Лабораторная работа №8

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

Кекишева Анастасия Дмитриевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

3 Теоретическое введение

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Главным образом, шифрование служит для соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма .

Как мы узнали ранее, гаммирование — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле [1].

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование)той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила: > Ci = Pi ⊠Ki,

где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й символ открытого текста, Ki — i-й символ ключа, i = 1, m. Размерности открытого текста

и ключа должны совпадать, и полученный шифротекст будет такой же длины.

Если известны шифротекст и открытый текст, то задача нахождения ключа решается через формулу, а именно, обе части равенства необходимо сложить по модулю 2 с Pi: > Ci ⊠Pi = Pi ⊠Ki ⊠Pi = Ki, > Ki = Ci ⊠Pi.

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов [2].

4 Выполнение лабораторной работы

1. Написала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования (рис. 4.1, 4.2).
   Она определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе;

```
def shifr(P1, gamma):
  dicts = {"а": 1, "б": 2, "в": 3, "г": 4, "д": 5, "е": 6, "ё": 7, "ж": 8, "э": 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
    ch += 1
    digits_result.append(a)
  print("Числа шифротекста ", digits_result)
```

Рис. 4.1: Первая часть программы

```
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)
```

Рис. 4.2: Вторая часть программы

2. Придумала гамму и запустила программу - результаты представлены на 4.3 для P1 и на 4.5 для P2.

```
[5] len(P1)

    20

[7] gamma = "во3тватартыГГГвталв12"
    len(gamma)

    20

[10] shifr(P1, gamma)

    Числа текста  [47, 1, 35, 1, 26, 10, 19, 23, 16, 5, 32, 27, 10, 11, 16, 20, 66, 75, 67, 69]
    Числа гаммы  [3, 16, 41, 20, 3, 20, 1, 18, 20, 29, 36, 36, 36, 3, 20, 1, 13, 3, 66, 67]
    Числа шифротекста  [50, 17, 1, 21, 29, 30, 20, 41, 36, 34, 68, 63, 46, 14, 36, 21, 4, 3, 58, 61]
    Шифротекст  РпауыьтЗГБЭЭМмГугвШЫ
    Расшифрованный текст  НаВашисходящийот1024
```

Рис. 4.3: Результат выполнения для P1

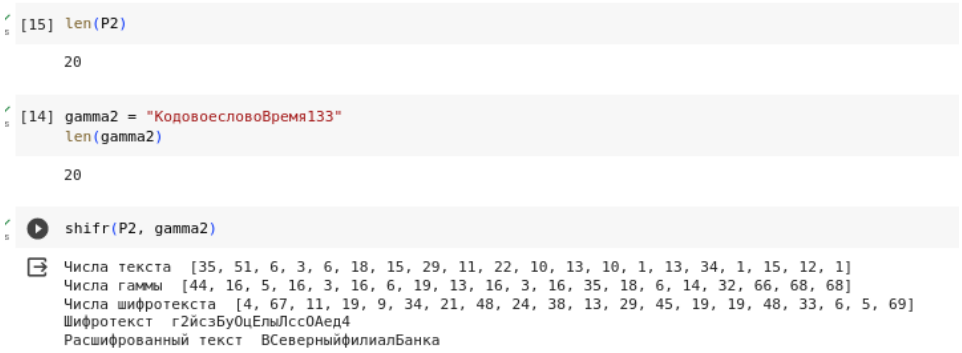

Рис. 4.4: Результат выполнения для P2

2. Определила и выразила аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить (рис. **??**).

Рис. 4.5: Вариант взлома

5 Выводы

1. Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.
2. Написала приложение, позволяющее шифровать и дешифровать тексты в режиме однократного гаммирования и определять вид шифротекстов при известном ключе.

Список литературы

1. Однократное гаммирование [Электронный ресурс]. URL: https://studfile.net/preview/272674/page:7/.
2. Лабораторная работа No 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/2090423/mod_resource/content/2/008-lab_crypto-key.pdf.