Лабораторная №8

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Освоение на практике применения 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 Выполнение лабораторной работы

Для выполнения данной лабораторной работы воспользуемся программой, написанной в предыдущей лабораторной работе №7. Зашифруем исходные сообщения, предварительно сгенерировав ключ(рис. 1).

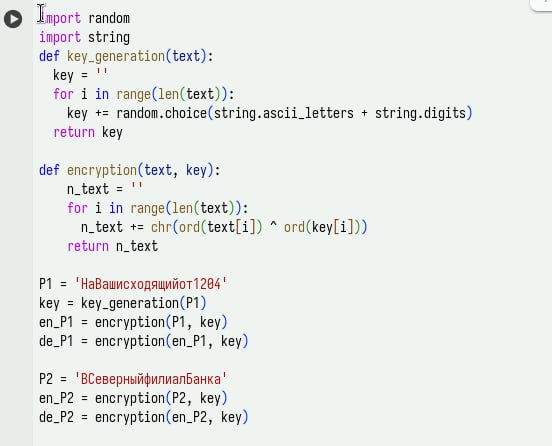


Рис. 1: Сообщения 1 и 2

Затем сгенерируем шифротекст, посмотрим на вывод программы. Также выполним задание и расшифруем сообщение 1 за счет сообщения 2 и наоборот(для этого также используем сложение по модулю 2)(рис. 2).



Рис. 2: Расшифровка сообщений

Посмотрим на вывод программы - все проеобразования прошли успешно(рис. 3).

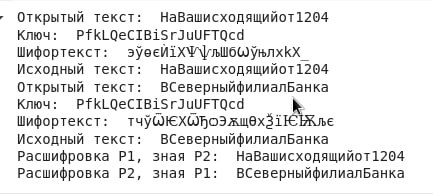


Рис. 3: Вывод программы

# 4 Листинг и вывод

import random  
import string  
def key\_generation(text):  
 key = ''  
 for i in range(len(text)):  
 key += random.choice(string.ascii\_letters + string.digits)  
 return key  
  
def encryption(text, key):  
 n\_text = ''  
 for i in range(len(text)):  
 n\_text += chr(ord(text[i]) ^ ord(key[i]))  
 return n\_text  
  
P1 = 'НаВашисходящийот1204'  
key = key\_generation(P1)  
en\_P1 = encryption(P1, key)  
de\_P1 = encryption(en\_P1, key)  
  
P2 = 'ВСеверныйфилиалБанка'  
key = key\_generation(P2)  
en\_P2 = encryption(P2, key)  
de\_P2 = encryption(en\_P2, key)  
  
print("Открытый текст: ", P1, "\nКлюч: ", key, "\nШифортекст: ", en\_P1, "\nИсходный текст: ", de\_P1)  
print("Открытый текст: ", P2 ,"\nКлюч: ", key ,"\nШифортекст: ", en\_P2 ,"\nИсходный текст: ", de\_P2)  
  
encr = encryption(de\_P1, de\_P2)  
print("Расшифровка Р1, зная Р2: ", encryption(P2, encr))  
print("Расшифровка Р2, зная Р1: ", encryption(P1, encr))

Вывод:

Открытый текст: НаВашисходящийот1204

Ключ: PfkLQeCIBiSrJuUFTQcd

Шифортекст: эўѳєЍїХѰѱљШбѠўњлxkX\_

Исходный текст: НаВашисходящийот1204

Открытый текст: ВСеверныйфилиалБанка

Ключ: PfkLQeCIBiSrJuUFTQcd

Шифортекст: тчўѾѤХѾЂѻЭѫщѲхѮїѤѬљє

Исходный текст: ВСеверныйфилиалБанка

Расшифровка Р1, зная Р2: НаВашисходящийот1204

Расшифровка Р2, зная Р1: ВСеверныйфилиалБанка

# 5 Ответы на контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Если один и тот же ключ (K) был использован для шифрования двух открытых текстов (P1 и P2) с помощью однократного гаммирования, то:

• C1 = P1 XOR K • C2 = P2 XOR K

Зная C1 и C2, можно вычислить:

• C1 XOR C2 = (P1 XOR K) XOR (P2 XOR K) = P1 XOR P2 (Ключ K исключается)

Теперь, зная P1 (один из открытых текстов), можно вычислить P2:

• P2 = (P1 XOR C1 XOR C2) или P2 = (C1 XOR C2) XOR P1

1. Что будет при повторном использовании ключа при шифровании текста?

Повторное использование ключа при шифровании однократным гаммированием позволяет злоумышленнику, имеющему доступ к шифротекстам и знающему часть одного из открытых текстов, восстановить другой открытый текст. Однократное гаммирование перестаёт быть однократным, и перестаёт быть безопасным.

1. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?
2. Сгенерировать случайный ключ K длиной, равной длине самого длинного из двух открытых текстов (P1 и P2).
3. Шифровать первый открытый текст: C1 = P1 XOR K
4. Шифровать второй открытый текст: C2 = P2 XOR K
5. Перечислите недостатки шифрования одним ключом двух открытых текстов.

• Отсутствие безопасности: Зная один открытый текст и оба шифротекста, можно восстановить второй открытый текст. • Возможность восстановления ключа: При наличии достаточного количества информации о открытых текстах или их структуре, возможна частичная или полная дедукция ключа. • Уязвимость к частотному анализу: Если открытые тексты имеют предсказуемые элементы или повторяющиеся фрагменты, это упрощает криптоанализ. • Нарушение принципа однократного использования: Главный принцип OTP - однократное использование ключа - полностью нарушен, что делает систему эквивалентной намного более слабым шифрам.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Их нет. Использование одного ключа для шифрования нескольких сообщений с помощью однократного гаммирования - это серьезная ошибка, которая делает шифр абсолютно небезопасным. Нет никаких ситуаций, когда это было бы оправдано.

# 6 Выводы

В ходе работы было произведено повторное знакомство с элементами криптографии, произведена шифровка и дешифровка даннных с помощью ключа, расшифровка сообщений, закодированных одним ключом без ключа, зная только сообщения

# Список литературы

* [ТУИС](https://esystem.rudn.ru/pluginfile.php/2580990/mod_resource/content/2/008-lab_crypto-key.pdf)