Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

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

| Кафе, | дра защищенных систем связи | | | | |
|---|-----------------------------|--|--|--|--|
| Дисци | плина «Основы криптографии» | | | | |
| | | | | | |
| | | | | | |
| Л | абораторная работа № 11 | | | | |
| «Исследование безусловно стойкой аутентификации сообщений на основе строго-универсальных хэш-функций» | | | | | |
| | | | | | |
| Выполнила: | ст. гр. ИКТЗ-83 | | | | |
| | Громов А.А. | | | | |
| | Вариант 4 | | | | |
| | | | | | |
| П | a DA | | | | |
| Проверил: | Яковлев В. А. | | | | |
| | | | | | |

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 $E_s = [M * K_0 + K_1]_b$,

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

$$K_0 = 0101$$

$$K_1 = 1100$$

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

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

$$E_{S} = [0100 \cdot 0101 + 1100]_{4}$$
1) $0100 \cdot 0101 = \sqrt{2} \cdot (\sqrt{2} + 1) = \sqrt{4} + \sqrt{2}$

$$- \sqrt{4} + \sqrt{2} | \sqrt{4} + \sqrt{4} + 1$$

$$- \sqrt{4} + \sqrt{4} | 1$$

$$- \sqrt{4} + \sqrt{4} | 1$$
2) $0111 + 1100 = 10011_{2} = 19_{10}$

$$E_{S} = 10011$$

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 Es - |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 и M ' в E 's $M \neq M$ ' - |H ''.

$$|H'''| = |H|/|E_s|^2$$

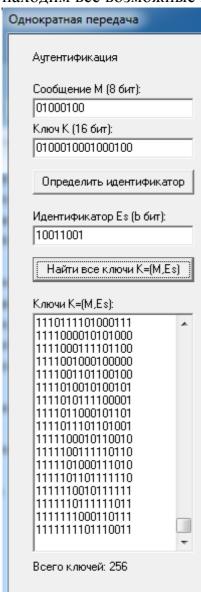
При
$$b = 4$$
: $|H''| = |256|/|16^2| = 1$

При
$$b = 3$$
: $|H''| = |256|/|8^2| = 4$

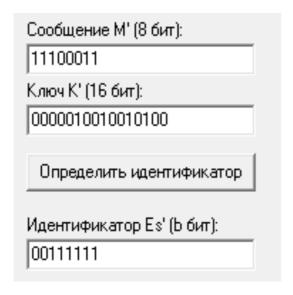
2 часть

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

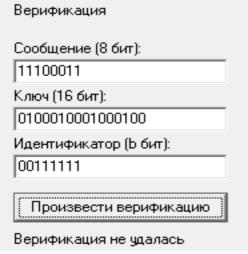
1. Задаём произвольное сообщение и ключ, вычисляем аутентификатор и находим все возможные ключи.



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



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



Видим, что верификация не удалась.

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



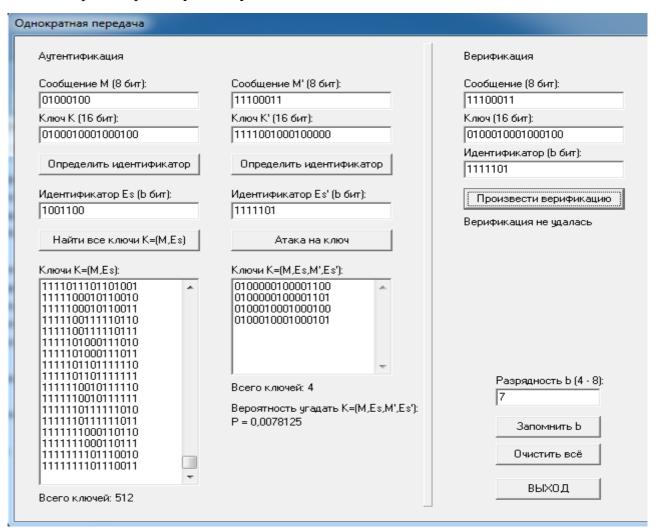
Убедимся, что расчёт вероятности выполнен верно

$$P = |H''|/|H'| = 1/256 = 0,00390625.$$

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

| Верификация | | | | |
|------------------------|--|--|--|--|
| Сообщение (8 бит): | | | | |
| 11100011 | | | | |
| Ключ (16 бит): | | | | |
| 0100010001000100 | | | | |
| Идентификатор (b бит): | | | | |
| 11111010 | | | | |
| Произвести верификацию | | | | |
| Верификация не удалась | | | | |

5. Повторяем предыдущие пункты для b = 7.

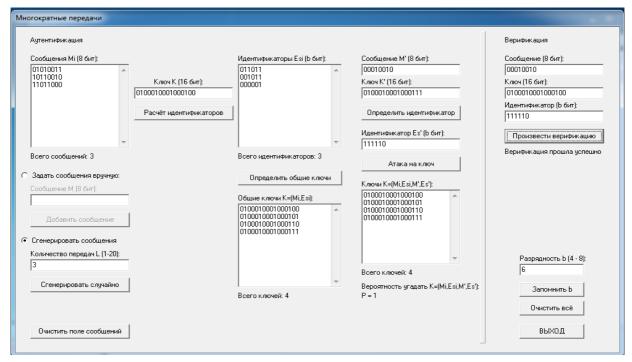


Расчёт вероятности P = |H''|/|H'| = 4/512 = 0,0078125

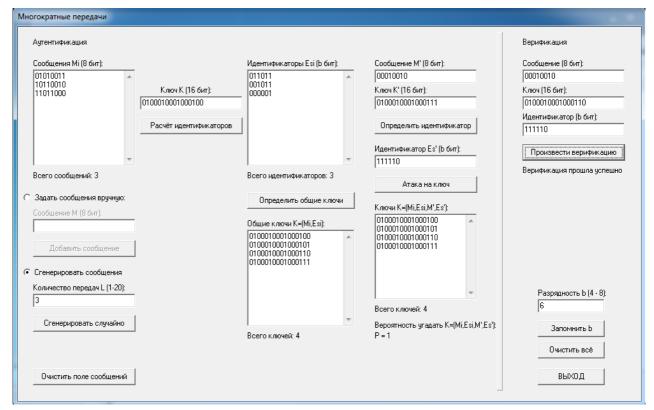
6. Выбираем режим Многократная передача. Установим длину аутентификатора b = 6 и при случайном генерировании сообщений для

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 Мі (8 бит): 01010011 10110010 11011000 | Ключ К (16 бит): 00010001000100 Расчёт идентификаторов | Идентификаторы Esi (b бит): 011011 001011 000001 | Сообщение М' (8 бит): 00010010 Ключ К' (16 бит): 0100010001000111 Определить идентификатор Идентификатор Es' (b бит): 111110 | Верификация Сообщение (8 бит): 00010010 Ключ (16 бит): 0100010001000111 Идентификатор (b бит): 1111110 |
| Всего сообщений: 3 | | Всего идентификаторов: 3 | Атака на ключ | Верификация прошла успешно |
| С Задать сообщения вручную: Сообщение М (8 бит): Добавить сообщение С Сгенерировать сообщения | | Определить общие ключи Общие ключи К={Mi,Esi}: 0100010001000100 010001000100100 0100010001001 | K.novu K=(Mi,Esi,M',Es'): 0100010001000100101 010001000100101 0100010001000110 0100010001000111 | |
| Количество передач L (1-20): 3 Сгенерировать случайно | | Всего ключей: 4 | Всего ключей: 4 Вероятность угадать K=(Mi,Esi,M',Es'): P = 1 | Разрядность b (4 · 8): 6 Запомнить b Очистить всё |
| Очистить поле сообщений | | | | выход |



| Многократные передачи | | | | |
|---|---|----|--|--------------------------------|
| Аутентификация | | | | Верификация |
| 01000 | Идентификаторы Esi (b бит 011011 001011 000001 000001 счёт идентификаторов |): | Сообщение М' (8 бит): 00010010 | Сообщение (8 бит): 00010010 |
| | | ~ | 111110 | Верификация прошла успешно |
| Всего сообщений: 3 | Всего идентификаторов: 3 | | Атака на ключ | |
| С Задать сообщения вручную: | Определить общие клю | чи | Ключи K=(Mi,Esi,M',Es'): | |
| Сообщение М (8 бит): Добавить сообщение | Общие ключи K=(Mi,E si): 0100010001000100 010001000100100 0100010001001 | A | NIIO94 NII(ILES) | |
| Сгенерировать сообщения | | | | |
| Количество передач L (1-20): 3 Сгенерировать случайно | | ¥ | Всего ключей: 4 Вероятность угадать K=(Mi,Esi,M',Es'): | Разрядность b (4 - 8): |
| | Всего ключей: 4 | | P = 1 | Запомнить в |
| Очистить поле сообщений | | | | выход |



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 необнаружения - 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.