Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 6

Изучение алгоритмов хэширования

Студент: _____ Чернякова Валерия, группа 1304

Руководитель: _____ Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2024

Цель работы

Повысить компетенции в работе с алгоритмами хэширования.

Задачи:

- Оценить лавинный эффект хэш-функций;
- Изучить алгоритм работы функции перестановок Keccak;
- Изучить алгоритм работы функции диверсификации ключа;
- Изучить алгоритм вычисления кода аутентификации сообщения;
- Провести атаку дополнительной коллизии на хэш-функцию MD-5.

Задание

1. Открыть текст не менее 1000 знаков. Добавить ваши ФИО последней строкой.
2. Задать хеш-функцию, подлежащую исследованию: MD5, SHA-1, SHA-256, SHA-512.
3. Для каждой хеш-функции повторить следующие действия:

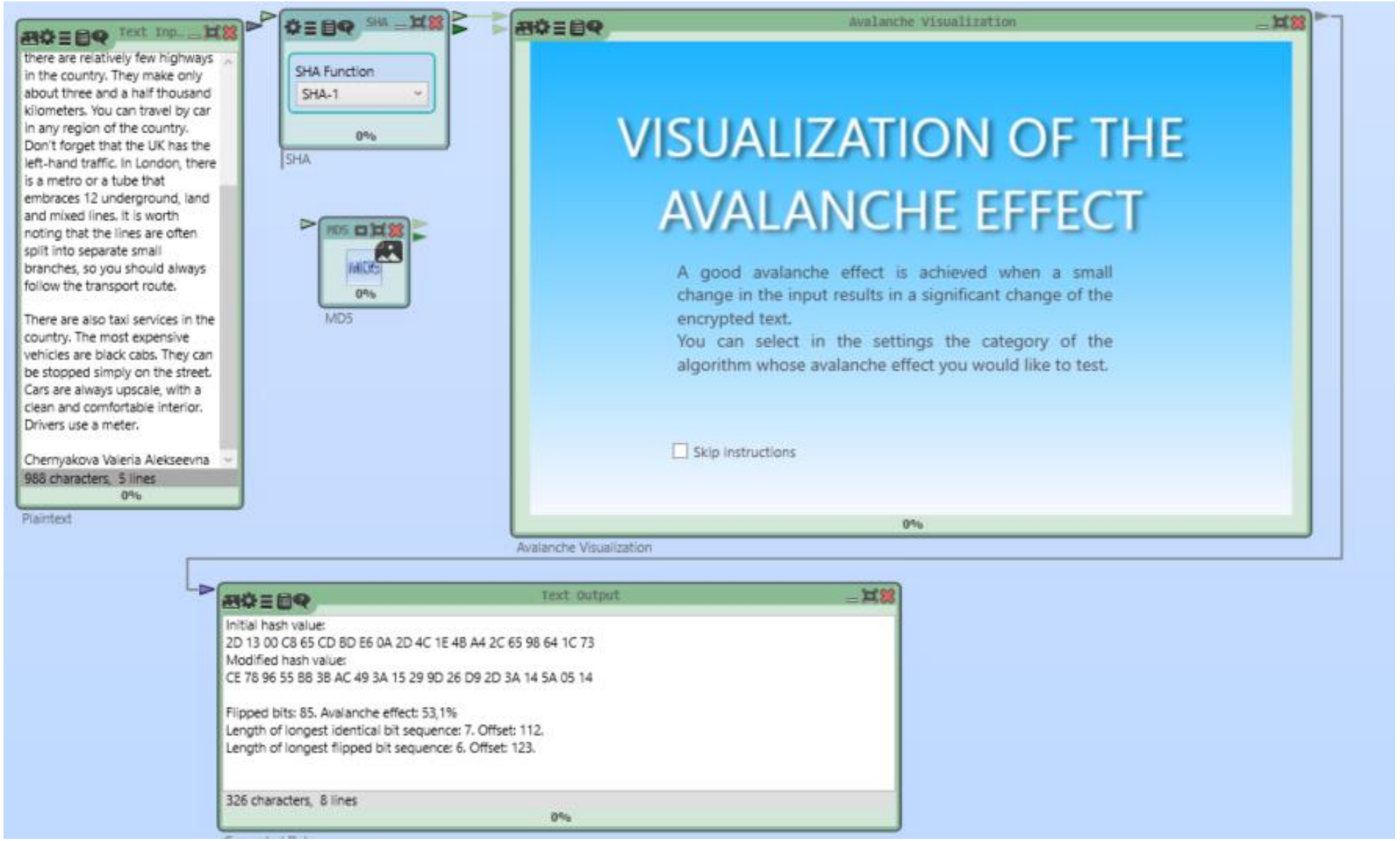
а)изменить (добавлением, заменой, удалением символа) исходный файл;

б)зафиксировать количество измененных битов в дайджесте модифицированного сообщения;

в)вернуть сообщение в исходное состояние.

4. Выполнить процедуру 3 раза (добавлением, заменой, удалением символа) и подсчитать среднее количество измененных бит дайджеста. Зафиксировать результаты в таблице.

Измерение лавинного эффекта



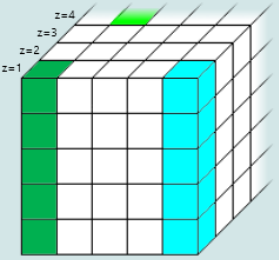
Исследование лавинного эффекта

Хэш-функция	№ измерения	Удаление	Вставка	Замена
MD5	1	44.3%	47.1%	48.4%
	2	43.8%	44.5%	57%
	3	50.2%	49.6%	51.6%
	Среднее	**48.93%**	**48.67%**	**52.33%**
SHA-1	1	51.1%	49.2%	48.4%
	2	50.8%	50%	50.5%
	3	45.1%	49.5%	45%
	Среднее	**49.67%**	**49.57%**	**49.97%**
SHA-256	1	50.3%	50.2%	46.8%
	2	47%	47.4%	49.8%
	3	45.4%	51.8%	49.2%
	Среднее	**48.23%**	**49.47%**	**48.6%**
SHA-512	1	49%	47.7%	46.8%
	2	47.6%	44.8%	49%
	3	48.6%	53.8%	47.6%
	Среднее	**48.07%**	**48.1%**	**48.47%**

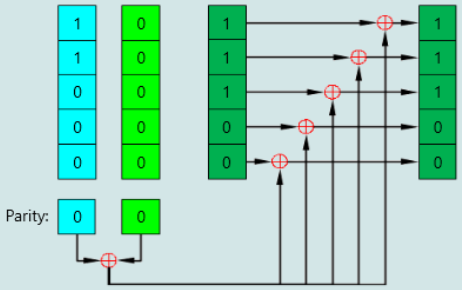
Алгоритм работы функции перестановок Keccak

Keccak-f
Theta

Theta iterates over each column of the state.

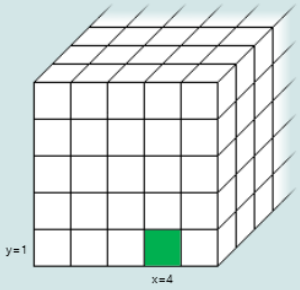


The parities of two nearby columns (turquoise and light green) are XORed. The result is XORed with each bit of the considered column (green).

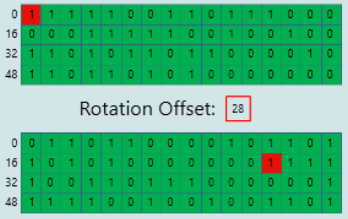


Keccak-f
Rho

Rho iterates over each lane of the state.



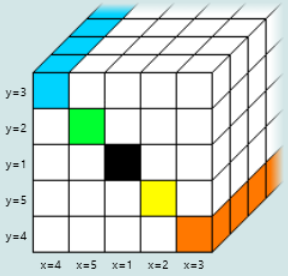
Each lane is right-rotated by a certain value (depicted in the red rectangle). The upper green block represents the lane before rotation, the lower green block represents the lane after rotation.



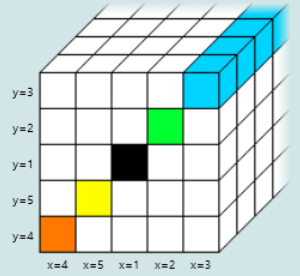
	x=1	x=2	x=3	x=4	x=5
y=1	0	1	62	28	27
y=2	36	44	6	55	20
y=3	3	10	43	25	39
y=4	41	45	15	21	8
y=5	18	2	61	56	14

Keccak-f
Pi

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

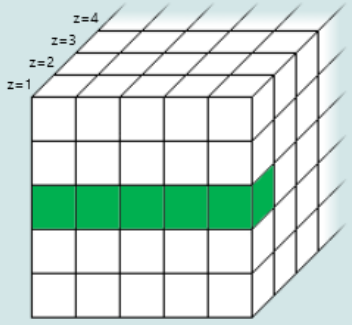


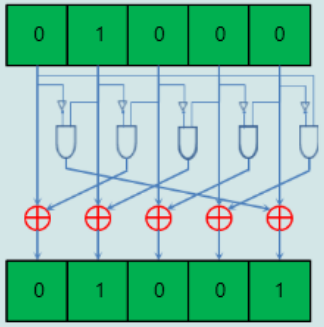
Every lane except the lane at x=1, y=1 (black) is moved to a differe position. The right cube presents the new lane positions of the col lanes. Already moved lanes are grayed out.



Chi iterates over each row of the state.

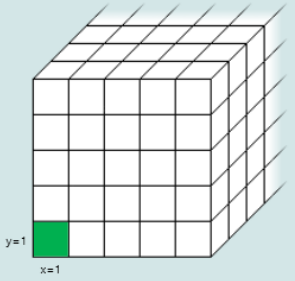
Each bit of a row is XORed with the logical conjunction of the two bits to the right of the considered bit. The first bit of those two bits is inverted before the logical conjunction.





Keccak-f
Iota

Iota XORs a round constant on the first lane (x=1, y=1).



The value of the current round constant is presented in the red rectangle between the green blocks. The green blocks present the old and new value of the lane. The round constants differ in each round.

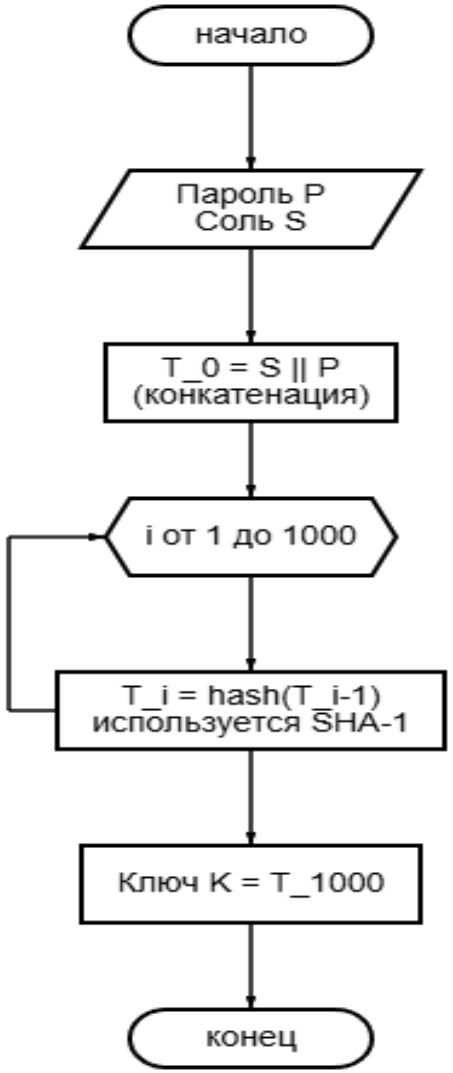
Исследование лавинного эффекта. SHA-3

Хэш-функция	№ измерения	Удаление	Вставка	Замена
SHA-3	1	55%	54.6%	59.4%
	2	55.7%	56%	55,4%
	3	57.4%	55.2%	56.7%
	Среднее	**56.7%**	**55.9%**	**57.17%**

Задание

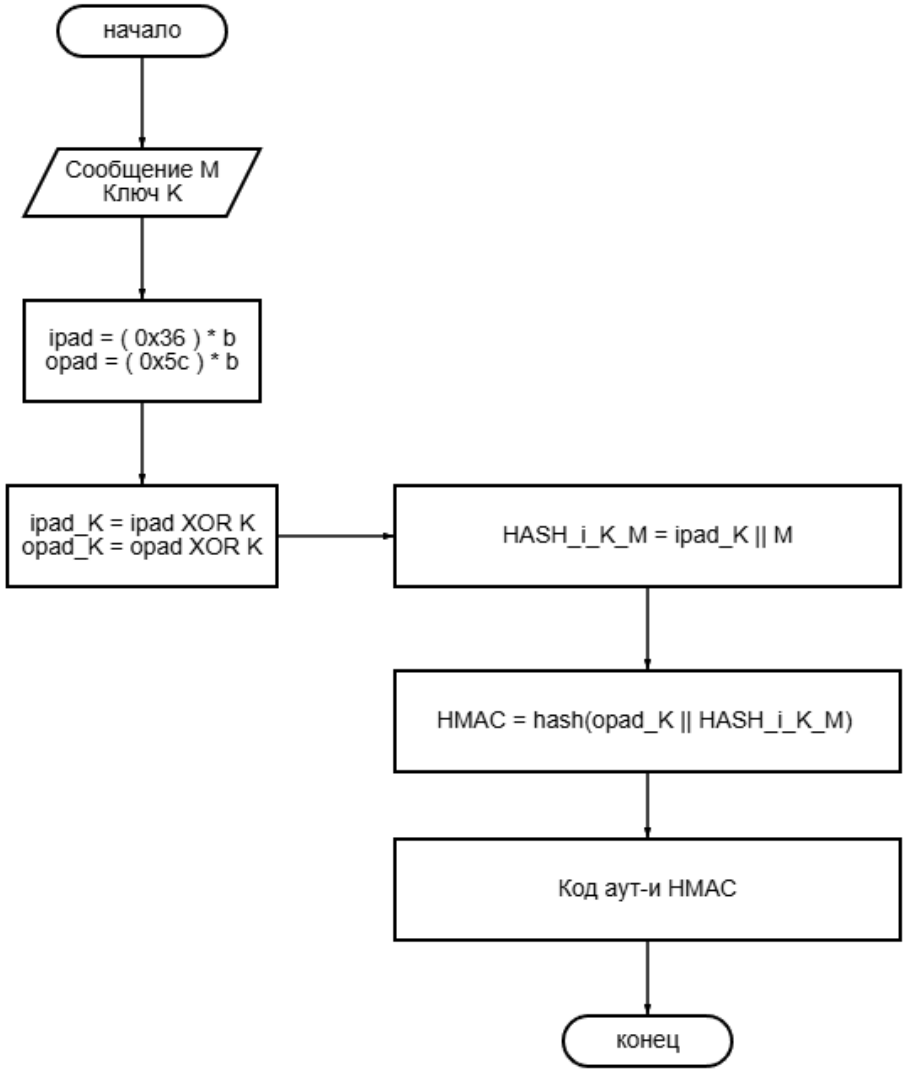
1. Изучить алгоритм работы функции диверсификации ключа с помощью шаблонной схемы PBKDF-1 в CrypTool 2. Получить симметричный ключ из персонального пароля, содержащего Фамилию, Имя, Отчество и дату рождения. Сохранить ключ для использования в 4 этого задания.
2. Выбрать текст на английском языке (не менее 1000 знаков), добавить ваши ФИО и сохранить в файле формата .txt.
3. 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.
4. 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.
5. Передать пароль, HMAC (и его характеристики), исходный и модифицированный тексты коллеге, не раскрывая, какой текст корректен. Попросить коллегу определить это самостоятельно.

Алгоритм работы функции диверсификации ключа PBKDF-1

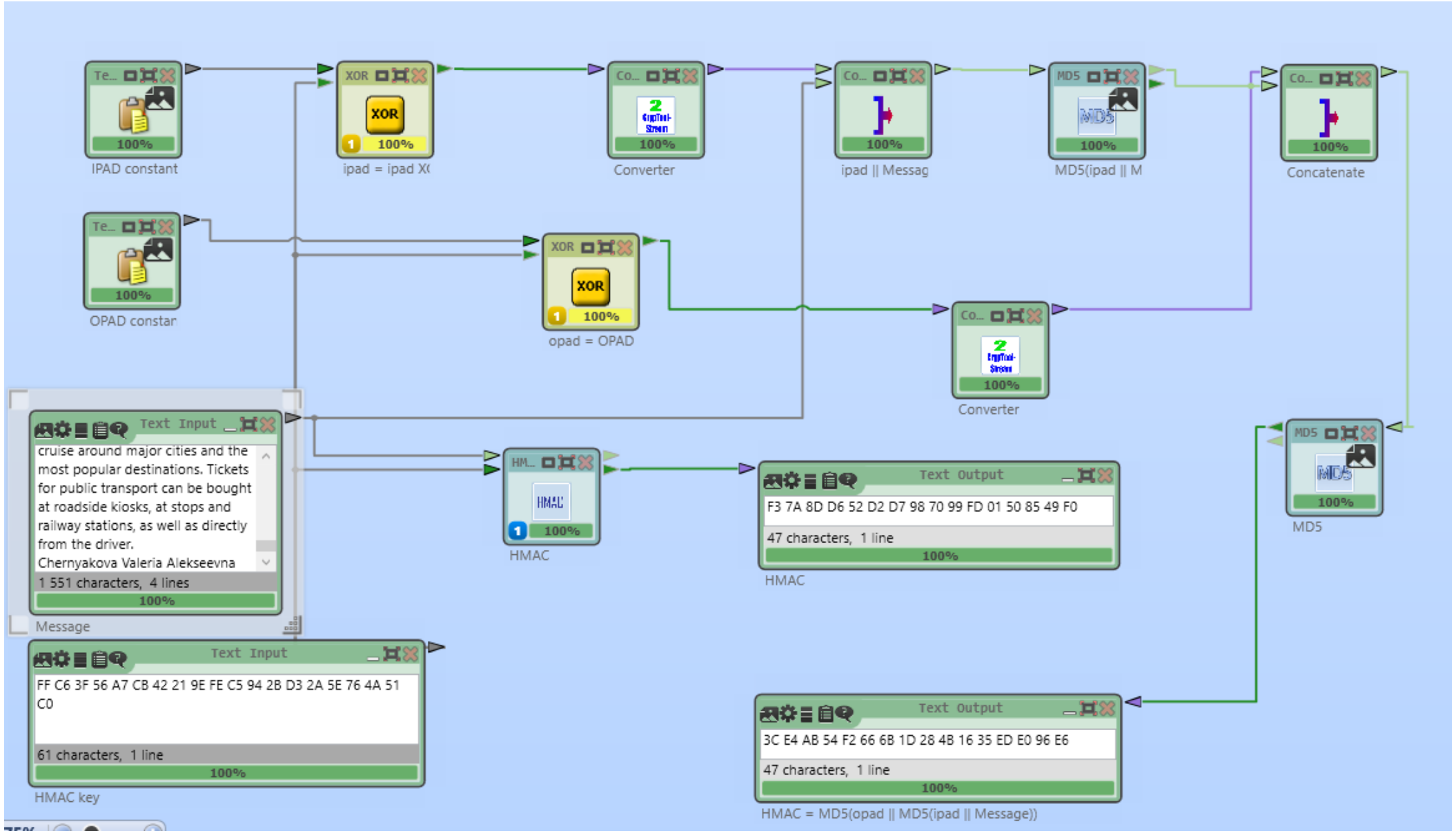


Сгенерированный ключ:
FF C6 3F 56 A7 CB 42 21 9E FE C5 94 2B D3 2A 5E 76 4A 51 C0

Алгоритм вычисления код аутентификации сообщения HMAC



Вычисление кода аутентификации сообщения HMAC



Задание

1. Сформировать два текста на английском языке – истинный и фальсифицированный. Сохранить тексты в файлах формата .txt.
2. Утилитой Analysis –> Attack on the hash value... модифицировать сообщения 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.

Атака дополнительной коллизии на хэш-функцию MD5

Кол-во бит совпадающих частей	Время	Кол-во бит совпадающих частей	Время
8	0 с	56	1 ч 35 м
16	0 с	64	1.1 дня
24	0.09 с	72	17 дней
32	1.06 с	80	272 дня
40	17.07 с	88	12 лет
48	4 м 33.2 с	96	200 лет

Заключение

- Исследован лавинный эффект в результате операций преобразования исходного текста для хэш-функций MD5, SHA-1, SHA-256, SHA-512. В среднем значение лавинного эффекта для всех функций составило 50%, то есть при изменении одного бита во входных данных примерно половина битов в выходном хэше изменится.
- Изучен алгоритм работы функции перестановок Keccak(SHA-3) и исследован лавинный эффект. Среднее значение лавинного эффекта составило 55% (наивысший показатель).
- Изучен алгоритм работы функции диверсификации ключа PBKDF-1. Основное свойство алгоритма PBKDF1 заключается в использовании пароля и случайной соли для генерации ключа. Был получен симметричный ключ из персонального пароля ФИО и дата рождения: ChernyakovaValeriaAlekseevna_27082003 и FF C6 3F 56 A7 CB 42 21 9E FE C5 94 2B D3 2A 5E 76 4A 51 C0.
- Изучен алгоритм вычисления код аутентификации сообщения HMAC. Основное свойство алгоритма это использование хэш-функции в сочетании с секретным ключом для проверки целостности и аутентичности данных.
- Провести атаку дополнительной коллизии на хэш-функцию MD5. С увеличением количества совпадающих битов в дайджестах хэш-функции MD5 время выполнения атаки возрастает, так как требуется больше вычислений для нахождения подходящих входных данных.