Отчёт по лабораторной работе №3

Шифрование Гаммированием

Студент: Гонсалес Ананина Луис Антонио, 1032175329
Группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

List of Figures

1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать алгоритм шифрования гаммированием с конечной гаммой.

2 Теоретические сведения

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (mod). Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, 5+10 mod 4 = 15 mod 4 = 3).

В шифрах гаммирования может использоваться сложение по модулю N (общий случай) и по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию).

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы:

Ci = (Pi + Ki) mod N

Pi = (Ci + N - Ki) mod N

где Pi, Ci - i-ый символ открытого и шифрованного сообщения; N - количество символов в алфавите; Ki - i-ый символ гаммы (ключа).

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Figure 2.1: Таблица

Например, для шифрования используется русский алфавит (N = 33), открытое

сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква А будет представлена как 0, Б – 1, …, Я – 32. Результат шифрования показан в следующей таблице [1].

Символ								
	открытого сообщения, P_i	А	Б	Р	А	М	О	В
		0	1	17	0	13	15	2
	гаммы, K_i	Ж	У	Р	И	Х	И	Н
		7	20	17	9	22	9	14
	шифрограммы, C_i	Ж	Ф	Б	И	В	Ч	П
		7	21	1	9	2	24	16

Figure 2.2: Таблица2

3 Выполнение работы

```
In [21]: alpha=[chr(i) for i in range(1072,1072+34) if i!=1104]
         alphabet=alpha[:6]+[alpha[-1]]+alpha[6:-1]
         alpha

Out[21]: ['а',
          'б',
          'в',
          'г',
          'д',
          'е',
          'ж',
          'з',
          'и',
          'й',
          'к',
          'л',
          'м',
          'н',
          'о',
          'п',
          'р',
          'с',
          'т',
          'у',
          'ф',
          'х',
          'ц',
          'ч',
          'ш',
          'щ',
          'ъ',
          'ы',
          'ь',
          'э',
          'ю',
          'я',
          'ё']
```

Figure 3.1: Код

```
In [22]: index={v:k+1 for k,v in enumerate(alphabet)}
         index

Out[22]: {'а': 1,
          'б': 2,
          'в': 3,
          'г': 4,
          'д': 5,
          'е': 6,
          'ё': 7,
          'ж': 8,
          'з': 9,
          'и': 10,
          'й': 11,
          'к': 12,
          'л': 13,
          'м': 14,
          'н': 15,
          'о': 16,
          'п': 17,
          'р': 18,
          'с': 19,
          'т': 20,
          'у': 21,
          'ф': 22,
          'х': 23,
          'ц': 24,
          'ч': 25,
          'ш': 26,
          'щ': 27,
          'ъ': 28,
          'ы': 29,
          'ь': 30,
          'э': 31,
          'ю': 32,
          'я': 33}
```

Figure 3.2: Код1

```
          'я': 33}

In [30]: def gamma(message,password,m):
             message=[index[i] for i in message.lower()]
             password=[index[i] for i in password.lower()]
             print("Message: ",message)
             print("Password: ", password)

             gamma_message=[]
             for idx,char in enumerate(message):
                 cod= char + password[idx%len(password)]%m
                 gamma_message +=[cod]

             text_gamma= ''.join([alphabet[i-1] for i in gamma_message]).upper()
             return gamma_message, text_gamma

In [35]: gamma_message= gamma('приказ','гамма',33)

         Message:  [17, 18, 10, 12, 1, 9]
         Password:  [4, 1, 14, 14, 1]

In [36]: gamma_message

Out[36]: ([21, 19, 24, 26, 2, 13], 'УСЦШБЛ')

In [ ]:
```

Figure 3.3: Код2

4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал алгоритм шифрования гаммированием с конечной гаммой.

Список литературы

1. Шифры гаммирования [Электронный ресурс]. Википедия, 2021. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6.