

Лабораторная работа №7. Элементы криптографии. Однократное гаммирование

Евдокимов Иван Андреевич. НФИбд-01-20

20 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цель лабораторной работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования.


Процесс выполнения лабораторной работы

1. Вывод запуска программы 1

```
Z:\учёба\ИНФ06ез\lab7_code\venv\Scripts\python.exe Z:\учёба\ИНФ06ез\lab7_code\main.py
Введите открытый текст: С Новым Годом, друзья!
Ключ: а1еътйьвтлфбее19иџ1ашх
Ключ в 16 бит: 430 31 435 44а 442 439 44с 432 442 43b 444 431 435 435 31 39 436 444 31 430 449 445
Зашифрованный текст: —(tprpBQ~p~ й~йv~I|~Е
Зашифрованный текст в 16 бит: 11 11 28 74 70 72 70 412 51 5 70 f 9 419 11 40d 76 7 406 7с 6 404
Расшифрованный текст: С Новым Годом, друзья!
```

Рис. 2: шифровка и дишифровка текста

2. Вывод запуска программы 2



Введите фрагмент открытого текста: *Новым*
Возможные ключи для шифротекста: ['КЯКП']


Рис. 3: шифровка фрагмента текста

3. Вывод запуска программы 3 на английском

```
Z:\учёба\инфо06ез\lab7_code\venv\Scripts\python.exe Z:\учёба\инфо06ез\lab7_code\main.py
Введите открытый текст: Hello World!
Ключ: ссрйзъэсуя0я
Ключ в 16 бит: 441 441 440 439 437 44а 44d 441 443 44f 30 44е
Зашифрованный текст: MФbsjzK06YTЃ
Зашифрованный текст в 16 бит: 409 424 42c 455 458 46а 41а 42е 431 423 54 46f
Расшифрованный текст: Hello World!
```

Рис. 4: шифровка и дишифровка текста

4. Вывод запуска программы 4 на английском



```
Введите фрагмент открытого текста: World  
Возможные ключи для шифротекста: ['ЩеуЧдЎ']
```

Рис. 5: шифровка фрагмента текста

Контрольные вопросы

Контрольные вопросы

1. Поясните смысл однократного гаммирования. Ответ: это шифрование симметричным методом, сущность которого заключается в «наложении» последовательности, сформированной из случайных чисел, на открытый текст. Прощё говоря это шифрование где количество символов совпадает в ключе и тексте совпадает и без ключа нельзя однозначно декодировать текст обратна. С моей точки зрения это аналог принципа шифрование в знаменитой Энигме, но с случайными символами в ключе.
2. Перечислите недостатки однократного гаммирования. Ответ: Необходимо передавать ключ с словом так как его невозможно создать заранее, а также сложность обмена ключами в большой системе и вероятность его повреждение что сразу сделает дешифровку

3. Перечислите преимущества однократного гаммирования. Ответ: Простой и одинаковый процесс кодирования и декодирования, единый ключ для шифровки и дешифровки, скорость обработки и передачи так как требуется лишь текст и его ключ.
4. Почему длина открытого текста должна совпадать с длиной ключа? Ответ: Так как при кодирование элемент ключа закрепляется за соответствующим элементом сообщения из-за чего и возможна однозначна декадировать сообщение.

Контрольные вопросы

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? Ответ:
Фактически ответ содержится в одном из названий этого принципа “Шифр XOR”, то есть в его основе находится строгая дизъюнкция которая и принимает в себя случайный ключ и текст и обратно “отзеркаливает” если вернуть зашифрованный текст вместе с ключём.
6. Как по открытому тексту и ключу получить шифротекст? Ответ: Для получения шифротекста применяем операцию исключающего ИЛИ (XOR) между каждым символом открытого текста и соответствующим символом ключа. Процесс можно построить следующим образом: открытый текст и ключ в виде последовательности байтов или символов; поэлементно выполняем операцию XOR с открытого текста и ключа;

Контрольные вопросы

7. Как по открытому тексту и шифротексту получить ключ? Ответ: Соответственно онологичная процедура из 6 пункта, так как процесс кодирования и декадирования одинаковы.
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Ответ: Определить это можно проведя проверку через “Доказательство абсолютной стойкости Шеннона” (в основе которого лежит принцип абсолютной стойкости шифра — шифр, характеризующийся тем, что криптоаналитик принципиально не сможет извлечь статистическую информацию относительно выбираемых ключей из перехватываемого шифротекста.). Так Клод Шеннон доказал, что при определённых свойствах гаммы этот метод шифрования является абсолютно стойким (гамма

Выводы:

Выводы:

Мною были освоино на практике применение режима однократного гаммирования.