для шифра Цезаря [1]:

$$T_m = T^j, j = 0, 1, \dots, m - 1,$$

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

где T_m — циклическая подгруппа; $(a + j) \bmod m$ - операция нахождения остатка от целочисленного деления $a + j$ на m .

3.2 Шифр Атбаш

Шифрование Атбаш - шифрование, правило замены которого строится из следующего соотношения:

$$m - n + 1,$$

где переменная m - число букв в алфавите; n - порядковый номер заданного символа. Говоря по простому метод сдвига на порядковый номер буквы в алфавите.

Более подробно о шифрах см. в [1,2].

4 Выполнение лабораторной работы

Для выполнения данной работы были описаны два метода: `caesar(message, shift)` для выполнения алгоритма шифрования Цезаря и `atbash(message)` для шифрования Атбаш. Первый метод принимает исходное сообщение и ключ смещения `shift`, а второй метод только сообщение. Оба метода возвращают зашифрованное сообщение. В качестве алфавита был выбран английский строчный алфавит, а для взаимодействия с ним была использована таблица ASCII (рис. 4.1).

!	32	5	53	J	74	т	95	t	116	й	137	ю	158		179	┌	200	└	221	€	242
"	33	6	54	K	75	а	96	u	117	к	138	я	159	└	180	└	201	└	222	€	243
#	34	7	55	L	76	б	97	v	118	л	139	а	160	└	181	└	202	└	223	€	244
\$	35	8	56	M	77	в	98	w	119	м	140	б	161	└	182	└	203	└	224	€	245
%	36	9	57	N	78	с	99	x	120	н	141	в	162	└	183	└	204	└	225	€	246
&	37	:	58	O	79	д	100	y	121	о	142	г	163	└	184	└	205	└	226	€	247
'	38	:	59	P	80	е	101	z	122	п	143	д	164	└	185	└	206	└	227	€	248
(39	<	60	Q	81	ф	102	[123	р	144	е	165	└	186	└	207	└	228	€	249
)	40	=	61	R	82	г	103]	124	с	145	ж	166	└	187	└	208	└	229	€	250
*	41	>	62	S	83	h	104	^	125	т	146	з	167	└	188	└	209	└	230	€	251
+	42	?	63	T	84	i	105	_	126	у	147	и	168	└	189	└	210	└	231	€	252
,	43	@	64	U	85	j	106	0	127	ф	148	й	169	└	190	└	211	└	232	€	253
-	44	А	65	V	86	k	107	А	128	х	149	к	170	└	191	└	212	└	233	€	254
.	45	В	66	W	87	l	108	Б	129	ц	150	п	171	└	192	└	213	└	234	€	255
/	46	С	67	X	88	m	109	В	130	ч	151	н	172	└	193	└	214	└	235		
0	47	Д	68	Y	89	n	110	Г	131	■	152	н	173	└	194	└	215	└	236		
1	48	Е	69	Z	90	o	111	Д	132	■	153	о	174	└	195	└	216	└	237		
2	49	Ф	70	[91	p	112	Е	133	Ъ	154	п	175	└	196	└	217	└	238		
3	50	Г	71	\	92	q	113	Ж	134	■	155	■	176	└	197	└	218	└	239		
4	51	Н	72]	93	r	114	З	135	Ъ	156	■	177	└	198	└	219	└	240		
	52	И	73	^	94	s	115	И	136	З	157	■	178	└	199	└	220	└	241		

Figure 4.1: Таблица ASCII

На языке python системные методы `ord()` и `chr()` преобразуют строковой символ в порядковый номер ASCII и обратно соответственно. Благодаря этим методам в данной лабораторной работе осуществляется работа со смещением символов строковых элементов.

Более подробно о таблице ASCII и методах работы с ней см. в [3,4].

4.1 Листинг кода

Программный код был написан на языке python.

```
FIRST_SYMBOL_ACII = 97
LAST_SYMBOL_ACII = 122
alphabet = {"en": 26}
IGNORE_SYMBOLS = " 1234567890-=. /[]';<>*--+|? ,!"

def caesar(message, shift):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        new_symbol = chr(FIRST_SYMBOL_ACII +
                        ((ord(symbol) - FIRST_SYMBOL_ACII + shift)
                         % alphabet["en"]))
        new_message += new_symbol
    return new_message

def atbash(message):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        new_symbol = chr(FIRST_SYMBOL_ACII +
```

```

        LAST_SYMBOL_ASCII -
        ord(symbol))

    new_message += new_symbol
return new_message

if __name__ == '__main__':
    while (True):
        code = int(input(
            "Нажмите: \n\t"
            "1 - для работы с шифром цезаря;\n\t"
            "2 - для работы с шифром атбаш;\n\t"
            "0 - для выхода из программы.\n"))
        if (code == 1):
            message = input("Введите сообщение: ")
            shift = int(input("Задайте сдвиг (от 1 до 25): "))
            result = caesar(message, shift)
            print("\nЗашифрованное сообщение (Шифр Цезаря):\n{}}"
                  .format(result))
        elif (code == 2):
            message = input("Введите сообщение: ")
            result = atbash(message)
            print("\nЗашифрованное сообщение (Шифр Атбаш):\n{}}"
                  .format(result))
        elif (code == 0):
            break
        else:
            print("Ошибка ввода!")

```

4.2 Результаты и анализ выполнения

В результате работы программы производится шифрование методом Цезаря и Атбаш. Для взаимодействия пользователя с программой был организован вывод меню в консоль для выбора пользователем алгоритма шифрования. На рис. 4.2 представлен сценарий выполнения программы шифрования Цезаря:

```
Нажмите:
  1 - для работы с шифром цезаря;
  2 - для работы с шифром атбаш;
  0 - для выхода из программы.
1
Введите сообщение: this is the 1st message!
Задайте сдвиг (от 1 до 25): 4

Зашифрованное сообщение (Шифр Цезаря):
xlmw mw xli lwx qiwweki!
```

Figure 4.2: Шифр Цезаря

Как видно на рисунке выше, на вход поступает строка, выполняется сдвиг каждой буквы этой строки на 4 символа, а знаки препинания, в свою очередь, остаются без изменений.

На рис. 4.3 представлен сценарий работы программы, если пользователь выбирает шифрование Атбаш:

```
Нажмите:
    1 - для работы с шифром цезаря;
    2 - для работы с шифром атбаш;
    0 - для выхода из программы.
2
Введите сообщение: and this is the 2nd sentence!?

Зашифрованное сообщение (Шифр Атбаш):
zmnw gsrh rh gsv 2mnw hvmgvmtxv!?
```

Figure 4.3: Шифр Атбаш

5 Выводы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрами простой замены на примере шиффов Цезаря и Атбаш.

В результате проделанной работы были реализованы методы шифрования Цезаря и Атбаш. Также были получены навыки работы с функциями преобразования строковых символов в таблицу ASCII.

Как итог, поставленные цели и задачи были успешно достигнуты.

Список литературы

1. Шифр Атбаш [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Атбаш>.
2. Шифр Цезаря [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/Шифр_Цезаря.
3. Таблица ASCII [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/ASCII>.
4. Функции ord() и chr() в Python [Электронный ресурс]. Pythonim, 2021. URL: <https://pythonim.ru/osnovy/ord-chr-python>.