МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №6

по дисциплине «Криптография и защита информации»

Тема: Изучение хэш-функций

Студент гр. 8383 _____ Ларин А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2021

Цель работы

Исследование хэш-функций MD5, SHA-256, SHA-512, SHA-3, кода контроля целостности HMAC и анализ атак дополнительной коллизии на хэш-функцию. Получить практические навыки работы с хэш-функциями и атакой на них, в том числе и в программном продукте Cryptool 1 и 2.

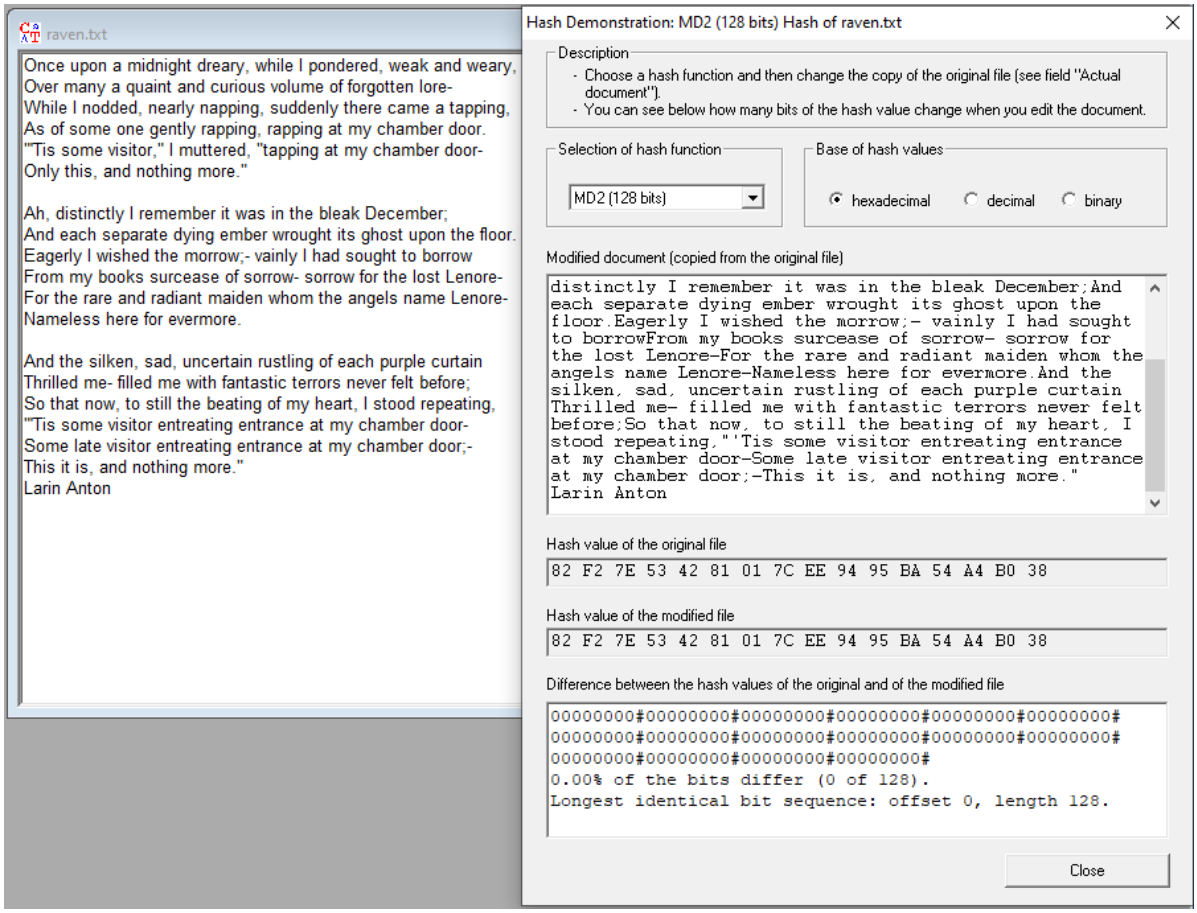
1. Исследование лавинного эффекта MD5, SHA-1, SHA-256, SHA-512

Задание

1. Открыть текст не менее 1000 знаков. Добавить свое ФИО последней строкой. Перейти к утилите Indiv.Procedures→Hash→Hash Demonstration..
2. Задать хэш-функцию, подлежащую исследованию: MD5, SHA-1, SHA-256, SHA-512
3. Для каждой хэш-функции повторить следующие действия:
   a. Измените (добавлением, заменой, удалением символа) исходный файле
   b. Зафиксировать количество измененных битов в дайджесте модифицированного сообщения.
   c. Вернуть сообщение в исходное состояние.
4. Выполните процедуру 3 раза (добавлением, заменой, удалением символа) и подсчитайте среднее количество измененных бит дайджеста.
5. Зафиксировать результаты в таблице.

Выполнение

1. В качетсве открытого текста взяты три параграфа поэмы Raven. В конец добавлена строка Larin Anton



2. Изменение хэша при изменении текста

MD5

Hash value of the original file

```
72 A0 89 EF A2 42 04 39 24 91 81 4B 62 5A E3 75
```

Hash value of the modified file

```
83 20 64 47 D8 BB 8E 93 C4 7F 54 A2 73 DD F4 51
```

Difference between the hash values of the original and of the modified file

```
11110001#10000000#11101101#10101000#01111010#11111001#
10001010#10101010#11100000#11101110#11010101#11101001#
00010001#10000111#00010111#00100100#
50.00% of the bits differ (64 of 128).
Longest identical bit sequence: offset 9, length 7.
```

SHA-1

Hash value of the original file

```
9F FD A8 BD 3E 05 E8 46 99 E2 49 65 72 50 E4 91 2E C9 64 7
```

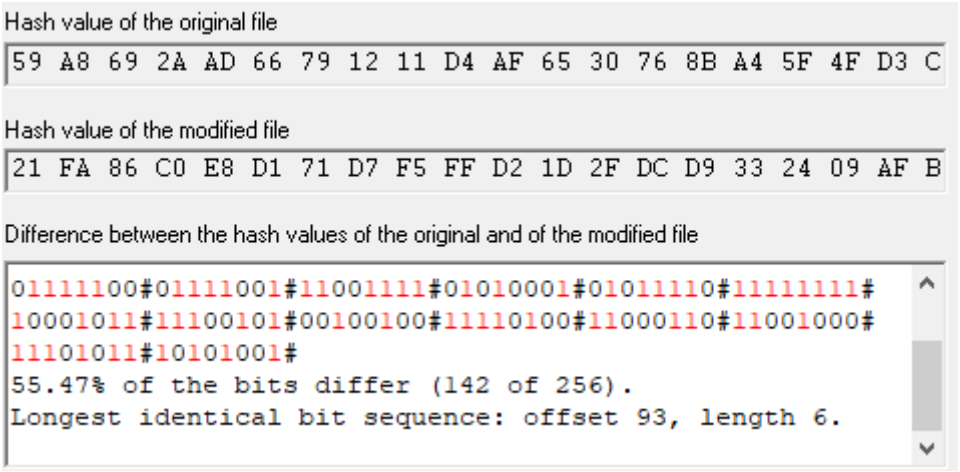
Hash value of the modified file

```
C4 A4 58 68 C9 5F 11 D5 9B AC F2 58 4F 7B 73 FD B1 A6 E3 D
```

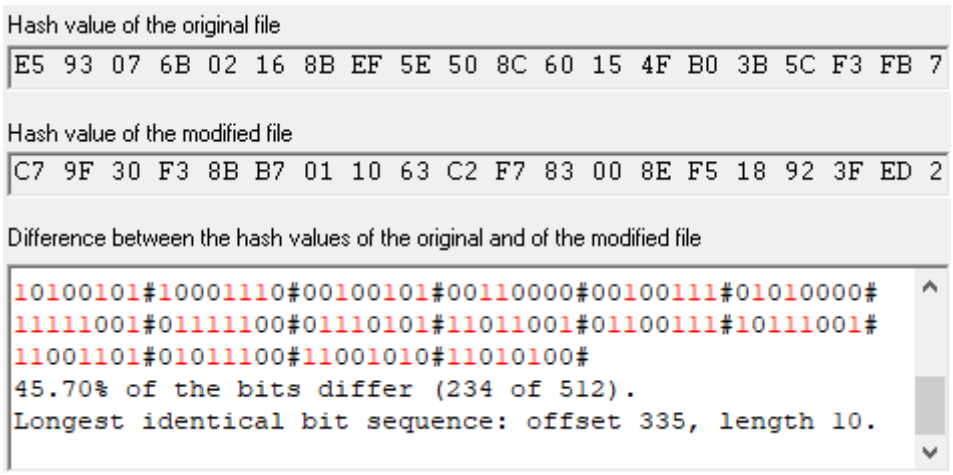
Difference between the hash values of the original and of the modified file

```
01011011#01011001#11110000#11010101#11110111#01011010#
11111001#10010011#00000010#01001110#10111011#00111101#
00111101#00101011#10010111#01101100#10011111#01101111#
10000111#10100010#
57.50% of the bits differ (92 of 160).
Longest identical bit sequence: offset 64, length 6.
```

SHA-256



SHA-512



3. Среднее количество изменившихся бит

	#1	#2	#3	среднее
MD5 (128)	64	61	56	60.(3) (47%)
SHA-1 (160)	92	67	77	78.(6) (49%)
SHA-256	142	122	121	128.(3) (50%)
SHA-512	234	259	249	247(3) (48%)

2. Хэш-функция SHA-3

Задание

1. Открыть шаблон Keccak Hash (SHA-3) в Cryptool 2
2. В модуле Keccak сделать следующие настройки:
   1. Adjust manually=ON
   2. Keccak version= SHA3-512
3. Загрузить файл из предыдущего задания
4. Запустить проигрывание шаблона в режиме ручного управления:

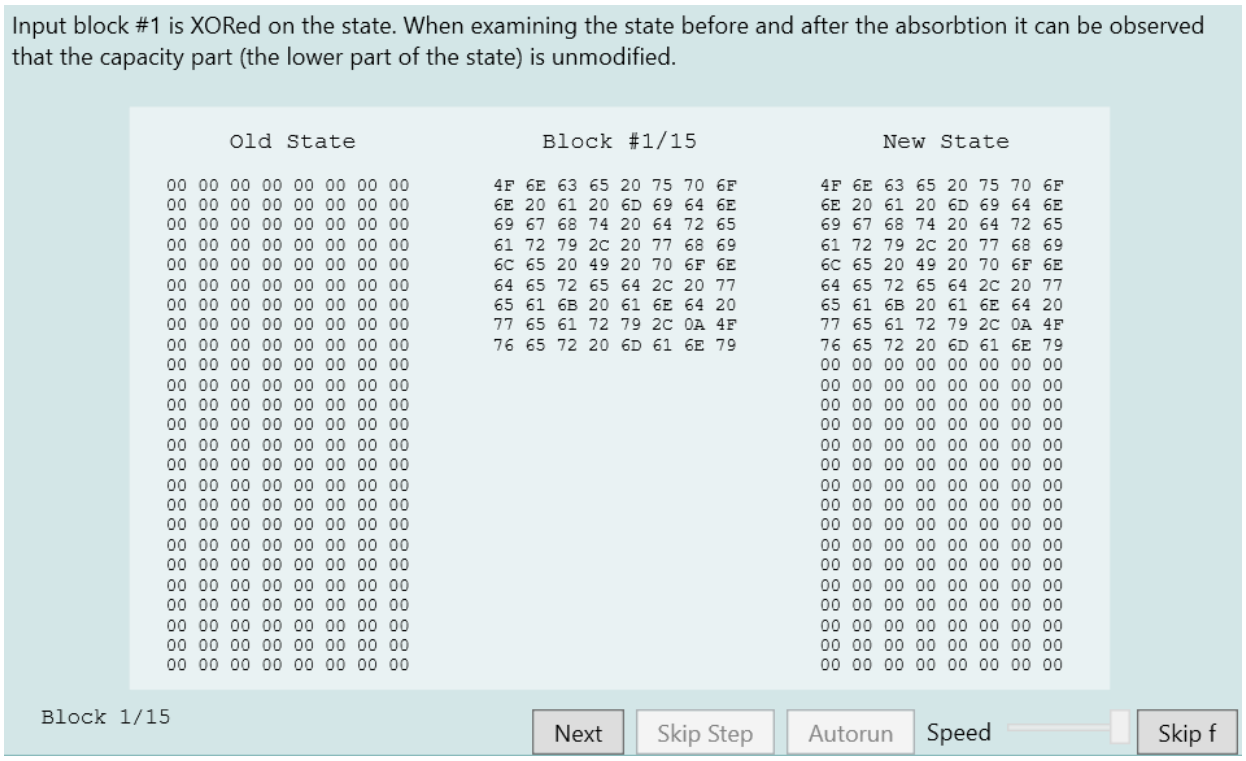
1. Сохранить скриншоты преобразований первого раунда
2. Сохранить скриншот заключительной фазы
3. Сохранить значение дайджеста

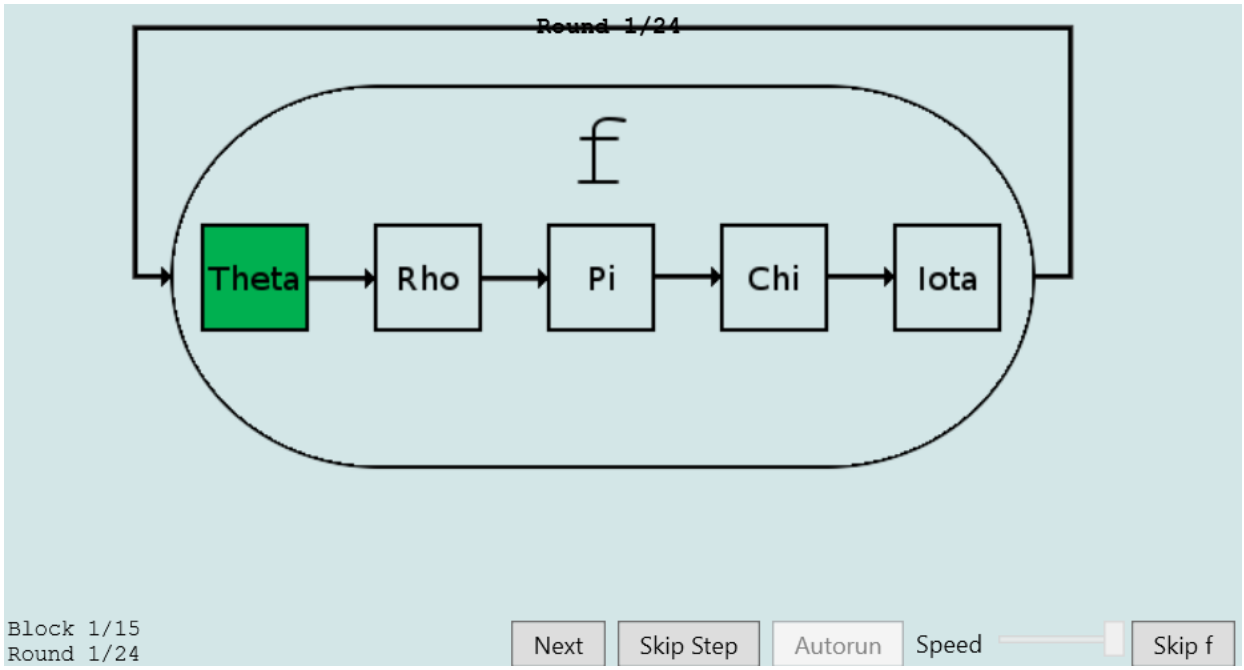
5. Вычислить значения дайджеста для модифицированных текстов из предыдущего задания
6. Подсчитать лавинный эффект с помощью самостоятельно разработанной автоматизированной процедуры

Выполнение

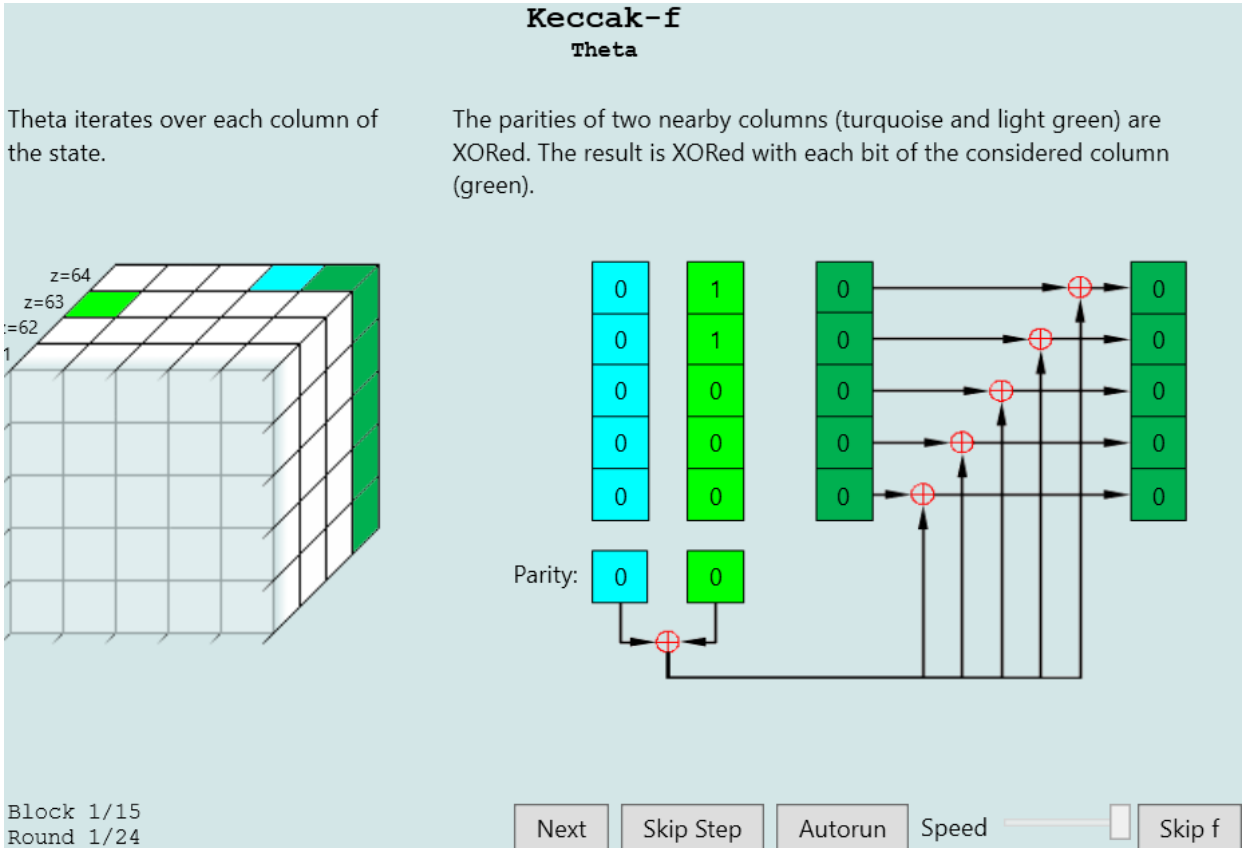
1. Открыт шаблон Keccak Hash (SHA-3) в Cryptool 2, сделаны нстройки, загружен текст

2. Первый раунд;




Round 1/24
f
Theta
Rho
Pi
Chi
Iota
Block 1/15
Round 1/24
Next
Skip Step
Autorun
Speed
Skip f

Theta


Keccak-f
Theta
Theta iterates over each column of the state.
The parities of two nearby columns (turquoise and light green) are XORed. The result is XORed with each bit of the considered column (green).
z=64
z=63
Parity:
Block 1/15
Round 1/24
Next
Skip Step
Autorun
Speed
Skip f

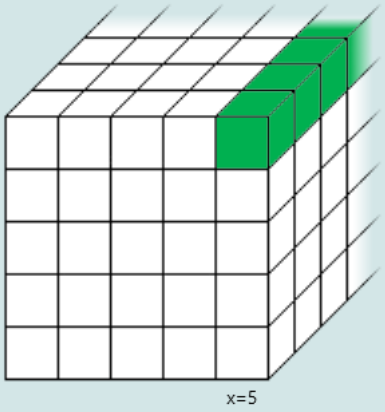
Rho

Keccak-f

Rho

Rho iterates over each lane of the state.

Each lane is right-rotated by a certain value (depicted in the red rectangle). The upper green block represents the lane before rotation, the lower green block represents the lane after rotation.



0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0
16	1	0	0	1	0	1	0	0	0	0	1	1	0	0	0
32	1	0	1	0	0	0	1	1	0	0	1	0	0	1	0
48	0	1	1	0	0	1	0	1	0	0	0	0	0	1	0

Rotation Offset: 14

0	1	0	0	1	0	1	0	0	0	0	1	0	0	1	0
16	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0
32	0	1	0	1	0	0	0	0	1	1	0	0	0	1	0
48	1	0	0	0	1	1	0	0	1	0	0	1	0	1	0	1

	x=1	x=2	x=3	x=4	x=5
y=1	0	1	62	28	27
y=2	36	44	6	55	20
y=3	3	10	43	25	39
y=4	41	45	15	21	8
y=5	18	2	61	56	14

Block 1/15
Round 1/24

Next | Skip Step | Autorun | Speed | Skip f

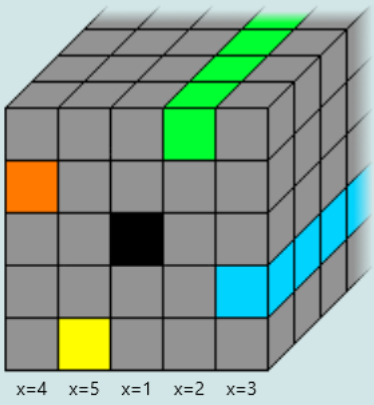
Pi

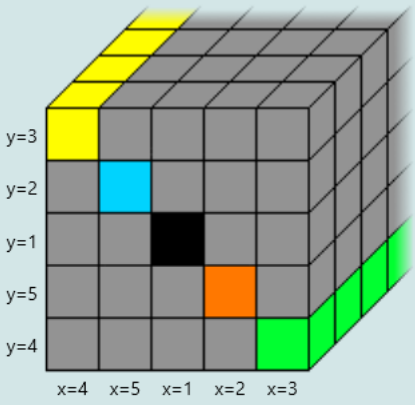
Keccak-f

Pi

Pi permutes the positioning of the lanes within the state. The lane coordinates of the cube are shifted for improved visualization.

Every lane except the lane at x=1, y=1 (black) is moved to a different position. The right cube presents the new lane positions of the colored lanes. Already moved lanes are grayed out.

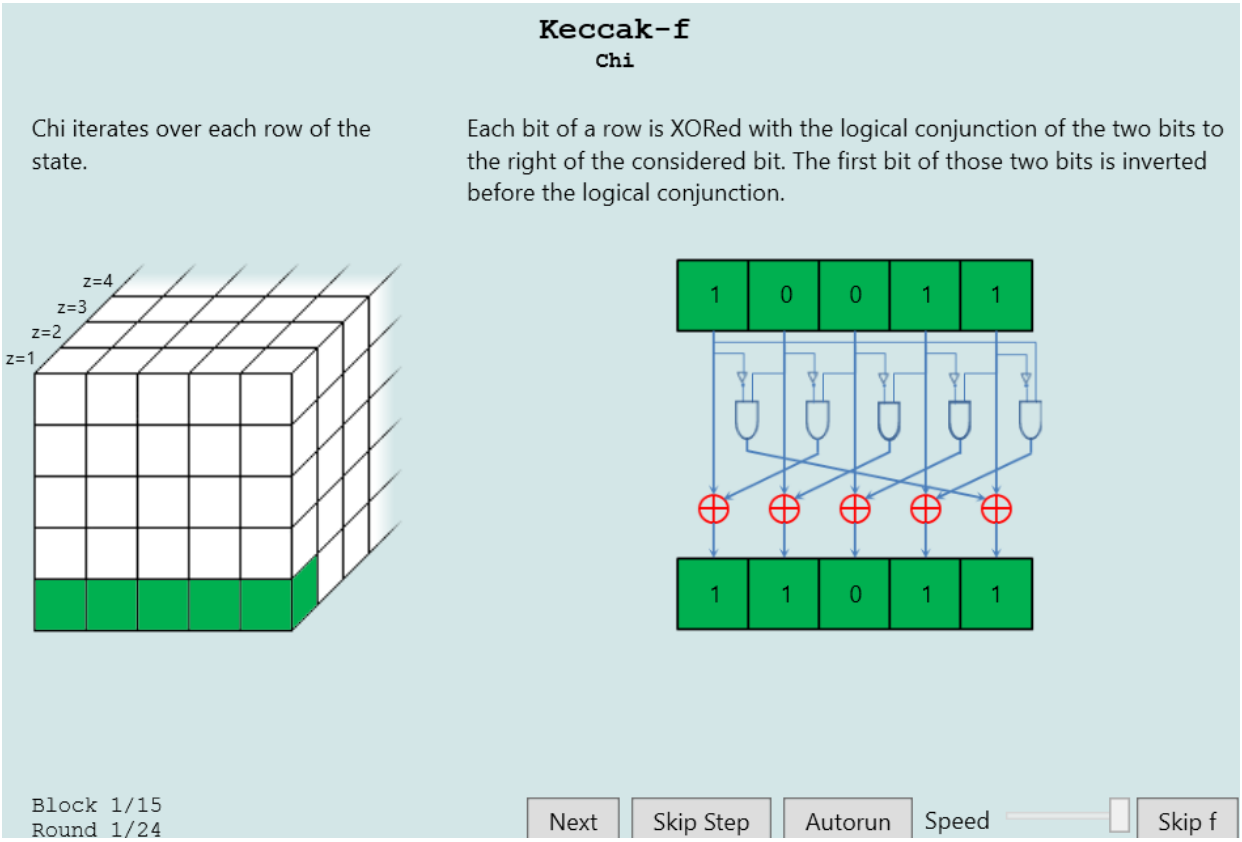




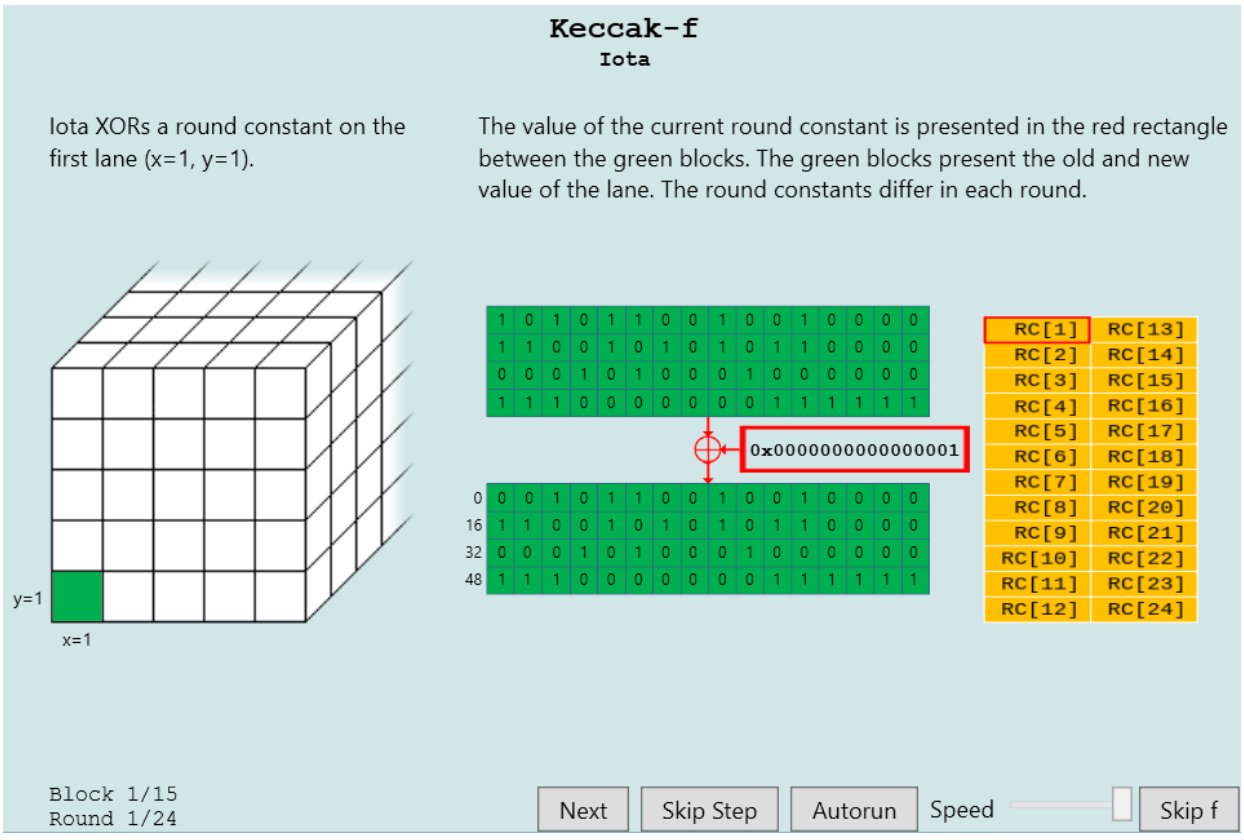
Block 1/15
Round 1/24

Next | Skip Step | Autorun | Speed | Skip f

Chi



Iota



Фаза отжатия

The 512-bit hash value is extracted from the bit rate part (upper part of the state).

State	Hash Output
7C E5 A1 E6 50 1B EC 01	7C E5 A1 E6 50 1B EC 01
20 37 66 BA 73 3A 4A 18	20 37 66 BA 73 3A 4A 18
E7 9C 87 41 E2 22 ED C0	E7 9C 87 41 E2 22 ED C0
37 57 56 B9 42 79 C7 B4	37 57 56 B9 42 79 C7 B4
69 22 02 56 C3 84 FB 54	69 22 02 56 C3 84 FB 54
63 E2 B8 50 49 97 0E 3A	63 E2 B8 50 49 97 0E 3A
2F 5F 4D 25 5F A3 D0 F9	2F 5F 4D 25 5F A3 D0 F9
0E D6 61 A6 5D BB 1F 7D	0E D6 61 A6 5D BB 1F 7D
F1 43 6C F6 8F A2 E7 C1	
AA B4 35 12 31 61 5B 0F	
7A 91 F4 6D F2 23 33 C7	
09 88 0C 3F A8 4A 79 9F	
E3 22 18 88 F3 F3 E2 36	
B6 BD 96 39 7F 69 97 E2	
3A 57 D8 C9 82 E7 D3 5B	
34 96 2F 28 0F B6 32 B1	
68 8C 22 5D 13 05 6A 6C	
22 68 CA 24 25 62 CB E3	
56 D9 03 F6 ED AD DE 7D	
04 3E 5D 84 CA 7A 3C 2A	
D8 D9 A5 25 A7 63 26 7A	
E8 64 2A 95 3F 19 69 AC	
C9 BD 6A 16 FB B2 2A 12	
56 83 44 58 AE E3 F0 F4	
F6 DE 87 B5 68 5F FD F3	

Получившийся хэш
7C E5 A1 E6 50 1B EC 01 20 37 66 BA 73 3A 4A 18 E7 9C 87 41 E2 22 ED C0 37 57 56 B9 42 79 C7 B4 69 22 02 56 C3 84 FB 54 63 E2 B8 50 49 97 0E 3A 2F 5F 4D 25 5F A3 D0 F9 0E D6 61 A6 5D BB 1F 7D

#1
CF A7 9A D2 F7 A9 12 43 84 C1 C1 95 AD 71 7D 8A C3 BB 90 2E E9 76 FA 41 13 A2 85 5A 27 95 56 A1 B3 82 13 DA 07 10 CA 42 AA D5 D1 30 E0 17 1A 60 6A D4 6F E7 4E 22 BF ED 9E 88 F9 3B 08 D0 FE 4A

diff:1026

#2
FB 4B 90 97 EF 6F 3E D6 5C F5 DD 2B 83 F3 4B F8 5E 80 E9 02 4D 07 9B 7E B5 91 A3 B9 72 48 47 43 C2 32 C5 9D 1C FE E5 CE E0 9C C5 9B EF 6A 52 C5 3F 5C BA 1A 32 0C 45 F8 CD 59 77 F7 8D E7 FB FC

diff:1047

#3
EE 27 37 84 ED C2 C2 0C 40 60 67 35 05 6E 9C 5D D6 A5 0B EB 66 8F E9 55 97 2B 4D 50 EB 06 C2 DC 47 25 64 15 65 C7 6A 30 75 5F 0A 81 7E C1 D7 64 33 FF CA ED 89 09 82 D8 25 77 61 27 D3 75 96 79

diff:1028

mean:1033.(6) (49%)

Оценка лавинообразного эффекта проведена при помощи обработки на python

3. Контроль целостности по коду HMAC

Задание

1. Выбрать текст на английском языке (не менее 1000 знаков), добавить собственное ФИО и сохранить в файле формата .TXT
2. Придумать пароль и сгенерировать секретный ключ утилитой Indiv.Procedures->Hash-> Key Generation из Cryptool 1. Сохранить ключ в файле формата .TXT. Прочитать Help к этой утилите.
3. Сгенерировать HMAC для имеющегося текста и ключа с помощью утилиты Indiv.Procedures->Hash-> Generation of HMACs. Сохранить HMAC в файле формата .TXT. Прочитать Help к этой утилите.
4. Передать пароль, HMAC (и его характеристики), исходный текст и модифицированный текст коллеге, не раскрывая, какой текст является корректным. Попросите коллегу определить это самостоятельно.

Выполнение

1. Взят тот же исходный текст с тремя параграфами поэмы Raven и ФИ в конце.
2. Взят пароль 123456. Использована хэш-функция MD5, соль 1846741, 1000 итераций, на вызоде 16 байт
   Получившийся ключ:
   ED BB 27 07 A9 16 93 DB 23 C9 A7 DB 3B BB 61 4A

3. Сгенерирован HMAC. Выбрана схема H(k,m) (ключ перед текстом). Ключ взят из предыдущего пункта
   Получившийся HMAC:
   AD AA 4F FE BE 6F 58 33 FC CE BE 81 19 3C 41 53
4. Коллега при получении текста совершает те же действия — считает хэш от текста и сравнивает его с полученым.Если отличается — сообщение модифицировано, либо передано с искажениями

4. Контроль целостности по коду HMAC

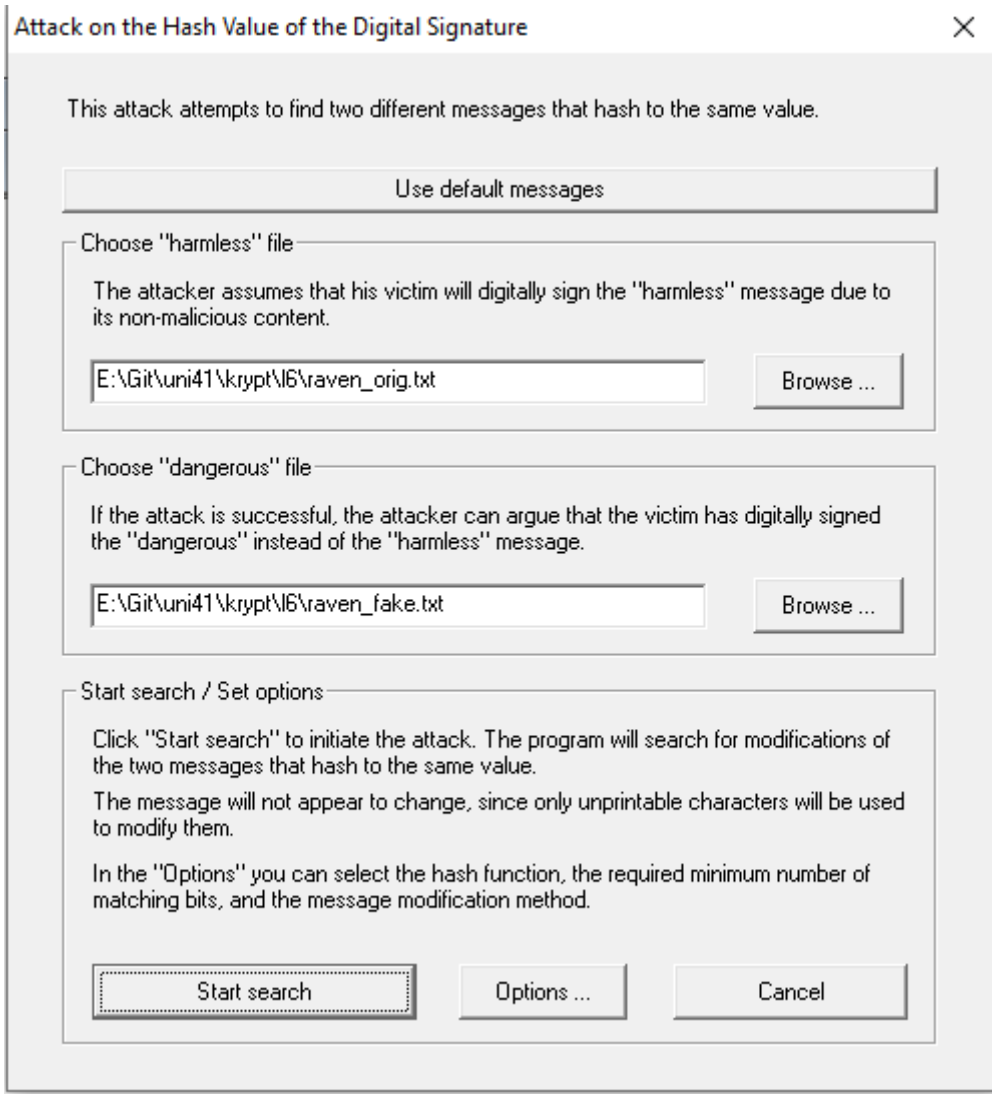
Задание

1. Сформировать два текста на английском языке - один истинный, а другой фальсифицированный. Сохранить тексты в файлах формата *.txt
2. Утилитой Analysis-> Attack on the hash value... произвести модификацию сообщений для получения одинакового дайджеста. В качестве метода модификации выбрать Attach characters-> Printable characters.

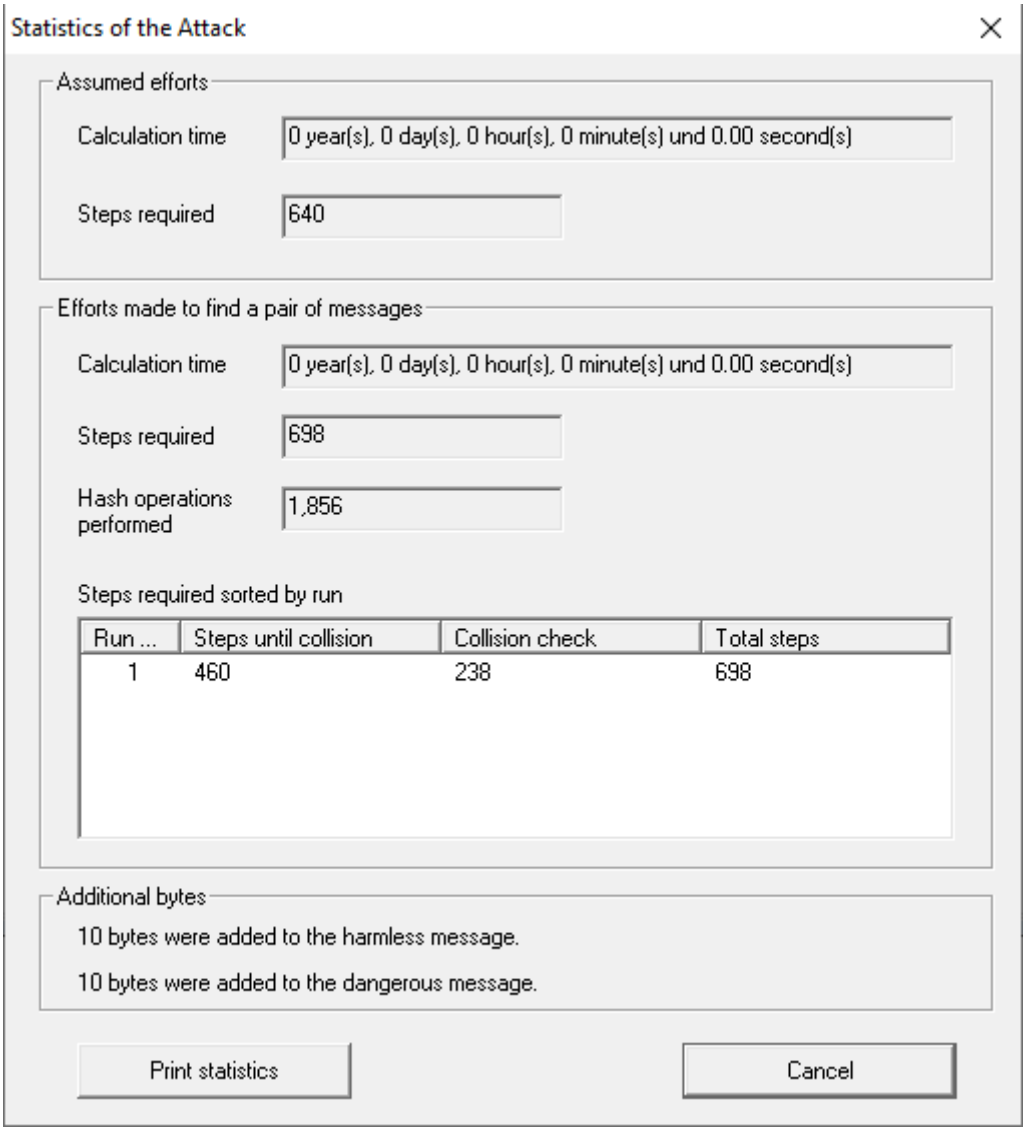
3. Проверить, что дайджесты сообщений действительно совпадают с заданной точностью.
4. Сохранить исходные тексты, итоговые тексты и статистику атаки для отчета.
5. Зафиксировать временную сложность атаки для 8, 16, 32,40, 48, … бит совпадающих частей дайджестов.

Выполнение

1. Взяты те же параграфы, изменено несколько слов
2. a



3. Хэш первого сообщения:
   03 CD C3 98 07 44FB 94 71 99 3F CA C5 3F 70 E1
   Хэш ложного сообщения:
   03 CD C3 98 05 AF 94 E4 3A 37 43 65 84 58 F1 11



4. Итоговый верный текст

Once upon a midnight dreary, while I pondered, weak and weary,
Over many a quaint and curious volume of forgotten lore-
While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, rapping at my chamber door.
"'Tis some visitor," I muttered, "tapping at my chamber door-
Only this, and nothing more."

Ah, distinctly I remember it was in the bleak December;
And each separate dying ember wrought its ghost upon the floor.
Eagerly I wished the morrow;- vainly I had sought to borrow
From my books surcease of sorrow- sorrow for the lost Lenore-
For the rare and radiant maiden whom the angels name Lenore-
Nameless here for evermore.

And the silken, sad, uncertain rustling of each purple curtain
Thrilled me- filled me with fantastic terrors never felt before;
So that now, to still the beating of my heart, I stood repeating,

"'Tis some visitor entreating entrance at my chamber door-
Some late visitor entreating entrance at my chamber door;-
This it is, and nothing more."
Larin AntonAACDCCCACC

5. Итоговый ложный текст

Once upon a midnight dreary, while I pondered, weak and weary,
Over many a quaint and curious volume of forgotten lore-
While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, tapping at my chamber door.
"'Tis some visitor," I muttered, "tapping at my chamber door-
Merely this, and nothing more."

Ah, distinctly I remember it was in the bleak December;
And each separate dying ember wrought its ghost upon the floor.
Eagerly I wished the morrow;- vainly I had sought to borrow
From my books surcease of sorrow- sorrow for the lost Lenore-
For the rare and radiant maiden whom the angels name Lenore-
Nameless here for evermore.

And the silken, sad, uncertain rustling of each purple curtain
Thrilled me- filled me with fantastic terrors never felt before;
Presently, to still the beating of my heart, I stood repeating,
"'Tis some visitor entreating entrance at my chamber door-
Some late visitor entreating entrance at my chamber door;-
Merely this, and nothing more."
Larin Anton
AADABDACDC

Статистика
Partial MD5-Collision Search

Filename original: E:\Git\uni41\krypt\l6\raven_orig.txt
Filename fake: E:\Git\uni41\krypt\l6\raven_fake.txt
PROJECTED EFFORTS

Calculating time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)
Steps required

COMPUTING EFFORTS

Calculating time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)
Steps required
Hash operations performed

RunNo. Steps until collision Check of the collision Total steps

01 460 238 698

TEXT MODIFICATION

10 bytes were added to the harmless message.
10 bytes were added to the dangerous message.

6. Временая сложность атаки (в секундах)

8	16	32	40	48	56
0	0	2.76	8.44	2.4e+2	3.6e+3

Выводы.

1. Исследованы хэш-функции MD5, SHA-1,SHA-256, SHA-512. Произведены панипуляции с текстом(изменений, добавление, удалений), исследован лавинообразный эффект. Во всех случаях изменение текста приводила к изменению состояния в среднем на 50%(+-3)
2. Исследована хэш-функция SHA-3 (Keccak) на основе демонстрации в программе Cryptool2. Использована верия SHA3-512.

   Вычислены значения хэшей исходнго и модифицированного текстов

   При помощи программы на python оценен лавинных эффект.

   Во всех случаях количество изменившихся бит было близко к 50%
3. Исследован механизм проверки целостности информации — HMAC, являющийся надстройкой над MAC.

   Сгенерирован ключ на основе пароля. Предполагается, что его знают обе стороны. Использована функция MD5, соль 1846741, 1000 итераций, на выходе 16 байт

   Для HMAC использован механизм H(k,m) -ключ перед текстом.

   Полученый хеш вместе с открытымтекстом отправляется «коллеге».

   Для проверки совершаются те же действия для расчета HMAC, после чего он сравнивается в присланным. Из не совпадение скажет о том, что открытый текст был модифицирован или исказился при передаче(или/и исказился хэш).
4. Исследована атаки дополнительной коллизии на хэш-функцию, основанная на парадоксе дней рождения.

   Сгенерировано два текста (оригинальный и моифицированный), они дополнены символами (печатными, для наглядности) так, чтобы их хэши совпадали с точностью до n бит. Посчитана трудоемкость атаки для различных n. По грубой оценка за каждые 8 бит сложность увеличивается на десятичный порядок, что похоже на теоритическую оценка (Пропорционально $\sqrt{2^N}$)