Шифр гаммирования

НВЕ МАНГЕ ХОСЕ ХЕРСОН МИКО НКАбд-03-22

10/05/2024, Москва, Россия

Российский Университет Дружбы Народов

Информация

Информация

- НВЕ МАНГЕ ХОСЕ ХЕРСОН МИКО
- Студент, НКАбд-03-22
- Российский университет дружбы народов
- 1032225355@pfur.ru

Цели и задачи

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Выполнение лабораторной работы

Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Гаммирование

Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения ксорится с блоком криптографической гаммы, длина которого должна соответствовать длине блоков открытого сообщения. При этом, если размер блока исходного текста меньше, чем размер блока гаммы, блок гаммы обрезается до размера блока исходного текста (выполняется процедура усечения гаммы).

Алгоритм

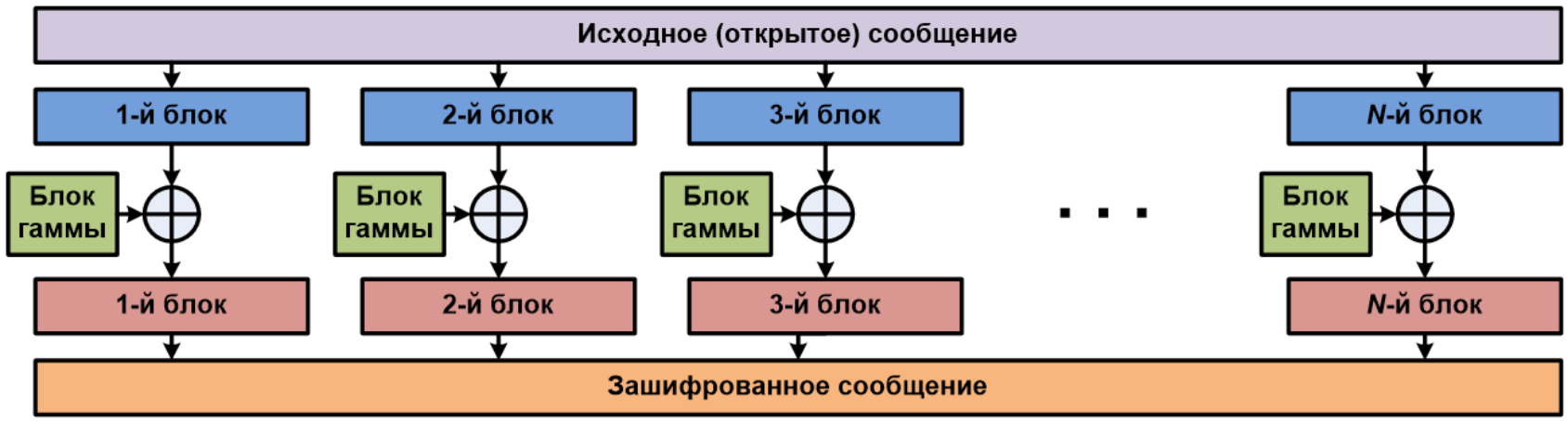

Рис. 1: Шифрование

Алгоритм

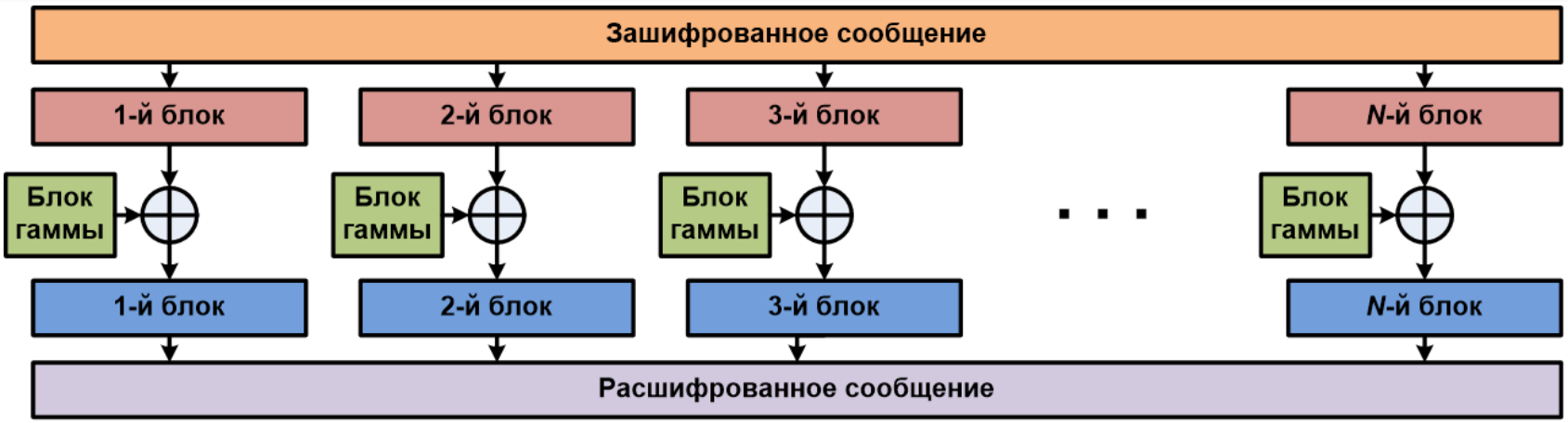

Рис. 2: Дешифровка

T	К	А	Ф	Е	Д	Р	А		С	И	С	Т	Е	М		И	Н	Ф	О	Р	М	А	Т	И	К	И
G	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И
T	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10
G	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10
T+G	31	11	36	9	21	31	20	44	33	13	35	33	25	24	48	13	31	35	35	28	28	4	36	23	31	20
mod N	31	11	36	9	21	31	20	0	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
0 →N	31	11	36	9	21	31	20	44	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20

Формула

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$Ci = (Ti + Gi) mod N$$

Пример работы алгоритма

jupyter LAB-7 (autosaved)

Logout

File Edit View Insert Cell Kernel Widgets Help

Not Trusted | Python 3 (ipykernel)

Run Code

НВЕ МАНГЕ ХОСЕ ХЕРСОН МИКО

НКАьд-03-22

ЛАВ-7

In [7]:
```
def main(text, gamma):
    dict = {"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"
            "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
            }
    dict2 = {v: k for k, v in dict.items()}
    digits_text = list()
    digits_gamma = list()

    for i in text:
        digits_text.append(dict[i])
    print("Числа текста: ", digits_text)

    for i in gamma:
        digits_gamma.append(dict[i])
    print("Числа гаммы: ", digits_gamma)

    digits_res = list()
    ch = 0
    for i in text:
        try:
            a = dict[i] + digits_gamma[ch]
        except:
            ch = 0
            a = dict[i] + digits_gamma[ch]
        if a>=33:
            a = a%33
        ch += 1
        digits_res.append(a)
    print("Числа шифровки: ", digits_res)

    text_enc = ""
    for i in digits_text:
        text_enc += dict2[i]
    print("Расшифровка: ", text_enc)
```

Пример работы программы

jupyter LAB-7 (autosaved) Logout

File Edit View Insert Cell Kernel Widgets Help Not Trusted Python 3 (ipykernel)

Run Code

```
        ch += 1
        digits_res.append(a)
    print("Числа шифровки: ", digits_res)

    text_enc = ""
    for i in digits_text:
        text_enc += dict2[i]
    print("Расшифровка: ", text_enc)

    digits = list()
    for i in text_enc:
        digits.append(dict[i])
    ch = 0
    digits1 = list()
    for i in digits:
        a = i - digits_gamma[ch]
        if a < 1:
            a = 33 + a
        digits1.append(a)
        ch += 1
    text_dec = ""
    for i in digits1:
        text_dec += dict2[i]
    print("шифровка: ", text_dec)
```

In [8]:
```
text = "ялюблюрудн"
len(text)
```

Out[8]: 10

In [9]:
```
gamma = "физматфизм"
len(gamma)
```

Out[9]: 10

In [10]:
```
main(text, gamma)
```

```
Числа текста:  [33, 13, 32, 2, 13, 32, 18, 21, 5, 15]
Числа гаммы:  [22, 10, 9, 14, 1, 20, 22, 10, 9, 14]
Числа шифровки:  [22, 23, 8, 16, 14, 19, 7, 31, 14, 29]
Расшифровка:  ялюблюрудн
шифровка:  йвхуккыйыа
```

In [ ]:

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования