Лабораторная работа №8

Элементы криптографии.
Шифрование (кодирование) различных исходных текстов одним ключом

Исаев Булат Абубакарович
Студ. Билет: 1132227131
Группа: НПИбд-01-22

Шифр гаммирования - наложение криптографической гаммы на данные для получения зашифрованных данных. Он основан на генерации гаммы шифра с помощью псевдослучайных чисел и ее наложении на открытые данные обратимым образом. Дешифрование сводится к повторной генерации гаммы шифра и ее наложению на зашифрованные данные.

Криптостойкость определяется размером ключа. Метод становится неприменимым, если известен фрагмент исходного текста и соответствующая шифрограмма. Метод с обратной связью включает генерацию гаммы с использованием контрольной суммы участка данных

Идея взлома заключается в получении открытого текста путем сравнения шифротекстов двух телеграмм, зашифрованных одним ключом. При помощи операции XOR можно найти открытый текст, зная значение шифротекстов. Предположим, что одна из телеграмм имеет фиксированный формат, известный злоумышленнику. Тогда он может определить символы открытого сообщения, находящиеся на позициях известного шаблона сообщения. Действуя поэтапно, злоумышленник может уменьшить пространство поиска открытого текста значительно

```
[10]:
a = ord("a")
liters = [chr(i) for i in range(a, a + 32)]
a = ord("0")
for i in range(a, a+10):
    liters.append(chr(i))

a = ord("A")
for i in range(1040, 1072):
    liters.append(chr(i))

P1 = "КодофаяФраза1"
P2 = "Безопасность2"

def vzlom(P1, P2):
    code = []
    for i in range(len(P1)):
        code.append(liters[(liters.index(P1[i]) + liters.index(P2[i])) % len(liters)])
    print(code)
    pr = "".join(code)
    print(pr)

[11]:
len(P1)

[11]:
13

[12]:
len(P2)

[12]:
13

[13]:
vzlom(P1, P2)

['х', 'у', 'л', 'ь', 'З', 'а', 'Ж', 'б', 'ю', 'с', 'щ', 'ь', 'Щ']
хульЗаЖбюсщьЩ
```

Рис. 1 – Код (1 часть)

```
[23]: def shifr(P1, gamma):
          dicts = {"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": 32, "А":33 , "Б": 34, "В": 35 , "Г":36,
                   "Д":37 , "Е":38 , "Ё":39 , "Ж":40 , "З":41, "И":42,"Й":43 , "К":44 , "Л":45 , "М":46 , "Н":47 , "О":48 ,
                   "П":49 , "Р":50 , "С":51 , "Т":52 , "У":53 , "Ф":54 , "Х":55 , "Ц":56 , "Ч":57 , "Ш":58,"Щ":59 , "Ъ":60 ,
                   "Ы":61 , "Ь":62 , "Э":63 , "Ю":64 , "Я":65 , "1":66 , "2":67 , "3":68 , "4":69 , "5":70 , "6":71 , "7": 72,
                   "8":73 , "9":74 , "0":75
          }

          dicts2 = {v: k for k, v in dicts.items()}
          text = P1
          digits_text = []
          digits_gamma = []

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

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

          digits_result = []
          ch = 0
          for i in text:
              try:
                  a = dicts[i] + digits_gamma[ch]
              except:
                  ch = 0
                  a = dicts[i] + digits_gamma[ch]
              if a > 75:
                  a = a%75
                  print(a)
              ch += 1
```

Рис. 2 – Код (2 часть)

```
        ch += 1
        digits_result.append(a)
    print("Числа шифротекста ", digits_result)

    text_cr = ""
    for i in digits_result:
        text_cr += dicts2[i]
    print("Шифротекст ", text_cr)

    digits = []
    for i in text_cr:
        digits.append(dicts[i])
    ch = 0
    digits1 = []
    for i in digits:
        try:
            a = i - digits_gamma[ch]
        except:
            ch = 0
            a = i - digits_gamma[ch]
        if a < 1:
            a = 75 + a
        digits1.append(a)
        ch += 1

    text_decr = ""
    for i in digits1:
        text_decr += dicts2[i]
    print("Расшифрованный текст: ", text_decr)
```

[24]:
```
P1 = "КодофаяФраза1"
gamma = "хульЗаЖбюсщьЩ"
```

[25]:
```
shifr(P1, gamma)
```

```
Числа текста  [44, 16, 5, 16, 22, 1, 32, 54, 18, 1, 9, 1, 66]
Числа гаммы  [23, 21, 13, 30, 68, 1, 40, 2, 32, 19, 27, 30, 59]
15
50
Числа шифротекста  [67, 37, 18, 46, 15, 2, 72, 56, 50, 20, 36, 31, 50]
Шифротекст  2ДрМнб7ЦРтГэР
Расшифрованный текст:  КодофаяФраза1
```

Рис. 3 – Код (3 часть)

Вывод

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.