

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

Жижченко Валерия Викторовна

Российский Университет Дружбы Народов

Цель лабораторной работы

Цель лабораторной работы

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

Выполнение работы

Разработали приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение определяет вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе.

Выполнение работы

1. Вывод работы программы:

```
lera@LAPTOP-H4VNRN0T:~/18/lab8$ ./a.out
P1: Как ваши дела?
P2: Как вас зовут?
C1: QpW5B{hx!4PA3T
C2: QpW5B{rB@!>Qy2)JT

C1 hex:
0x51  0x70  0xb5  0x9c  0x1b
0x52  0x80  0x57  0xf4  0x73
0x4   0xf0  0x7b  0x68  0x78
0xd7  0x21  0x34  0x90  0xe9
0x50  0x41  0x33  0x1b  0x4a
0x54

C2 hex:
0x51  0x70  0xb5  0x9c  0x1b
0x52  0x80  0x57  0xf4  0x73
0x4   0xf0  0x72  0x98  0x10
0x40  0x21  0x3e  0x90  0xee
0x51  0x79  0x32  0x29  0x4a
0x54

Key:
0x81  0xea  0x65  0x2c  0xcb
0xe8  0xa0  0x87  0x46  0xa3
0xb4  0x21  0xf3  0xb8  0xc0
0xf7  0xf1  0x80  0x40  0x5c
0x80  0xfa  0xe3  0xab  0x75
0x54

Decrypted P2: Как вас зовут?
```

Figure 1: Вывод программы

Ответы на контрольные вопросы

1. Как, зная один из текстов (P_1 или P_2), определить другой, не зная при этом ключа?

Необходимо воспользоваться формулой:

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

где C_1 и C_2 – шифротексты.

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

Тогда мы получим исходное сообщение.

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

Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K,$$

где C_i – шифротексты, P_i – открытые тексты, K – ключ шифрования.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

- Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа.
- Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения P_2 , которые находятся на позициях известного шаблона сообщения P_1 .

- В соответствии с логикой сообщения P_2 , злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P_2 . Таким образом, применяя формулу из п. 1, с подстановкой вместо P_1 полученных на предыдущем шаге новых символов сообщения P_2 злоумышленник если не прочитает оба сообщения, то значительно уменьшит пространство их поиска. Наконец, зная ключ, злоумышленник сможет расшифровать все сообщения, которые были закодированы при его помощи.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных.

Вывод

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