Отчет по лабораторной работе №8

Информационная безопасноть

Астафьева Анна Андреевна НПИбд-01-18

Содержание

# Цель работы

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

# Теоретическое описание

Исходные данные.  
Две телеграммы Центра:

= НаВашисходящийот1204

= ВСеверныйфилиалБанка

Ключ Центра длиной 20 байт:  
 = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем

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 , которые находятся на позициях известного шаблона сообщения .

В соответствии с логикой сообщения , злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения . Затем используется подстановка вместо полученных на предыдущем шаге новых символов сообщения . И так далее.  
Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

# Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста.  
Исходные данные.  
Две телеграммы Центра:

= НаВашисходящийот1204

= ВСеверныйфилиалБанка

1. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты и в режиме однократного гаммирования. Приложение должно определить вид шифротекстов и обоих текстов и при известном ключе ;

Используем функции из лабораторной работы №7:

1.1. Функция *encryption* с помощью однократного гаммирования из сообщения и ключа получает шифротекст (рис. 1).

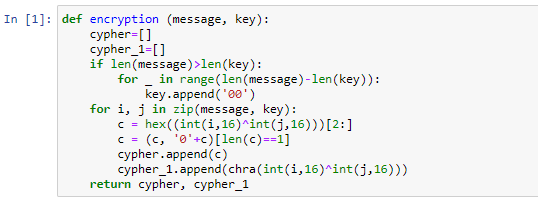


Figure 1: Код функции *encryption*

1.2. Функция *to\_hex*, трансформирующая текст в шестнадцатиричное представление (рис. 2).

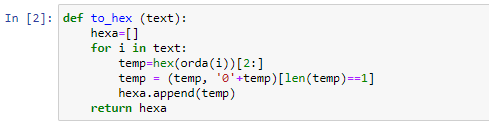


Figure 2: Код функции *to\_hex*

Написаны еще несколько функций:

1.3. Функция *to\_text*, трансформирующая текст в шестнадцатиричном представлении в символьное (рис. 3)

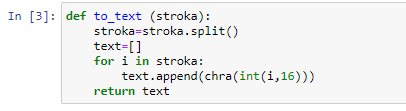


Figure 3: Код функции *to\_text*

1.4. Функция *chra*, преобразовывающая число в символ (рис. 4)

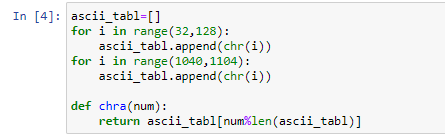


Figure 4: Код функции *chra*

1.5. Функция *orda*, преобразовывающая символ в число (рис. 5)

Figure 5: Код функции orda

Figure 5: Код функции *orda*

Шифруем оба сообщения (рис. 6):

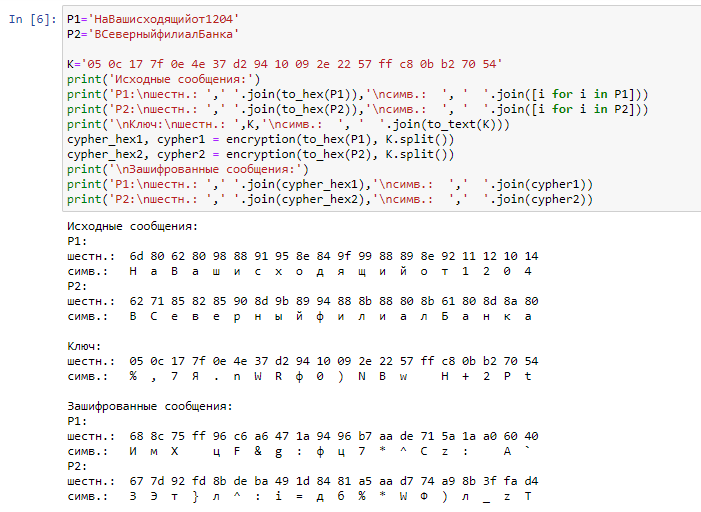


Figure 6: Получение шифротекста сообщений

1. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Далее преположим ситуацию, что злоумышленнику каким-то образом удалось заполучить оба сообщения в зашифрованном виде (рис. 7):

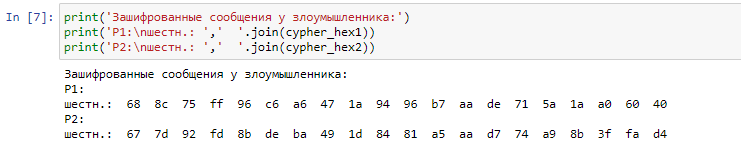


Figure 7: Злоумышленник получил шифротексты

Складывая по модулю шифротексты можно получить гамму (рис. 8):

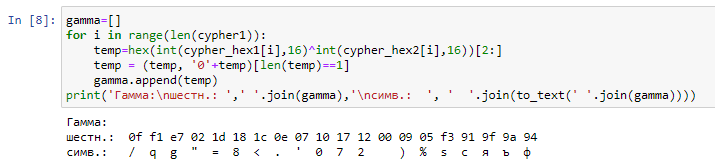


Figure 8: Получение гаммы

Допустим, одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику известен формат телеграммы . Ему известны в телеграмме P\_1 выделенны жирным части:  
 = **НаВаш**исходящий**от**1204.  
Таким образом, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения :  
 = **ВСеве**рныйфилиа**лБ**анка.  
В соответствии с логикой сообщения , злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения :  
 = **ВСеверный**филиа**лБ**анка.  
Затем используется подстановка полученных на предыдущем шаге новых символов сообщения . И так далее.  
Работа описанного выше алгоритма реализована в программе (рис. 9), (рис. 10), (рис. 11).

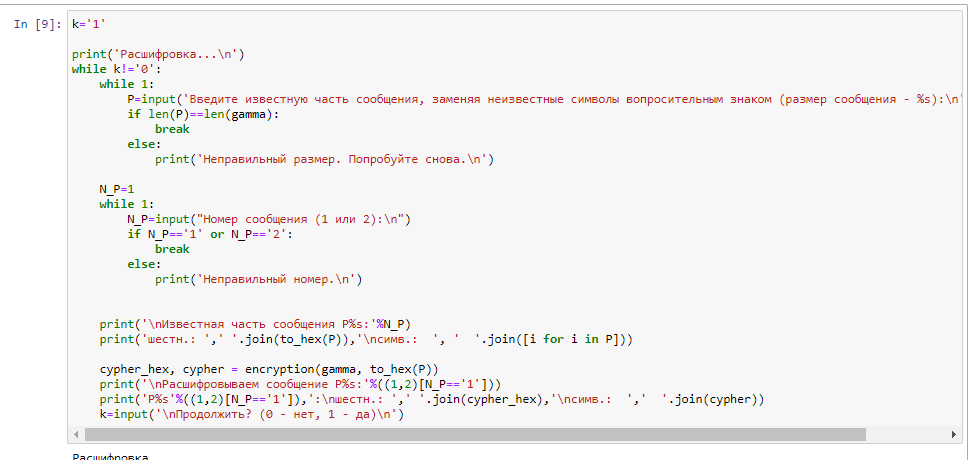


Figure 9: Взлом сообщений

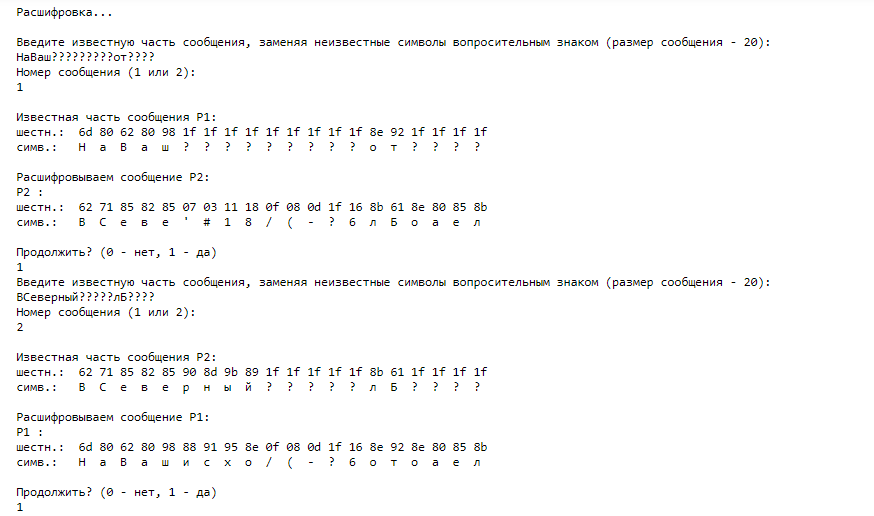


Figure 10: Взлом сообщений

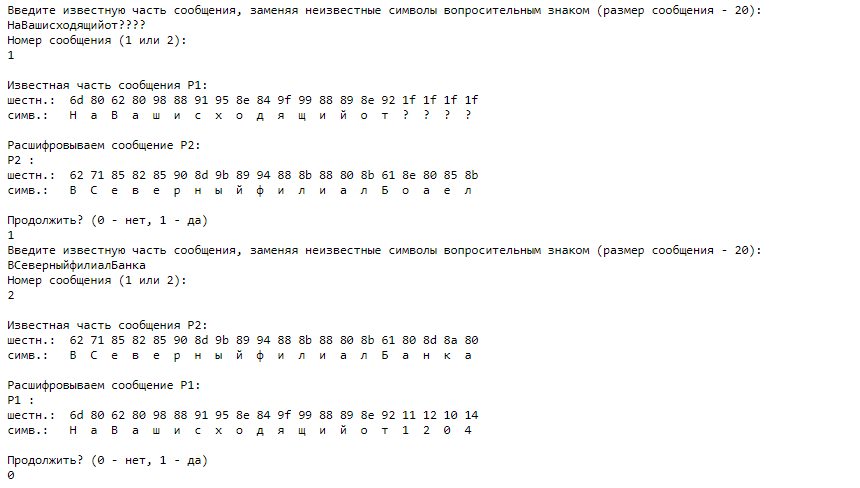


Figure 11: Взлом сообщений

# Контрольные вопросы

1. Как, зная один из текстов ( или ), определить другой, не зная при этом ключа?  
   По формуле
2. Что будет при повторном использовании ключа при шифровании текста?  
   Текст расшифруется.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?  
   по формулам режима однократного гаммирования:
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

* ключ, попав не в те руки, даст возможность злоумышленнику расшифровать оба текста;
* можно расшифровать с помощью открытого текста другие известные шифротексты;
* можно узнать часть текста, используя заранее известный шаблон и формат другого текста.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

* скорость шифрования выше;
* простой алгоритм шифрования;
* шифротекст сильно меняется, если изменяется ключ или открытый текст.

# Выводы

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