Отчёт по лабораторной работе N8

Основы информационной безопасноти

Соловьев Богдан НКАбд-04-23

Содержание

Цель работы

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

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.

Выполнение лабораторной работы

вот листинг программы:

```
def generate_key(length):
  return "".join(random.choice(string.ascii_letters + string.digits) for _ in range(length))

def xor(text, key):
  return "".join(chr(ord(text[i]) ^ ord(key[i % len(key)])) for i in range(len(text)))

P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
key_length = max(len(P1), len(P2))
key = generate_key(key_length)

print(key, "\n")

C1 = xor(P1, key)
C2 = xor(P2, key)
```

```
print(C1, "\n", C2, "\n")

P1 = xor(C1, key)
P2 = xor(C2, key)

print(P1, "\n", P2)
```

вывод:

```
n0Q684e0XGuIDWKGXfW1

өÈyIΨЌΦvMөкÈÕ3vSiTg
 ÕБЌЄЙVjowѓэӨÕлΨiЏЋЊЁ

НаВашисходящийот1204
 ВСеверныйфилиалБанка
```

Однократное гаммирование реализовано через логическую оперцаию XOR между ключём и текстом, поэтому имея зашифрованные тексты и 1 из открытых текстов, можно расшифпрваит все тексты, зашифрованные этим ключём

Дополнительное задание

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

- Для определения второго текста можно взять зашифрованные тексты и выполнить над ними операцию C1 xor C2, потом применить xor к ним и известному тексту C1 xor C2 xor P1 = P2

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

- Получится дешифрованный текст

3. Как реализуется режим шифрования однократного гаммирования одним
   ключом двух открытых текстов?

- (Бит текста) xor (бит ключа)

4. Перечислите недостатки шифрования одним ключом двух открытых
   текстов.

- Легко прочитать все тексты, зная открытый текст или ключ

5. Перечислите преимущества шифрования одним ключом двух открытых
текстов.

- Быстро, всего один ключ

Выводы

Я научился однократному гаммированию