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

Лабораторная работа № 6

Изучение и исследование алгоритмов хэширования

Студентка: Усачева Дарья, группа 1384

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

Санкт-Петербург, 2024

Цель работы и задачи

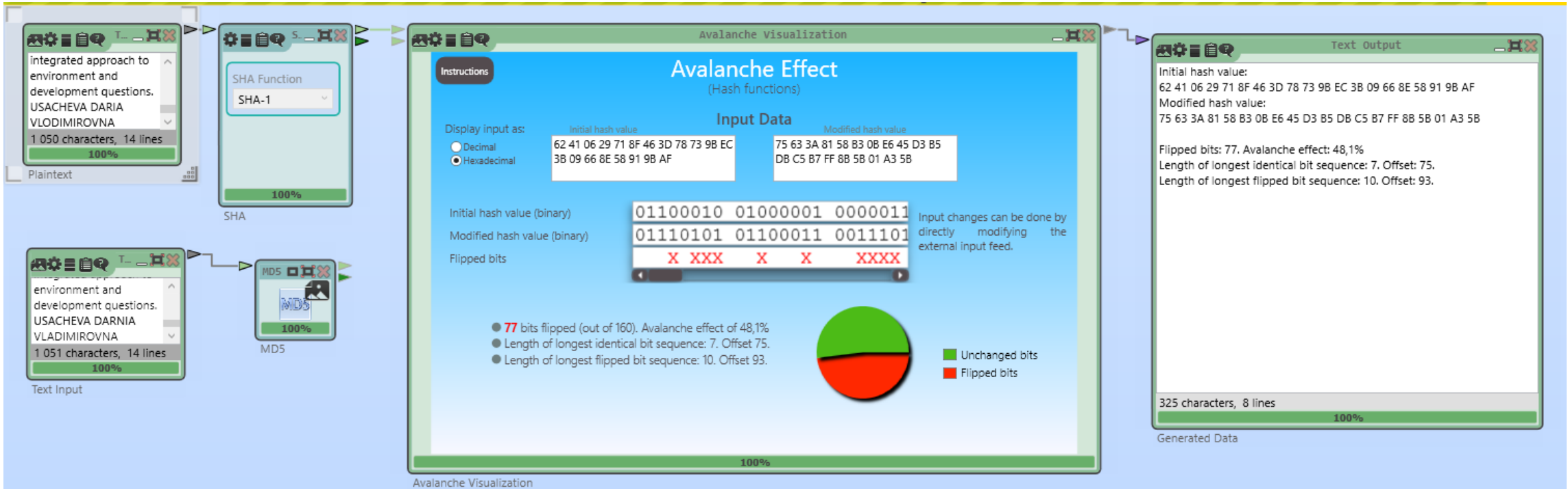
Цель: Повысить свою компетенцию в области алгоритмов хэширования и в криптографии в целом.

Задачи:

1. Оценить лавинный эффект хэш-функции MD5, SHA-1, SHA-256, SHA-512.
2. Изучить алгоритм работы функции перестановок Keccak. Оценить лавинный эффект хэш-функции SHA-3.
3. Изучить алгоритм работы функции диверсификации ключа.
4. Изучить алгоритм вычисления код аутентификации сообщения HMAC.
5. Провести атаку дополнительной коллизии на хэш-функцию MD-5.

Оценка лавинного эффекта хэш-функций MD5, SHA-1, SHA-256, SHA-512

Шаблонная схема оценки лавинного эффекта хэш-функции CrypTool 2

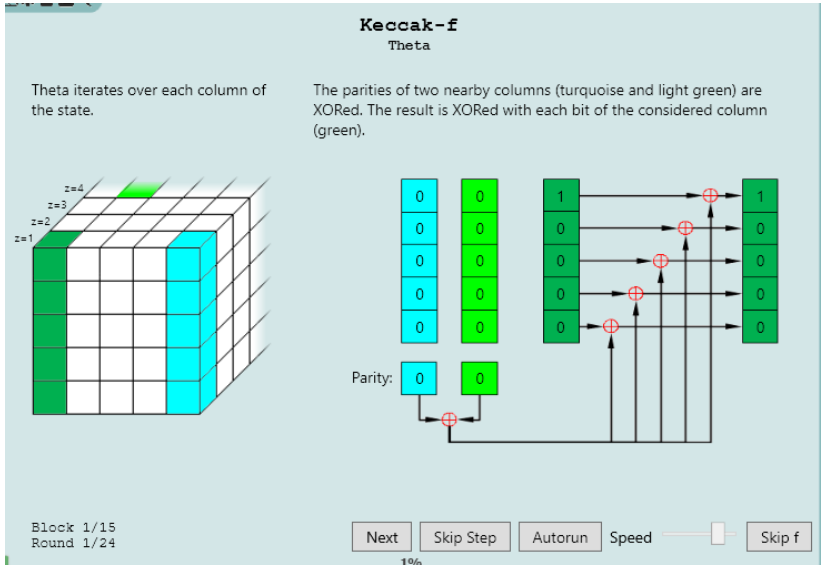


Исследование лавинного эффекта

Название	Номер измерения	Изменение символа	Добавление символа	Удаление символа
MD5	1	57%	53,1%	50%
	2	43%	49,2%	49,2%
	3	55,5%	50,8%	41,4%
	Среднее	51,8%	51%	46,9%
SHA-1	1	50%	61,3%	51,2%
	2	48,1%	51,9%	47,5%
	3	56,3%	56,9%	54,4%
	Среднее	51,5%	56,7%	51%
SHA-256	1	53,9%	48%	54,3%
	2	43%	48,8%	49,6%
	3	47,7%	51,2%	51,2%
	Среднее	48,2%	49,3%	51,7%
SHA-512	1	51,2%	50,8%	49,4%
	2	47,1%	48,4%	51,6%
	3	51,4%	48,6%	50%
	Среднее	49,9%	49,3%	50,3%

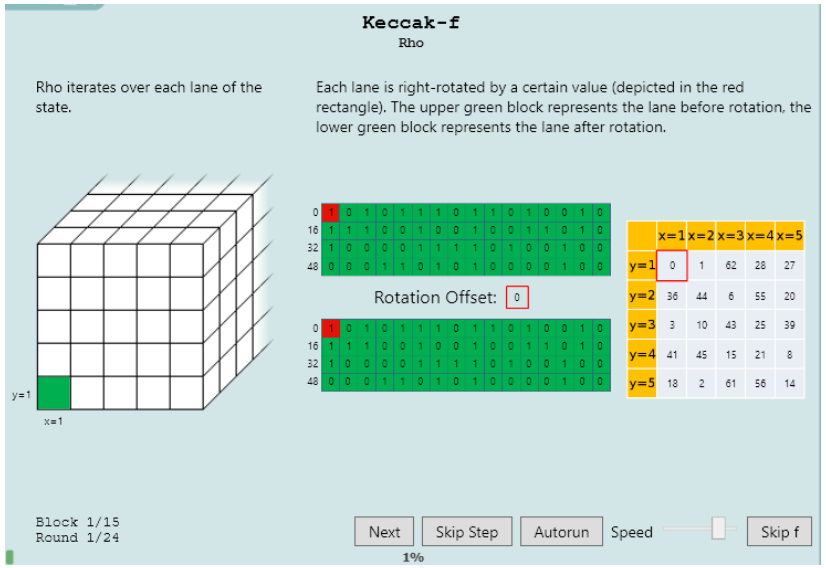
Изучение алгоритма работы функции перестановок Keccak. Оценка лавинного эффекта хэш-функций SHA-3

Преобразования первого раунда



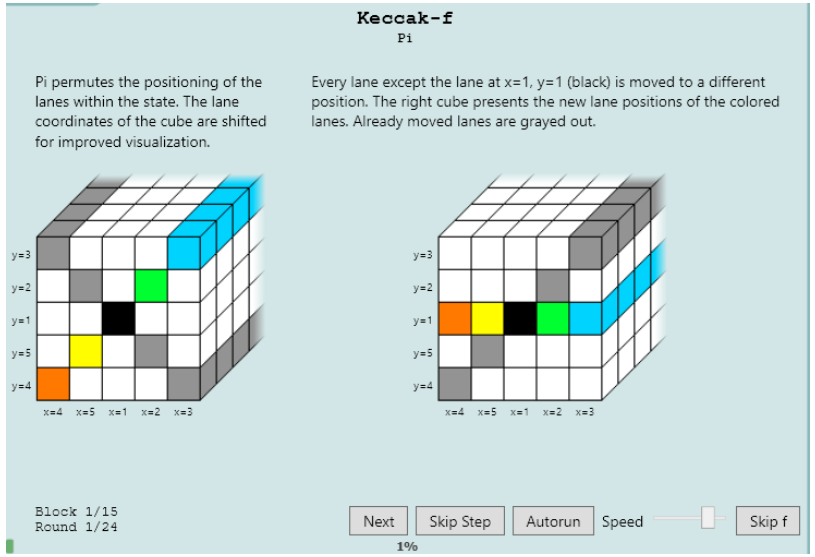
Первым преобразованием в функции перестановок f идет преобразование тета.
В ходе преобразования пересчитывается значения столбца, который имеет темно-зеленый цвет:

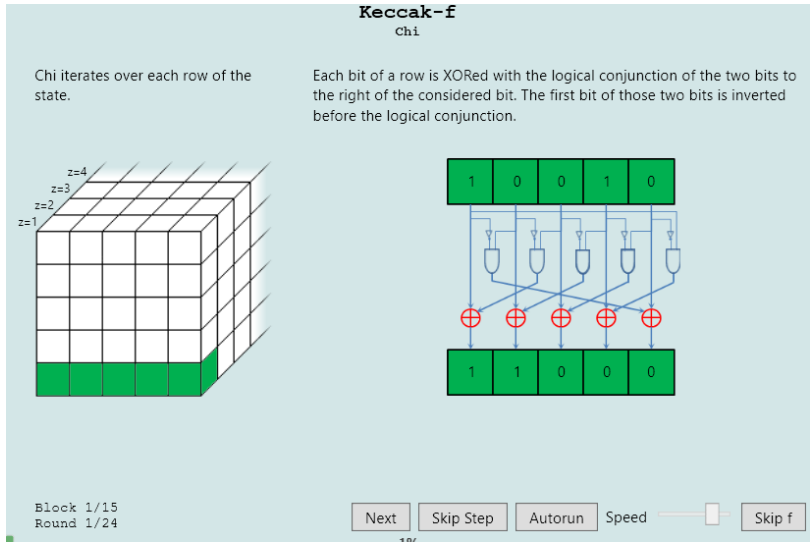
- вычисляется XOR элементов столбцов (сумма по модулю 2) светло-зеленого и бирюзового цвета
- XOR полученных значений из столбцов
- полученное значение XOR с элементами столбца темно-зеленого цвета.



Следующим является преобразование ро.
В ходе преобразования каждый проход (по z) сдвигается циклически вправо на значение, указанное в таблице в соответствии с координатами x, y прохода.
Верхний зеленый блок - проход до поворота.
Нижний зеленый блок - проход после поворота.

Преобразования первого раунда

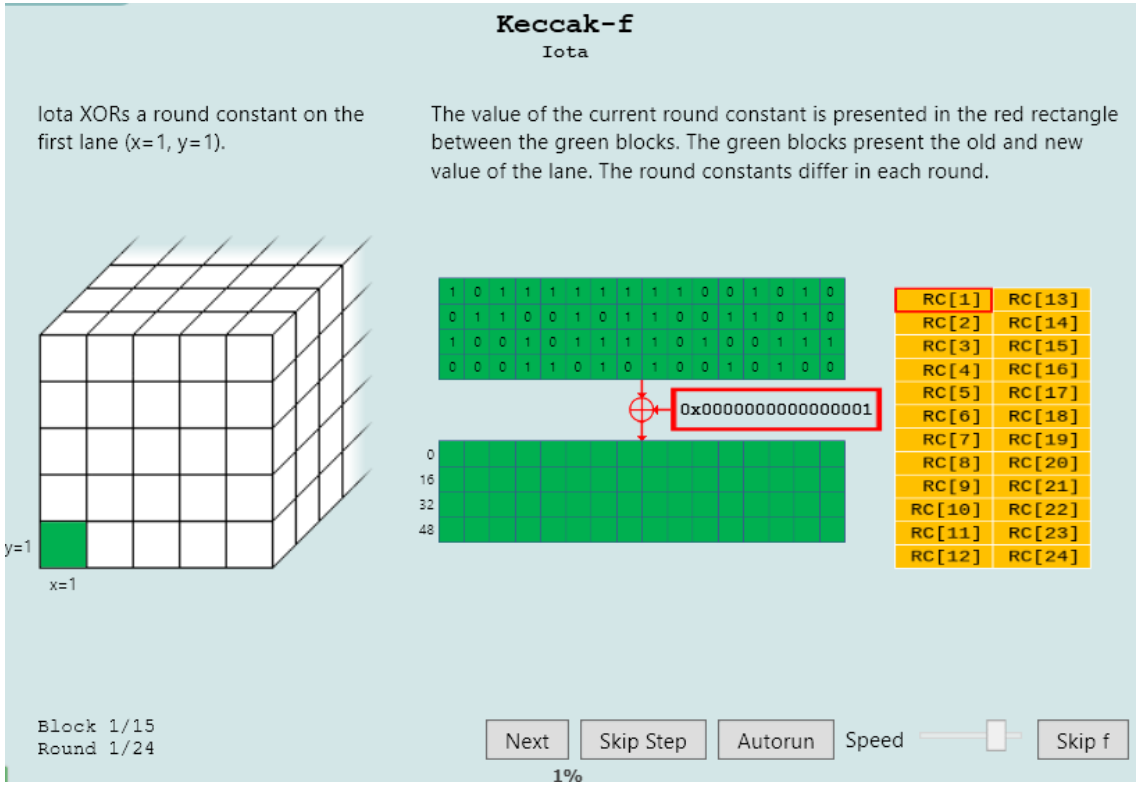




Следующим является преобразование пи.
Для улучшения визуализации координаты полос смещены.
В ходе этого преобразования происходит перезаписывание (перемешивание) проходов матрицы состояний.
Левый куб — начальное промежуточное состояние, правый — новое. Следовательно проходы одного цвета станут на места, указанные этим же же цветом на правом кубе.
Перемещенные проходы выделены серым.
Проход с координатами x = 1, y = 1 не перемещается.

Следующим является преобразование хи, в ходе которого содержимое каждой строки перезаписывается в соответствии с формулой:
A[x,y] = a[x,y] XOR ((NOT a[(x+1)mod 5, y]) AND a[(x+2) mod 5, y])

Преобразования первого раунда



Следующим и заключительным является преобразование йота, в ходе которого содержимое первого прохода (x=1,y=1) XOR-ится с раундовой константой RC[i], где i — номер раунда.
Верхний зеленый блок - проход до XOR.
Нижний зеленый блок - проход после XOR.

Исследование лавинного эффекта

Название	Номер измерения	Изменение символа	Добавление символа	Удаление символа
SHA-3	1	49,4	48,4	53,1
	2	48,8	52,1	49
	3	52,1	48,2	48
	Среднее	50,1	49,6	50,0

Изучение алгоритма работы функции диверсификации ключа

Получение симметричного ключа из персонального пароля

Пароль: USACHEVADARIAVLADIMIROVNA23102002
Ключ: DA 42 8B 87 58 99 BB 7B 33 1F E4 86 CF 53 CE 1D F7 E2 3A 9E

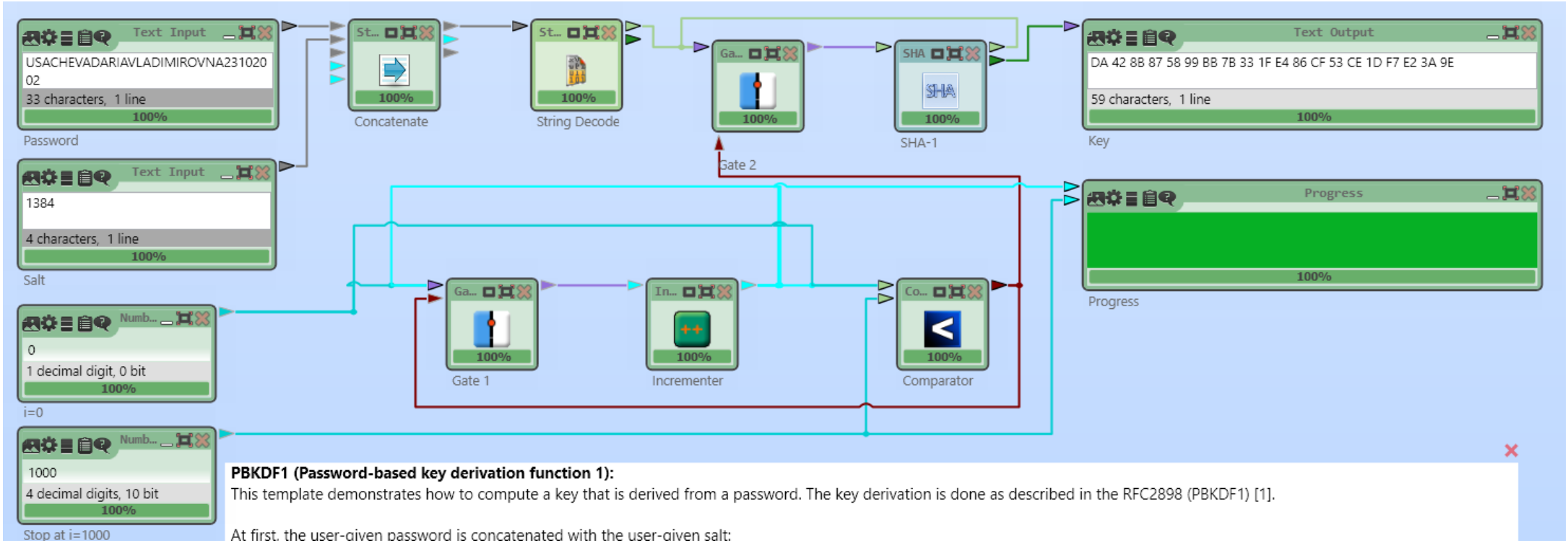
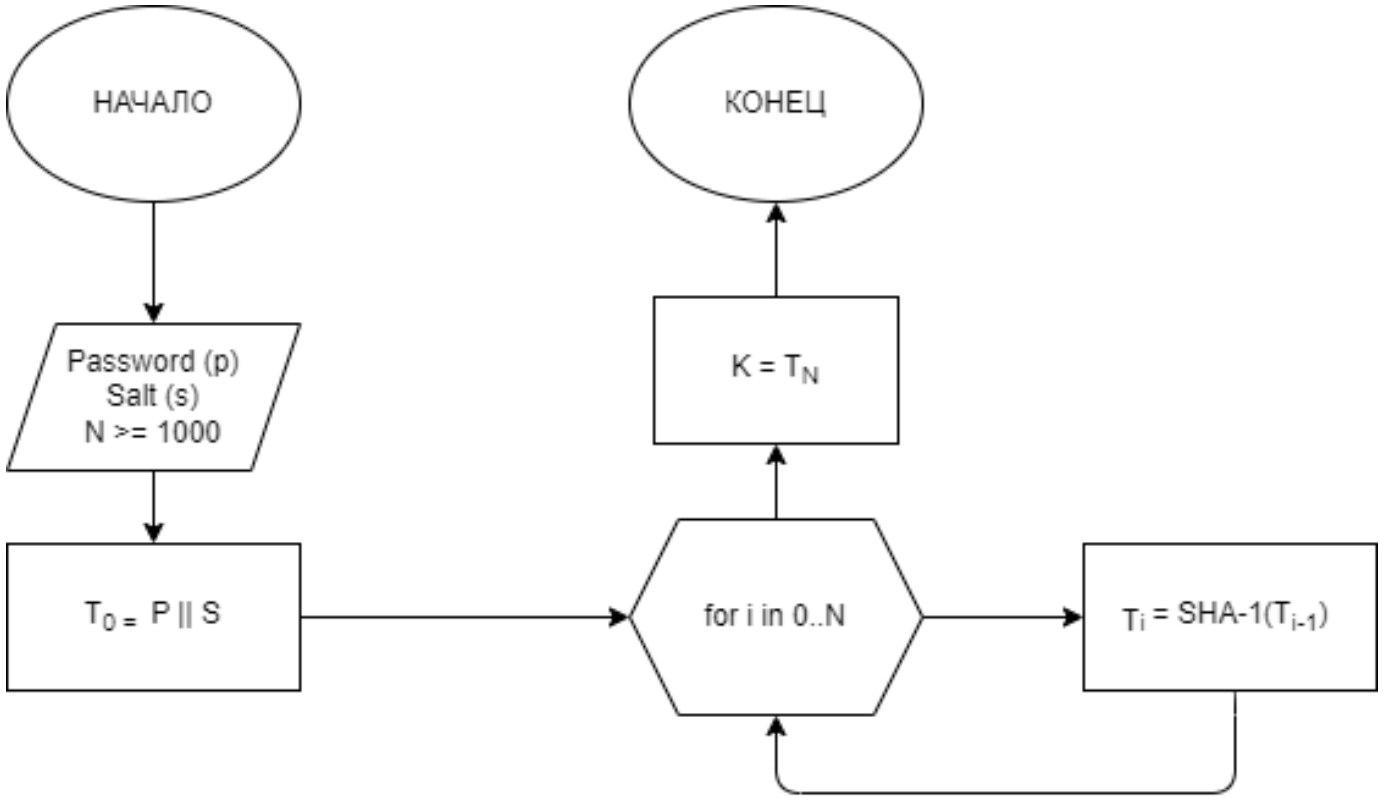


Схема алгоритма функции диверсификации ключа

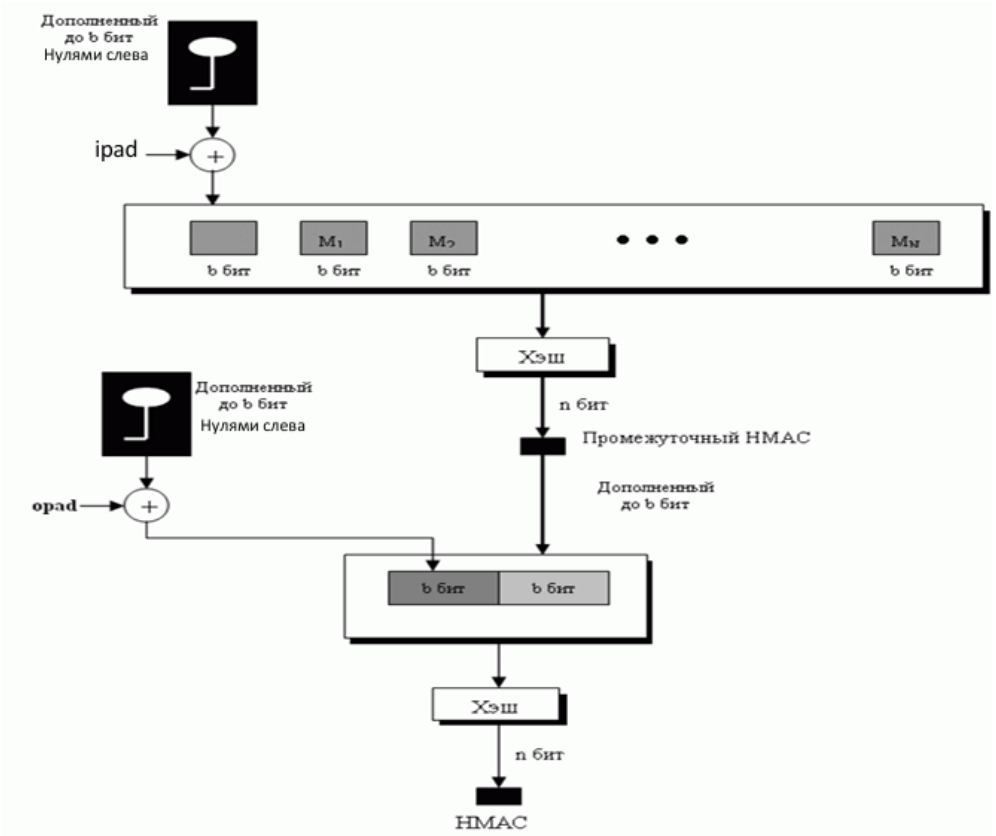


Изучение алгоритма вычисления кода аутентификации сообщения HMAC

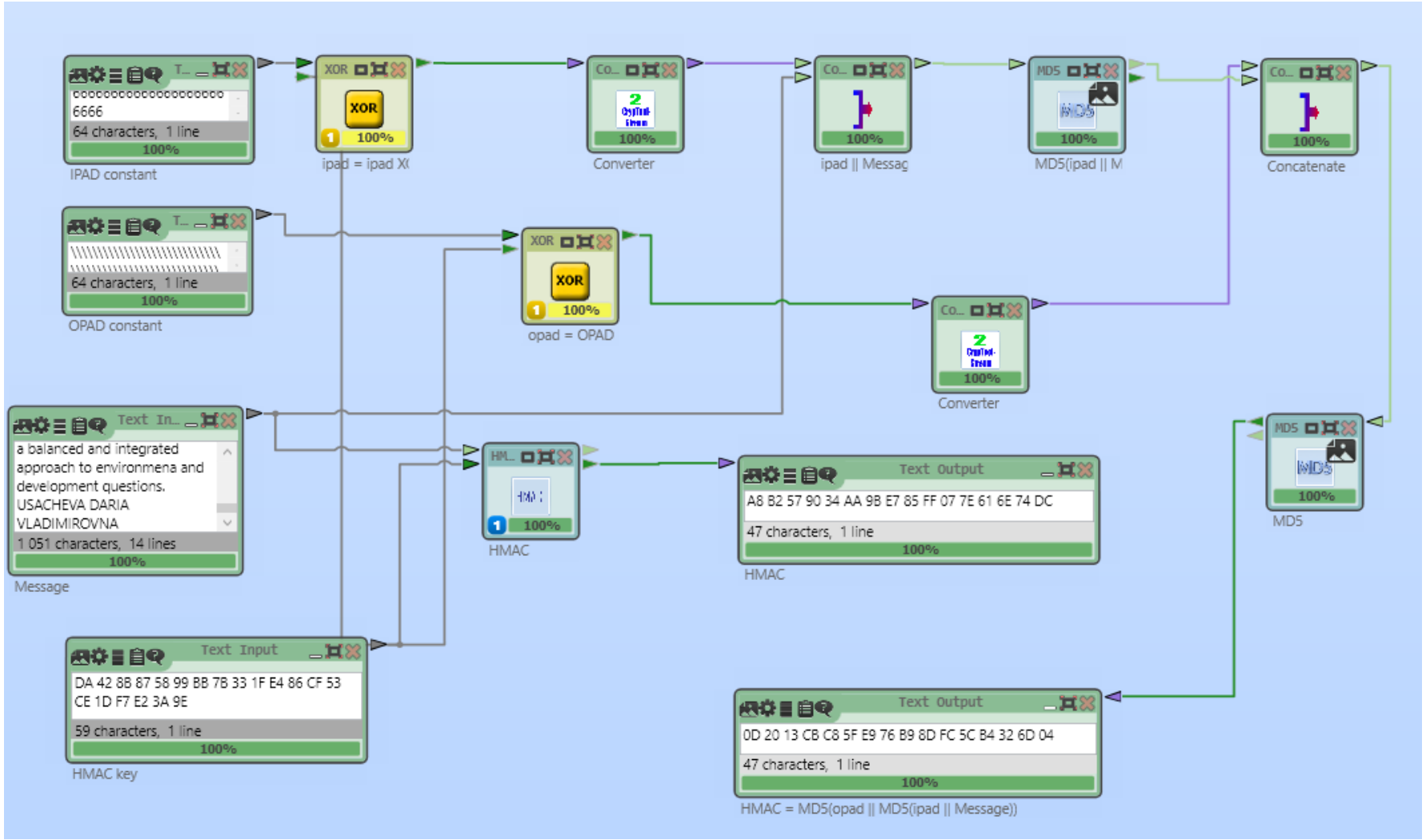
Схема алгоритма вычисления кода аутентификации HMAC

$$\mathrm{HMAC}_K(\text{text}) = H\left\{(K \oplus \text{opad}) \| H\left[(K \oplus \text{ipad}) \| \text{text}\right]\right\},$$

$\oplus$ – операция xor;
|| – конкатенация;
K – секретный ключ;
ipad – блок вида (0x36 0x36 0x36 ... 0x36), где байт 0x36 повторяется b раз;
H – хеш-функция;
opad – блок вида (0x5c 0x5c 0x5c ... 0x5c), где байт 0x5c повторяется b раз.

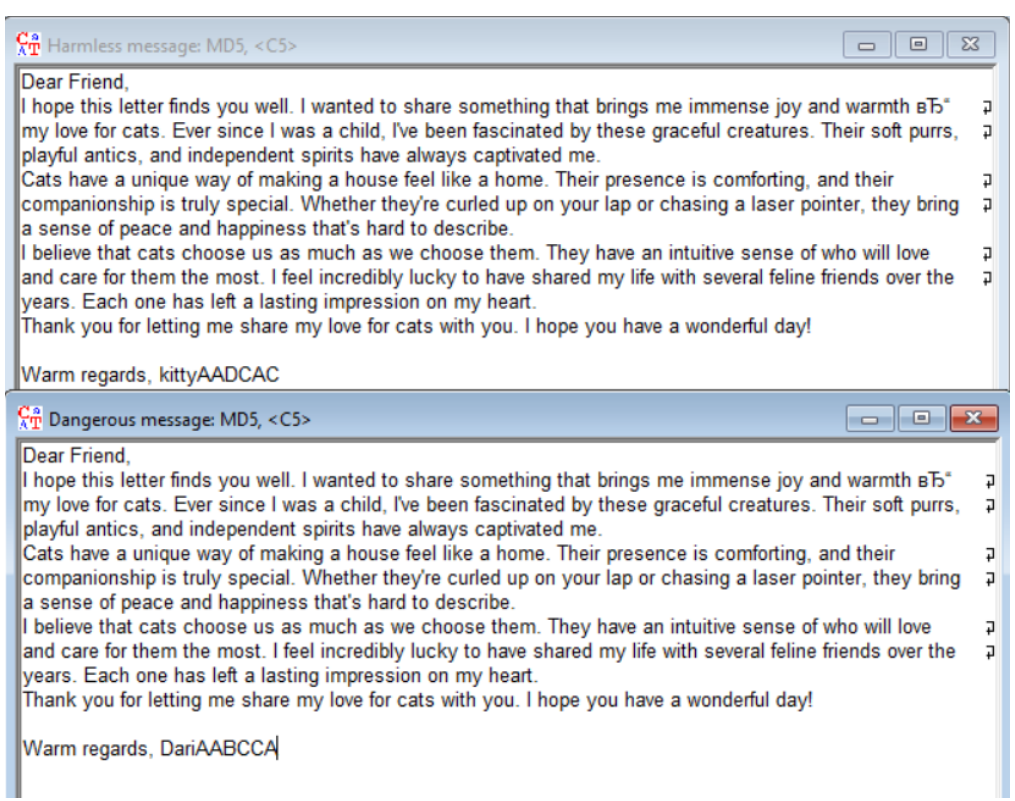


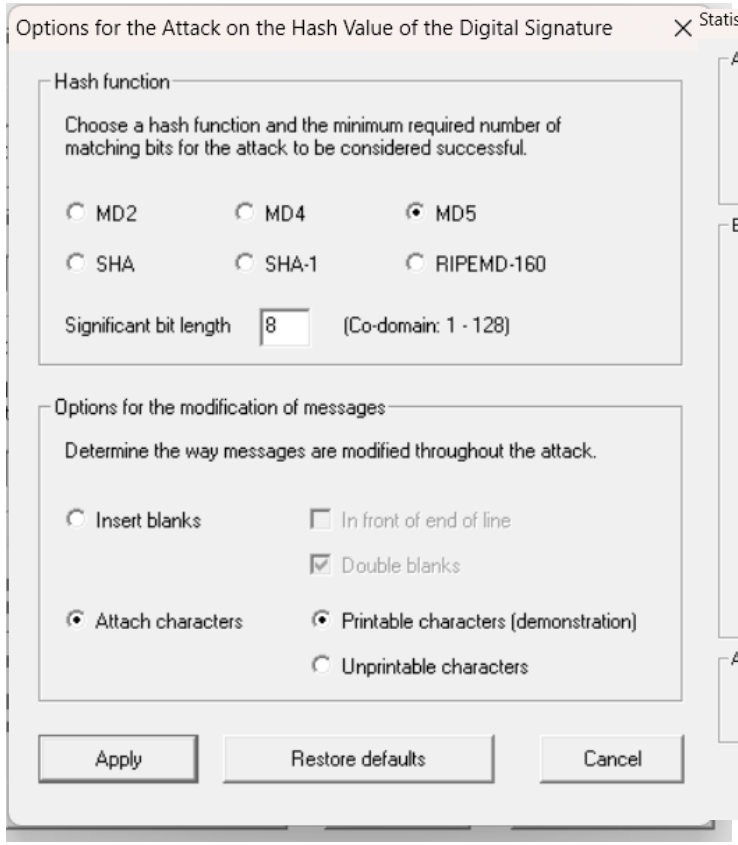
Вычисление кода аутентификации сообщения HMAC

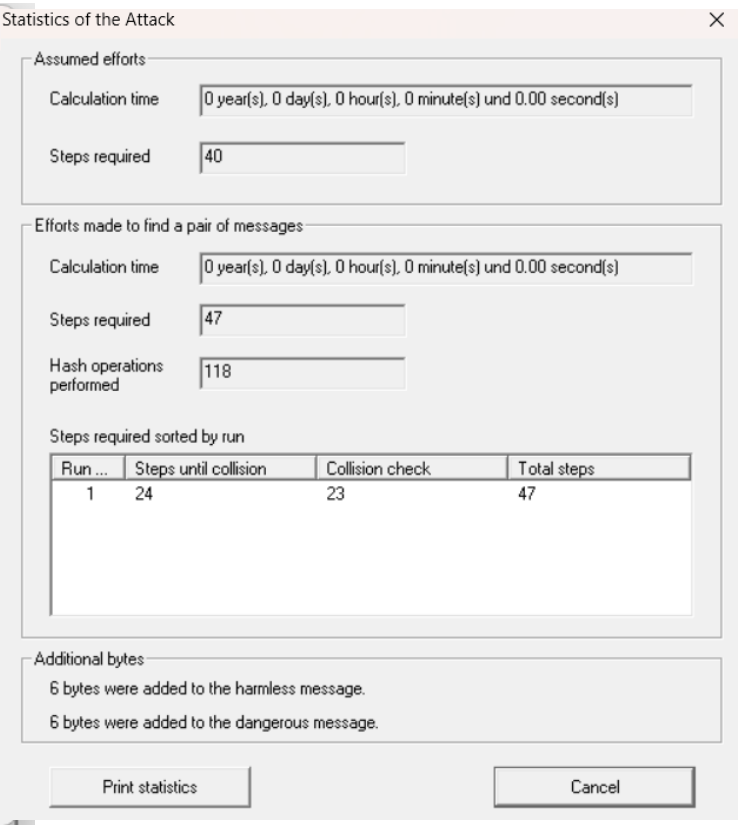


Проведение атаки дополнительной коллизии на хэш-функцию MD-5

Представление результатов атаки







Оценка временной сложности атак

Кол-во бит совпадающих частей	Время выполнения атаки	Кол-во бит совпадающих частей	Время выполнения атаки
8	0 сек	56	52 мин
16	0 сек	64	13 часов
24	0,06 сек	72	9,5 дней
32	1,06 сек	80	150 дней
40	17,07 сек	88	6,6 лет
48	3 мин	96	112 лет

Заключение

1. Изучено влияние лавинного эффекта на хэш-функции MD-5, SHA-1, SHA-256, SHA-512 с использованием шаблонных схем в CrypTool 2. На основе результатов эксперимента, собранных в таблице сделан вывод, что в среднее значение величины лавинного эффекта у всех хэш-функций 50%
2. Изучен алгоритм работы функции перестановок Keccak с использованием шаблонной схемы в CrypTool 2. Выполнено пять преобразований первого раунда: Тета (θ), Ро (ρ), Пи (π), Хи (χ), Йота (ι). Изучено влияние лавинного эффекта на хэш-функцию SHA-3 с использованием шаблонной схемы в CrypTool 2 На основе результатов эксперимента, собранных в таблице сделан вывод, что данная хэш-функция обладает величина лавинного эффекта также в районе 50%.
3. Изучен алгоритм диверсификации ключа, в результате которого получен симметричный ключ на основе заданного пароля.
4. Изучен алгоритм вычисления кода аутентификации сообщения HMAC с использованием одноимённой шаблонной схемы из CrypTool 2, где в качестве ключа использован симметричный ключ, полученный на предыдущем этапе.
5. Изучена и проведена атака дополнительной коллизии на хэш-функцию MD-5 в CrypTool 1, в результате которой определены значения времени для различного количества совпадающих бит дайджеста. Для хэш-функции с n-битным значением сложность атаки дополнительной коллизии — поиска двух разных значений с одинаковыми хэш-кодами — примерно равна O(2^n)