Университет ИТМО
Факультет ПИиКТ
Информационная безопасность

Лабораторная работа №3
«Поточное симметричное шифрование»

Вербовой Александр
Группа P3400
Вариант 4

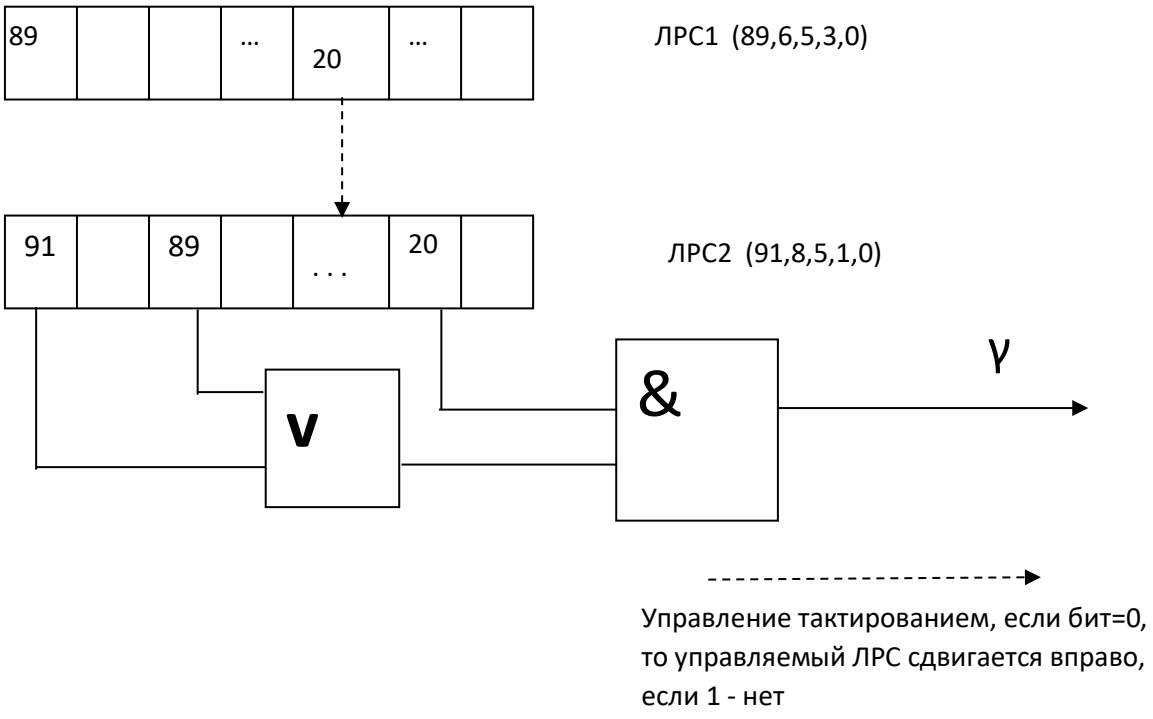
Санкт-Петербург
2021

Цель работы

изучение структуры и основных принципов работы современных алгоритмов поточного симметричного шифрования, приобретение навыков программной реализации поточных симметричных шифров

Задание (вариант 4)

4. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы РС



Описание:

```
class LRS:
    def __init__(self, textbin, n, polynom):
        self.bitlist = polynom
        self.text = self._placetext(textbin, n+1)

    # выравнивание количество сиволом к количеству разрядов ЛРС
    def _placetext(self, textbin, n):
        text = textbin[-n:]
        if len(textbin) < n:
            offset = n - len(textbin)
            rtextbin = r = ''.join(reversed(textbin))
            for i in range(offset):
                revnext = r[i % len(r)]
                text = revnext + self.text
        return text

    # сдвиг вправо и добавление бита специальных разрядов регистра
    def rotate(self):
        g = self._f()
        self.text = str(g) + self.text[:-1]

    # XOR на все специальные разряды регистра
    def _f(self):
        g = 0;
        rtext = ''.join(reversed(self.text))
        for b in self.bitlist:
            value = int(rtext[b])
            g = value ^ g
        return g

    # получение значение по разряду
    def i_bit(self, index):
        rtext = ''.join(reversed(self.text))
        return int(rtext[index])
```

```
# ввод текста для шифрования
text = str(input())
```

фенербахче

```
# бинарное представление строки
textbin = ''.join([bin(ord(c))[2:] for c in text])

l1 = LRS(textbin, 89, [0, 3, 5, 6, 89])
l2 = LRS(textbin, 91, [0, 1, 5, 8, 91])

# формирование выходной последовательности
result = ''
for _ in range(91):
    v = l2.i_bit(89) | l2.i_bit(91)
    g = l2.i_bit(20) ^ v
    result = result + str(g)
    shiftbit = l1.i_bit(20)
    if shiftbit == 1:
        l2.rotate()
    l1.rotate()
print("Для слова \"{}\" итоговым кодом будет \n {}".format(text, result))
```

Для слова "фенербахче" итоговым кодом будет
0000011110000111111000000000100000111111111111111000000111100000001
11110011101111111101111

Вывод

В ходе лабораторной работы были изучены структура и основные принципы работы современных алгоритмов поточного симметричного шифрования, приобретены навыков программной реализации поточных симметричных шифров.