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

Лабораторная работа №6
ИЗУЧЕНИЕ алгоритмов хэширования

Студент: _____ Порошина Алина, группа 0361

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

Санкт-Петербург 2024

0361
HOLD ON

Цель работы

Цель работы:

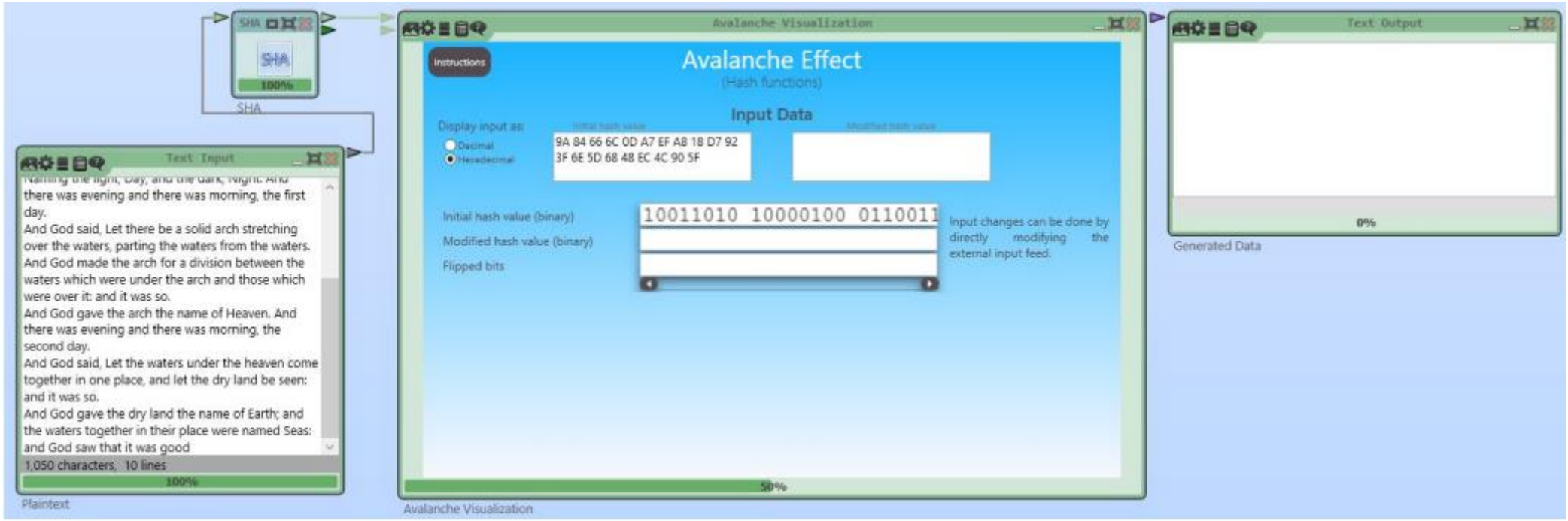
Приобретение знаний и умений в работе с алгоритмами хэширования.

Задачи:

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

0361
HOLD ON

Исследование лавинного эффекта: Шаблонная схема



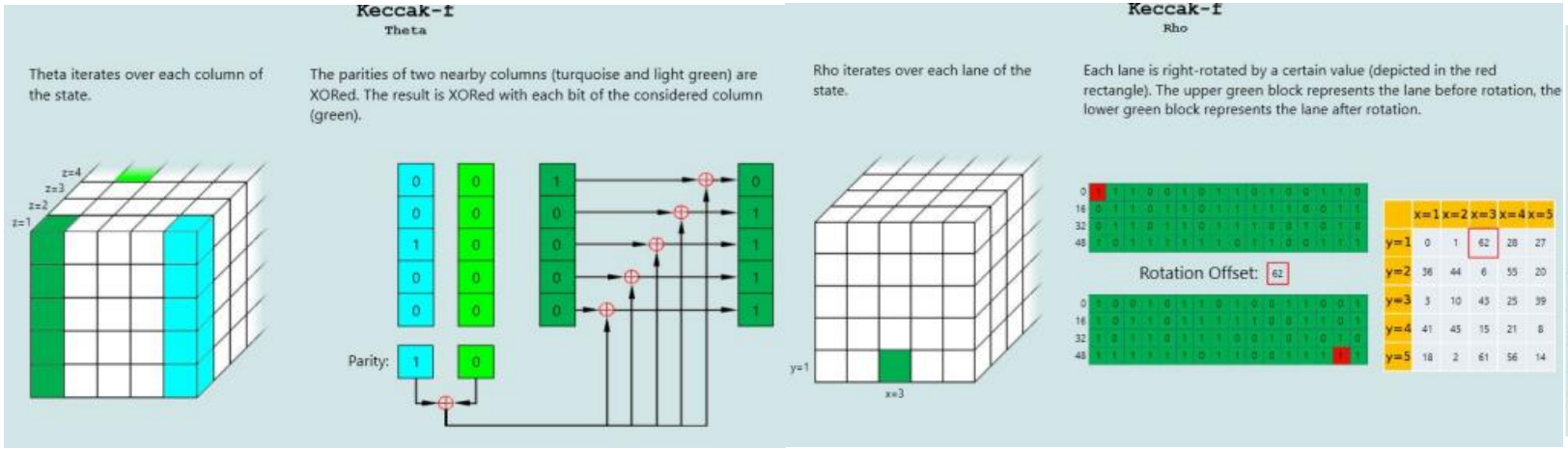
0361
HOLD ON

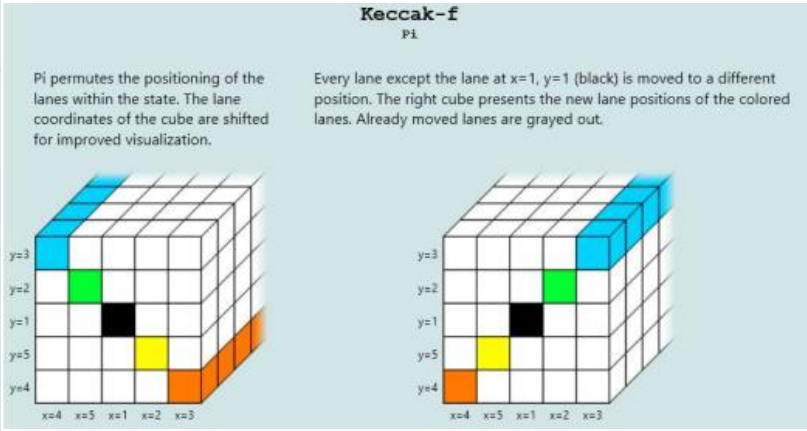
Исследование лавинного эффекта: таблица с результатами

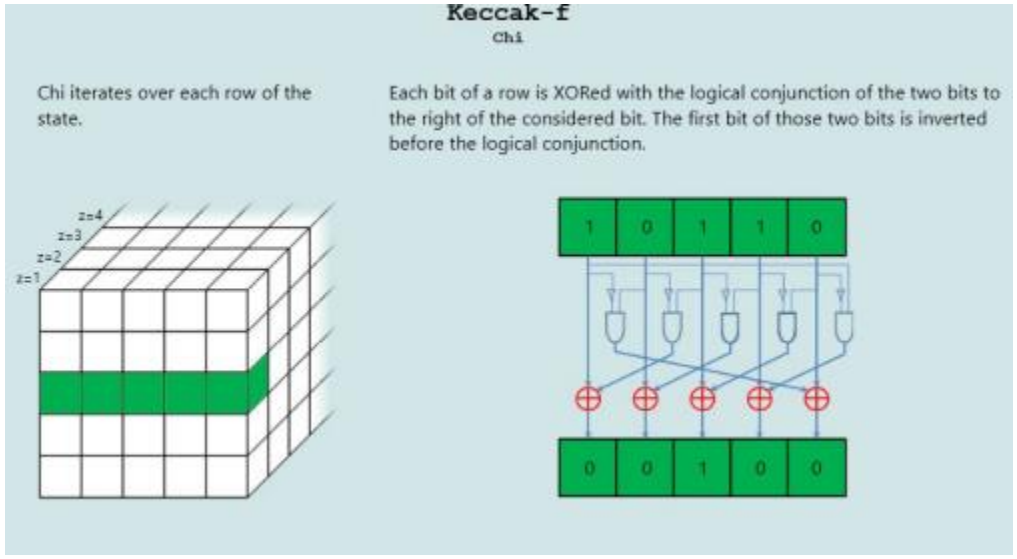
Хэш - функция	Изменение	Добавление	Удаление
MD5	46,1	41,4	53,1
SHA-1	48,1	50	48,8
SHA-256	53,1	51,6	51,6
SHA-512	49,4	47,1	52,1

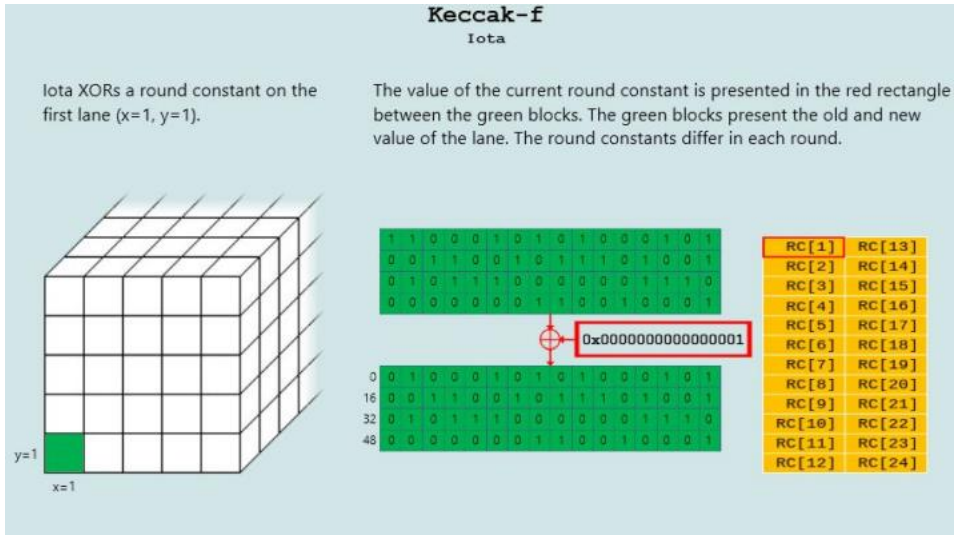
0361
HOLD ON

Keccak: Преобразования первого раунда









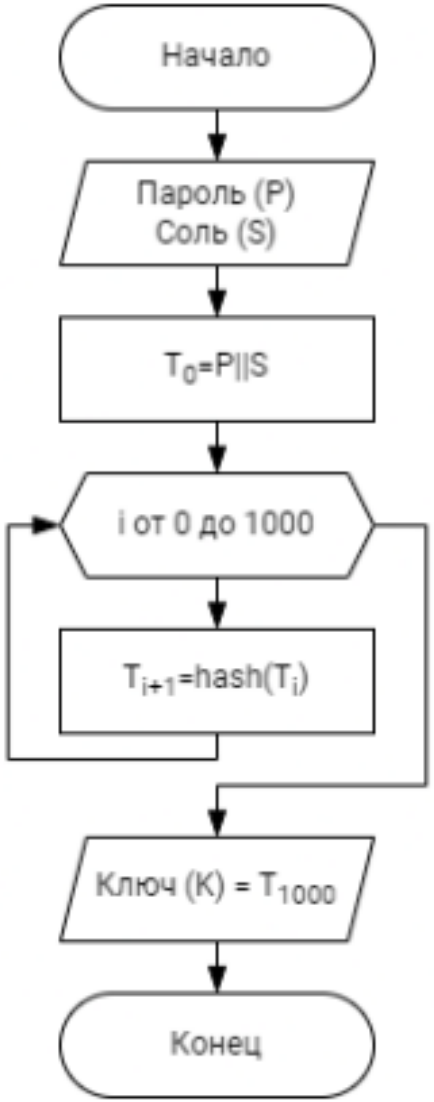
0361
HOLD ON

Величина лавинного эффекта в %%

Хэш-функция	Изменение	Добавление	Удаление	Среднее
MD5	46,1	41,4	53,1	46,7
SHA-1	48,1	50	48,8	49
SHA-3	52,7	50,8	53,9	52,5
SHA-256	53,1	51,6	51,6	52,1
SHA-512	49,4	47,1	52,1	49,5

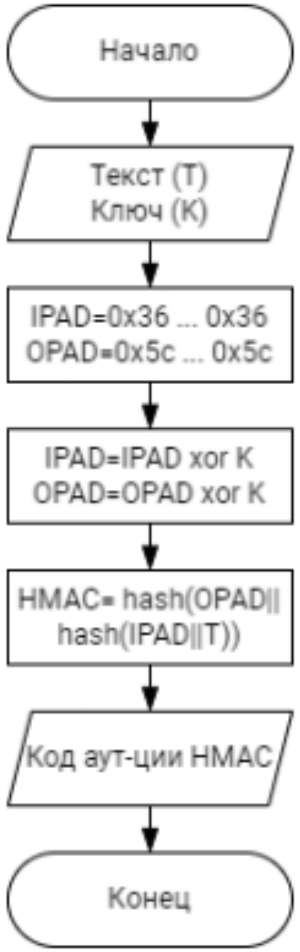
0361
HOLD ON

PBKDF-1: Схема алгоритма диверсификации ключа



0361
HOLD ON

HMAC: Схема алгоритма вычисления кода аутентификации ключа



0361
HOLD ON

MD-5: Атака дополнительной коллизии

Кол-во бит совпадающих частей	Время	Кол-во бит совпадающих частей	Время
8	0 с	56	1 ч. 35 мин.
16	0 с	64	1,1 дня
24	0,06 с	72	17 дней
32	1,06 с	80	272 дня
40	17,07 с	88	12 лет
48	4 мин. 33,22 с	96	200 лет

0361
HOLD ON

Выводы

1. Был исследован лавинный эффект хэш-функций MD5, SHA-1, SHA-256, SHA-512.

2. Был изучен алгоритм работы функции перестановок Keccak и исследован лавинный эффект. Посчитано среднее значение лавинного эффекта – наивысший показатель у Keccak.

3. Был изучен алгоритм работы функции диверсификации ключа PBKDF-1. Получен симметричный ключ из персонального пароля: POROSHINAALINAROMANO14102002 0361: FCF0A05E76FB74C1E34E95E187C489A30CDEF074

4. Был изучен алгоритм вычисления кода аутентификации сообщения HMAC. В качестве ключа использовался полученный на предыдущем шаге симметричный ключ. Были получены два текста от одногруппника и определен модифицированный текст.

5. Была проведена атака дополнительной коллизии на хэш-функцию MD-5.

0361
HOLD ON

Спасибо за внимание!
Готова ответить на ваши вопросы.