Отчет по лабораторной работе №8

Астафьева Анна Андреевна НПИбд-01-18[1]

Информационная Безопасность–2021, 18 декабря, 2021, Москва, Россия

[1]Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

Задание к лабораторной работе

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста.

Исходные данные.

Две телеграммы Центра:

P_1 = НаВашисходящийот1204

P_2 = ВСеверныйфилиалБанка

Процесс выполнения лабораторной работы

Процесс выполнения

1. Необходимо разработать приложение и определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе (рис. 1):

```
In [6]: P1='НаВашисходящийот1204'
        P2='ВСеверныйфилиалБанка'

        K='05 0c 17 7f 0e 4e 37 d2 94 10 09 2e 22 57 ff c8 0b b2 70 54'
        print('Исходные сообщения:')
        print('P1:\nшестн.: ',' '.join(to_hex(P1)),'\nсимв.:  ', '  '.join([i for i in P1]))
        print('P2:\nшестн.: ',' '.join(to_hex(P2)),'\nсимв.:  ', '  '.join([i for i in P2]))
        print('\nКлюч:\nшестн.: ',K,'\nсимв.:  ', '  '.join(to_text(K)))
        cypher_hex1, cypher1 = encryption(to_hex(P1), K.split())
        cypher_hex2, cypher2 = encryption(to_hex(P2), K.split())
        print('\nЗашифрованные сообщения:')
        print('P1:\nшестн.: ',' '.join(cypher_hex1),'\nсимв.:  ','  '.join(cypher1))
        print('P2:\nшестн.: ',' '.join(cypher_hex2),'\nсимв.:  ','  '.join(cypher2))

Исходные сообщения:
P1:
шестн.:  6d 80 62 80 98 88 91 95 8e 84 9f 99 88 89 8e 92 11 12 10 14
симв.:   Н  а  В  а  ш  и  с  х  о  д  я  щ  и  й  о  т  1  2  0  4
P2:
шестн.:  62 71 85 82 85 90 8d 9b 89 94 88 8b 88 80 8b 61 80 8d 8a 80
симв.:   В  С  е  в  е  р  н  ы  й  ф  и  л  и  а  л  Б  а  н  к  а

Ключ:
шестн.:  05 0c 17 7f 0e 4e 37 d2 94 10 09 2e 22 57 ff c8 0b b2 70 54
симв.:   %  ,  7  Я  .  n  W  R  ф  0  )  N  B  w     H  +  2  P  t

Зашифрованные сообщения:
P1:
шестн.:  68 8c 75 ff 96 c6 a6 47 1a 94 96 b7 aa de 71 5a 1a a0 60 40
симв.:   И  м  X     ц  F  &  g  :  ф  ц  7  *  ^  C  z  :     A  `
P2:
шестн.:  67 7d 92 fd 8b de ba 49 1d 84 81 a5 aa d7 74 a9 8b 3f fa d4
симв.:   З  Э  т  }  л  ^  :  i  =  д  б  %  *  W  Ф  )  л  _  z  T
```

Figure 1: Получение шифротекста сообщений

Процесс выполнения

2. Далее преположим ситуацию, что злоумышленнику каким-то образом удалось заполучить оба сообщения в зашифрованном виде (рис. 2):

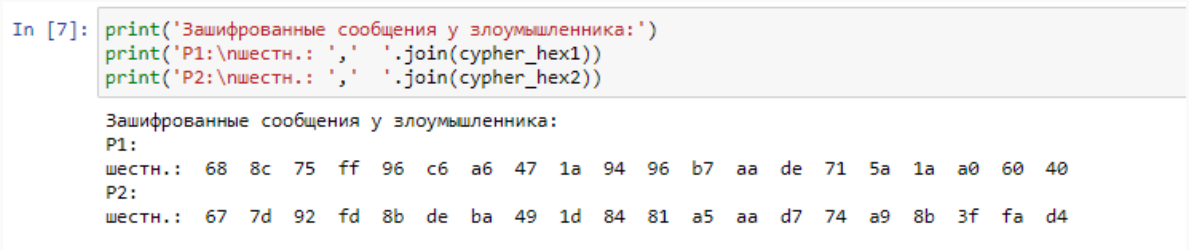

Figure 2: Злоумышленник получил шифротексты

Процесс выполнения

3. Складывая по модулю шифротексты можно получить гамму (рис. 3):

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

```
In [8]: gamma=[]
        for i in range(len(cypher1)):
            temp=hex(int(cypher_hex1[i],16)^int(cypher_hex2[i],16))[2:]
            temp = (temp, '0'+temp)[len(temp)==1]
            gamma.append(temp)
        print('Гамма:\nшестн.: ',' '.join(gamma),'\nсимв.:  ', '  '.join(to_text(' '.join(gamma))))

        Гамма:
        шестн.:  0f f1 e7 02 1d 18 1c 0e 07 10 17 12 00 09 05 f3 91 9f 9a 94
        симв.:   /  q  g  "  =  8  <  .  '  0  7  2     )  %  s  c  я  ъ  ф
```

Figure 3: Получение гаммы

Процесс выполнения

4. Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Таким образом, злоумышленник получает возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1.

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

В соответствии с логикой сообщения P_2, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P_2. Затем используется подстановка вместо P_1 полученных на предыдущем шаге новых символов сообщения P_2. И так далее.

Процесс выполнения

```
Расшифровка...

Введите известную часть сообщения, заменяя неизвестные символы вопросительным знаком (размер сообщения - 20):
НаВаш?????????от????
Номер сообщения (1 или 2):
1

Известная часть сообщения P1:
шестн.:  6d 80 62 80 98 1f 1f 1f 1f 1f 1f 1f 1f 8e 92 1f 1f 1f 1f
симв.:   H  a  B  a  ш  ?  ?  ?  ?  ?  ?  ?  ?  o  т  ?  ?  ?  ?

Расшифровываем сообщение P2:
P2 :
шестн.:  62 71 85 82 85 07 03 11 18 0f 08 0d 1f 16 8b 61 8e 80 85 8b
симв.:   B  C  e  в  e  '  #  1  8  /  (  -  ?  6  л  Б  o  a  e  л

Продолжить? (0 - нет, 1 - да)
1
Введите известную часть сообщения, заменяя неизвестные символы вопросительным знаком (размер сообщения - 20):
ВСеверный?????лБ????
Номер сообщения (1 или 2):
2

Известная часть сообщения P2:
шестн.:  62 71 85 82 85 90 8d 9b 89 1f 1f 1f 1f 1f 8b 61 1f 1f 1f 1f
симв.:   B  C  e  в  e  р  н  ы  й  ?  ?  ?  ?  ?  л  Б  ?  ?  ?  ?

Расшифровываем сообщение P1:
P1 :
шестн.:  6d 80 62 80 98 88 91 95 8e 0f 08 0d 1f 16 8e 92 8e 80 85 8b
симв.:   H  a  B  a  ш  и  c  x  o  /  (  -  ?  6  o  т  o  a  e  л

Продолжить? (0 - нет, 1 - да)
1
```

Figure 4: Взлом сообщений

Процесс выполнения

```
Введите известную часть сообщения, заменяя неизвестные символы вопросительным знаком (размер сообщения - 20):
НаВашисходящийот????
Номер сообщения (1 или 2):
1

Известная часть сообщения P1:
шестн.:  6d 80 62 80 98 88 91 95 8e 84 9f 99 88 89 8e 92 1f 1f 1f 1f
симв.:   Н  а  В  а  ш  и  с  х  о  д  я  щ  и  й  о  т  ?  ?  ?  ?

Расшифровываем сообщение P2:
P2 :
шестн.:  62 71 85 82 85 90 8d 9b 89 94 88 8b 88 80 8b 61 8e 80 85 8b
симв.:   В  С  е  в  е  р  н  ы  й  ф  и  л  и  а  л  Б  о  а  е  л

Продолжить? (0 - нет, 1 - да)
1
Введите известную часть сообщения, заменяя неизвестные символы вопросительным знаком (размер сообщения - 20):
ВСеверныйфилиалБанка
Номер сообщения (1 или 2):
2

Известная часть сообщения P2:
шестн.:  62 71 85 82 85 90 8d 9b 89 94 88 8b 88 80 8b 61 80 8d 8a 80
симв.:   В  С  е  в  е  р  н  ы  й  ф  и  л  и  а  л  Б  а  н  к  а

Расшифровываем сообщение P1:
P1 :
шестн.:  6d 80 62 80 98 88 91 95 8e 84 9f 99 88 89 8e 92 11 12 10 14
симв.:   Н  а  В  а  ш  и  с  х  о  д  я  щ  и  й  о  т  1  2  0  4

Продолжить? (0 - нет, 1 - да)
0
```

Figure 5: Взлом сообщений

Контрольные вопросы

Контрольные вопросы

1. Как, зная один из текстов (P_1 или P_2), определить другой, не зная при этом ключа?
2. Что будет при повторном использовании ключа при шифровании текста?
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Выводы по проделанной работе

Вывод

На основе проделанной работы освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.