

Лабораторная работа № 8

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

Аксёнова Алина Владимировна

Содержание

| | |
|-------------------------------|----|
| Цель работы | 5 |
| Задание | 6 |
| Теоретическое введение | 7 |
| Ход работы | 8 |
| Ответы на контрольные вопросы | 10 |
| Выводы | 11 |
| Библиографический список | 12 |

List of Figures

| | | |
|-----|--|---|
| 0.1 | Импорт библиотек и написание функций | 8 |
| 0.2 | Шифрование открытого текста | 8 |
| 0.3 | Определение открытых текстов | 9 |

List of Tables

Цель работы

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

Задание

Прочитать оба текста, не зная ключа и не стремясь его определить

Теоретическое введение

С точки зрения теории криптоанализа, метод шифрования однократной случайной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым (далее для краткости авторы будут употреблять термин “однократное гаммирование”, держа в уме все вышесказанное). Обоснование, которое привел Шеннон, основываясь на введенном им же понятии информации, не дает возможности усомниться в этом - из-за равных априорных вероятностей криптоаналитик не может сказать о дешифровке, верна она или нет. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько нибудь поправить положение - информация о вскрытом участке гаммы не дает информации об остальных ее частях.

Ход работы

1. Импортируем все необходимые библиотеки и пишем функцию генерирования ключа, а также функцию гаммирования. (Рис. 0.1).

```
In [2]: 1 import random
        2 import string

In [11]: 1 def generate_key(length, symbols = string.ascii_letters + string.digits):
        2     return ''.join(random.choice(symbols) for i in range(length))
        3 def gamming(text, key):
        4     text_conv = [ord(i) for i in text]
        5     key_conv = [ord(i) for i in key]
        6     return ''.join(chr(a ^ b) for a, b in zip(text_conv, key_conv))
```

Figure 0.1: Импорт библиотек и написание функций

2. Генерируем случайный ключ, а затем определяем вид шифротекстов C1 и C2 при известном ключе и известном открытом тексте. (Рис. 0.2).

```
In [4]: 1 P1 = 'НаВашисходящийот1204'
        2 P2 = 'ВСеверныйфилиалБанка'
        3 key = generate_key(len(P1))
        4 C1 = gmming(P1, key)
        5 C2 = gmming(P2, key)
        6 print('C1:', C1)
        7 print('C2:', C2)
```

C1: зйЫьЕОЖУжейЮяЯгRv
C2: QыЙjтjбхшкPЗлвнUуQьГfЕ

Figure 0.2: Шифрование открытого текста

3. Применяем функцию “gamming” к полученным шифрам, а затем еще и к одному из открытых текстов, чтобы получить другой, неизвестный открытй текст (Рис. 0.3).


```
In [11]: 1 summa = gamming(C1, C2)
          2 P2_uncyfered = gamming(summa,P1)
          3 print(P2_uncyfered)
```

ВСеверныйфилиалБанка

```
In [13]: 1 summa = gamming(C1, C2)
          2 P1_uncyfered = gamming(summa,P2)
          3 print(P1_uncyfered)
```

НаВашисходящийот1204

Figure 0.3: Определение открытых текстов

Ответы на контрольные вопросы

1. Необходимо прогаммировать один шифротекст вторым, а после прогаммировать результат одним из исходных текстов. Таким образом мы получим другой исходный текст.
2. Мы из зашифрованного текста обратно получим исходный незашифрованный..
3. Поочередно зашифруем каждый текст одним ключом.
4. Подверженность взлому, шифр становится абсолютно взламываемым. При утечке же хотя бы части одного из исходных текстов злоумышленник сможет расшифровать все тексты.
5. Можно сократить издержки по доставке ключей сторонам, либо вообще исключить их, если ключ использовать все время.

Выводы

В результате выполнения данной работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.
2. Алексеев, М. Е. Шифрование методом гаммирования / М. Е. Алексеев // 70-я научно-техническая конференция учащихся, студентов и магистрантов, 15-20 апреля 2019 г., Минск : сборник научных работ : в 4 ч. Ч. 4. - Минск : БГТУ, 2019. - С. 398-401.
3. Прикладные задачи шифрования [Электронный ресурс]. – Режим доступа : <http://citforum.ru/internet/securities/cryptobook07.shtml>, свободный. – Загл. с экрана.
4. Шифры гаммирования [Электронный ресурс]. – Режим доступа : https://bstudy.net/825827/tehnika/shifry_gammirovaniya, свободный. – Загл. с экрана.