

**Министерство цифрового развития, связи и массовых  
коммуникаций Российской Федерации**

**ФГБОУ ВО «Санкт-Петербургский государственный университет  
телекоммуникации им. проф. М.А. Бонч-Бруевича»**

---

Кафедра защищенных систем связи

Дисциплина «Основы криптографии»

**Лабораторная работа № 11  
«Исследование безусловно стойкой аутентификации сообщений на  
основе строго-универсальных хэш-функций»**

Выполнила:

ст. гр. ИКТЗ-83

Громов А.А.

Вариант 4

Проверил:

Яковлев В. А.

---

Санкт-Петербург

**Цель работы:**

Закрепить знания, полученные в лекционном курсе “Основы криптографии”, по разделу “Аутентификация сообщений”.

**Используемое программное обеспечение:**

Для работы используется программа Project2.exe

**Ход работы****1. Моделирование способа формирования аутентификатора на основе строго универсальных хэш-функций**

1. Аутентификатор для двоичного сообщения  $M$  на основе строго универсальных хэш-функций по алгоритму  $E_S = [M * K_0 + K_1]_b$ ,

$$M = 4 \bmod 15 = 4_{10} = 0100_2$$

$$K_0 = 0101$$

$$K_1 = 1100$$

$$E_S = [M * K_0 + K_1]_b = [0100 * 0101 + 1100]_b$$

Вычисления в поле  $GF(2^4)$  проводить по модулю неприводимого многочлена  $h(x) = x^4 + x + 1$ ,  $b=4$ .

$$E_S = [0100 \overset{1}{\cdot} 0101 \overset{2}{+} 1100]_b$$

$$1) 0100 \cdot 0101 = x^2 \cdot (x^2 + 1) = x^4 + x^2$$

$$\begin{array}{r|l} x^4 + x^2 & x^4 + x + 1 \\ - x^4 + x + 1 & 1 \\ \hline x^2 + x + 1 & \end{array}$$

$$2) 011 + 1100 = 1011_2 = 11_{10}$$

$$E_S = 1011$$

2. Рассчитать для  $b=4$  и  $b=3$ :

- общее количество хэш-функций в заданном классе -  $|H|$  ;  
для этого нам необходимо посчитать количество комбинаций  
подключей  $h_0$  и  $h_1$ .  
 $|H| = 16 * 16 = 256$
- количество хэш-функций, отображающих  $M$  в  $E_s$  -  $|H'|$  ;  
 $|H'| = |H|/|E_s| = |H|/2^b$   
При  $b = 4$ :  $|H'| = 256/2^4 = 16$   
При  $b = 3$ :  $|H'| = 256/2^3 = 32$
- количество хэш-функций, отображающих  $M$  в  $E_s$  и  $M'$  в  $E's$   $M \neq M'$  -  
 $|H''|$ .  
 $|H''| = |H|/|E_s|^2$   
При  $b = 4$ :  $|H''| = 256/16^2 = 1$   
При  $b = 3$ :  $|H''| = 256/8^2 = 4$

## 2 часть

### Исследование безусловно стойкой системы аутентификации на основе строго универсальных хэш-функций

1. Задаём произвольное сообщение и ключ, вычисляем аутентификатор и находим все возможные ключи.

Однократная передача

Аутентификация

Сообщение M (8 бит):  
01000100

Ключ K (16 бит):  
0100010001000100

Определить идентификатор

Идентификатор Es (b бит):  
10011001

Найти все ключи K=(M,Es)

Ключи K=(M,Es):

1110111101000111
1111000010101000
1111000111101100
1111001000100000
1111001101100100
1111010010100101
1111010111100001
1111011000101101
1111011101101001
1111100010110010
1111100111110110
1111101000111010
1111101101111110
1111110010111111
1111110111111011
1111111000110111
1111111101110011

Всего ключей: 256

2. Выбираем случайный ключ из полученного множества и для произвольно введённого ложного сообщения вычисляем фальшивый аутентификатор.

Сообщение  $M'$  (8 бит):

Ключ  $K'$  (16 бит):

Идентификатор  $E s'$  (b бит):

3. Используя поле «Верификация» проверяем, будет ли подделка обнаружена для ложного сообщения и фальшивого аутентификатора на ключе законного пользователя.

Верификация

Сообщение (8 бит):

Ключ (16 бит):

Идентификатор (b бит):

Верификация не удалась

Видим, что верификация не удалась.

4. Используя кнопку «Атака на ключ», наблюдаем множество всех ключей, при угадывании которых злоумышленник выполнит необнаруженную подделку.

Ключи  $K=(M, E s, M', E s')$ :

Всего ключей: 1

Вероятность угадать  $K=(M, E s, M', E s')$ :  
 $P = 0,00390625$

Убедимся, что расчёт вероятности выполнен верно

Выберем один из найденных ключей и убедимся, что его использование, действительно, приводит к обнаружению навязывания.

5. Повторяем предыдущие пункты для  $b = 7$ .

Расчёт вероятности  $P = |H''|/|H'| = 4/512 = 0,0078125$

6. Выбираем режим Многократная передача. Установим длину аутентификатора  $b = 6$  и при случайном генерировании сообщений для

произвольно выбранного ключа, находим минимальное число передач, при котором злоумышленник выполнит подделку любого выбранного сообщения с вероятностью 1. Проверим, что, действительно, любой из множества ключей  $K = [M_i, E_{Si}, M', E_S]$  дает правильную верификацию.

Многократные передачи

Аутентификация

Сообщения  $M_i$  (8 бит):

01010011  
10110010  
11011000

Всего сообщений: 3

☐ Задать сообщения вручную:

Сообщение  $M$  (8 бит):

Добавить сообщение

☒ Сгенерировать сообщения

Количество передач  $L$  (1-20):

3

Сгенерировать случайно

Очистить поле сообщений

Ключ  $K$  (16 бит):

0100010001000100

Расчёт идентификаторов

Идентификаторы  $E_{Si}$  (b бит):

011011  
001011  
000001

Всего идентификаторов: 3

Определить общие ключи

Общие ключи  $K=(M_i, E_{Si})$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Сообщение  $M'$  (8 бит):

00010010

Ключ  $K'$  (16 бит):

0100010001000111

Определить идентификатор

Идентификатор  $E_{S'}$  (b бит):

111110

Атака на ключ

Ключи  $K=(M_i, E_{Si}, M', E_{S'})$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Вероятность угадать  $K=(M_i, E_{Si}, M', E_{S'})$ :

$P = 1$

Верификация

Сообщение (8 бит):

00010010

Ключ (16 бит):

0100010001000111

Идентификатор (b бит):

111110

Произвести верификацию

Верификация прошла успешно

Разрядность  $b$  (4 - 8):

6

Запомнить  $b$

Очистить всё

ВЫХОД

Многократные передачи

Аутентификация

Сообщения  $M_i$  (8 бит):

01010011  
10110010  
11011000

Всего сообщений: 3

☐ Задать сообщения вручную:

Сообщение  $M$  (8 бит):

Добавить сообщение

☒ Сгенерировать сообщения

Количество передач  $L$  (1-20):

3

Сгенерировать случайно

Очистить поле сообщений

Ключ  $K$  (16 бит):

0100010001000100

Расчёт идентификаторов

Идентификаторы  $E_{Si}$  (b бит):

011011  
001011  
000001

Всего идентификаторов: 3

Определить общие ключи

Общие ключи  $K=(M_i, E_{Si})$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Сообщение  $M'$  (8 бит):

00010010

Ключ  $K'$  (16 бит):

0100010001000111

Определить идентификатор

Идентификатор  $E_{S'}$  (b бит):

111110

Атака на ключ

Ключи  $K=(M_i, E_{Si}, M', E_{S'})$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Вероятность угадать  $K=(M_i, E_{Si}, M', E_{S'})$ :

$P = 1$

Верификация

Сообщение (8 бит):

00010010

Ключ (16 бит):

0100010001000100

Идентификатор (b бит):

111110

Произвести верификацию

Верификация прошла успешно

Разрядность  $b$  (4 - 8):

6

Запомнить  $b$

Очистить всё

ВЫХОД

Многократные передачи

Аутентификация

Сообщения  $M_i$  (8 бит):

01010011  
10110010  
11011000

Всего сообщений: 3

☐ Задать сообщения вручную:

Сообщение  $M$  (8 бит):

☒ Сгенерировать сообщения

Количество передач  $L$  (1-20):

3

Ключ  $K$  (16 бит):

0100010001000100

Идентификаторы  $Esi$  (b бит):

011011  
001011  
000001

Всего идентификаторов: 3

Общие ключи  $K=(M_i, Esi)$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Сообщение  $M'$  (8 бит):

00010010

Ключ  $K'$  (16 бит):

0100010001000111

Идентификатор  $Es'$  (b бит):

111110

Ключи  $K=(M_i, Esi, M', Es')$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Вероятность угадать  $K=(M_i, Esi, M', Es')$ :  
 $P = 1$

Верификация

Сообщение (8 бит):

00010010

Ключ (16 бит):

0100010001000101

Идентификатор (b бит):

111110

Верификация прошла успешно

Разрядность  $b$  (4 - 8):

6

Многократные передачи

Аутентификация

Сообщения  $M_i$  (8 бит):

01010011  
10110010  
11011000

Всего сообщений: 3

☐ Задать сообщения вручную:

Сообщение  $M$  (8 бит):

☒ Сгенерировать сообщения

Количество передач  $L$  (1-20):

3

Ключ  $K$  (16 бит):

0100010001000100

Идентификаторы  $Esi$  (b бит):

011011  
001011  
000001

Всего идентификаторов: 3

Общие ключи  $K=(M_i, Esi)$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Сообщение  $M'$  (8 бит):

00010010

Ключ  $K'$  (16 бит):

0100010001000111

Идентификатор  $Es'$  (b бит):

111110

Ключи  $K=(M_i, Esi, M', Es')$ :

0100010001000100  
0100010001000101  
0100010001000110  
0100010001000111

Всего ключей: 4

Вероятность угадать  $K=(M_i, Esi, M', Es')$ :  
 $P = 1$

Верификация

Сообщение (8 бит):

00010010

Ключ (16 бит):

0100010001000110

Идентификатор (b бит):

111110

Верификация прошла успешно

Разрядность  $b$  (4 - 8):

6

3 - минимальное число передач, при котором злоумышленник выполнит подделку любого выбранного сообщения с вероятностью 1.



**Вывод:**

В ходе данной лабораторной работы был сформирован и исследован аутентификатор к двоичному сообщению. Также была проведена атака по подделке сообщения и рассчитана вероятность ее обнаружения - она крайне мала. Выполнено формирование аутентификаторов при многократной передаче сообщений на одном и том же ключе, произведена оптимальная атака и рассчитана вероятность необнаруженной подмены сообщения - она равна единице.