**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №6**

**по дисциплине «Криптография и защита информации»**

Тема: **Изучение хэш-функций**

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.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.

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

***Основные параметры и обобщенная схема хэш-функций MD5, SHA-1***

MD5:

* MD буфер, входное сообщение, дополненное недостающими битами (от 1 до 448 бит) и 64-битным представлением длины исходного сообщения, функция сжатия (MD буфер, массив вычисляемых величин (32 бита) – T, 4 элементарных функции (), – циклический сдвиг).
* Схема:

|  |  |  |
| --- | --- | --- |
|  |  |  |

SHA-1:

* MD буфер, входное сообщение, дополненное недостающими битами (от 1 до 448 бит) и 64-битным представлением длины исходного сообщения, функция сжатия (MD буфер, константа , 4 элементарных функции (), – циклические сдвиги, – 32-битовые слова (80 слов)).
* Схема:

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. Открыть текст не менее 1000 знаков. Добавить свое ФИО последней строкой. Перейти к утилите Indiv.Procedures->Hash->Hash Demonstration..

Возьмем текст из reference в CrypTool и добавим своё ФИО. Результат представлен на рис. 1.

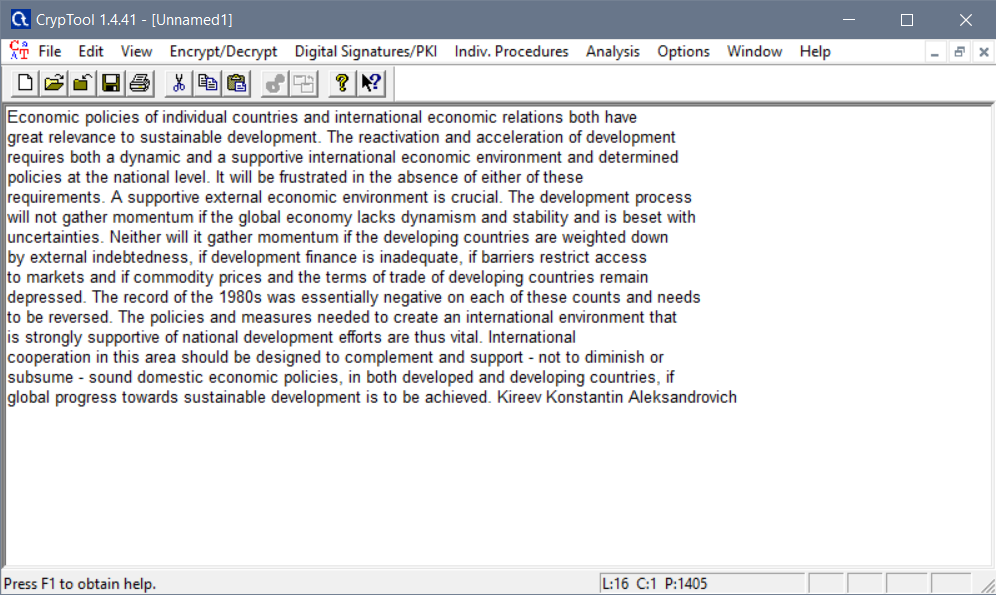


Рисунок 1 – Текст для хэш-функций

1. Задать хэш-функцию, подлежащую исследованию: MD5, SHA-1, SHA-256, SHA-512.,
2. Для каждой хэш-функции повторить следующие действия:
   1. Измените (добавлением, заменой, удалением символа) исходный файле
   2. Зафиксировать количество измененных битов в дайджесте модифицированного сообщения.
   3. Вернуть сообщение в исходное состояние.
3. Выполните процедуру 3 раза (добавлением, заменой, удалением символа) и подсчитайте среднее количество измененных бит дайджеста. Зафиксировать результаты в таблице.

Сведем выполнение пунктов 2-4 в единую таблицу 1 для простоты анализа.

*Таблица 1 – Фактические и усредненные параметры лавинного эффекта*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Хэш-функция*** | ***Тип изменения*** | ***Количество измененных битов в дайджесте*** | ***Среднее количество измененных бит дайджеста*** |
| MD5 | добавление | 70 бит – 54.69% | 69.3 бит – 54.17% |
| замена | 76 бит – 59.38% |
| удаление символа | 62 бит – 48.44% |
| SHA-1 | добавление | 78 бит – 48.75% | 80.6 бит – 50.42% |
| замена | 88 бит – 55% |
| удаление символа | 76 бит – 47.5% |
| SHA-256 | добавление | 127 бит – 49.61% | 130 бит – 50.78% |
| замена | 129 бит – 50.39% |
| удаление символа | 134 бит – 52.34% |
| SHA-512 | добавление | 238 бит – 46.48% | 246.6 бит – 48.18% |
| замена | 252 бит – 49.22% |
| удаление символа | 250 бит – 48.83% |

**Хэш-функция SHA-3.**

***Основные параметры и обобщенная схема хэш-функции Keccak Hash, (SHA-3) на основе изученной презентации***

* Основные параметры: исходное сообщение , внутреннее состояние , функция - многораундовая бесключевая псевдослучайная перестановка, длина слова . Размер части состояния, который записывается и считывается, называется «скоростью» и обозначается , а размер части, которая нетронута вводом / выводом, называется «ёмкостью» и обозначается .
* Схема:

|  |  |
| --- | --- |
|  |  |

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

Шаблон с установленными настройками представлен на рис. 2

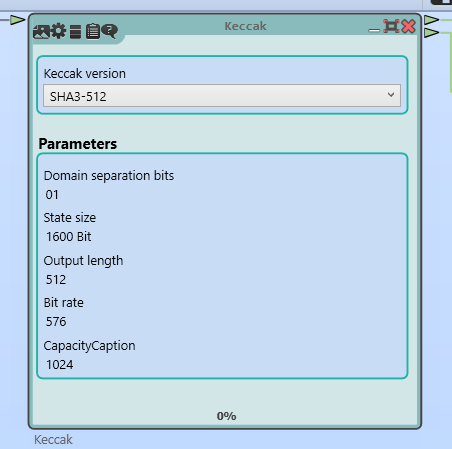


Рисунок 2 – Изменённые настройки

1. Загрузить файл из предыдущего задания

Шаблон с исходным текстом представлен на рис. 3.

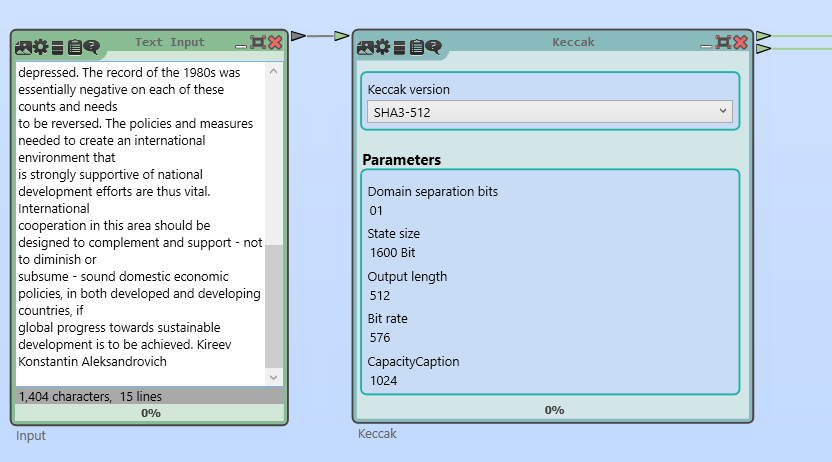


Рисунок 3 – Загруженный текст

1. Запустить проигрывание шаблона в режиме ручного управления:
   1. Сохранить скриншоты преобразований первого раунда
   2. Сохранить скриншот заключительной фазы
   3. Сохранить значение дайджеста

Запустим проигрывание шаблона в режиме ручного управления.

Так как CrypTool 2 показывает только 20 раундов, для демонстрации последнего был использован сторонний сайт. Скриншоты преобразований первого раунда представлены на рис. 4 -5. Скриншот заключительной фазы представлен на рис 6. Значение дайджеста представлено на рис 7.

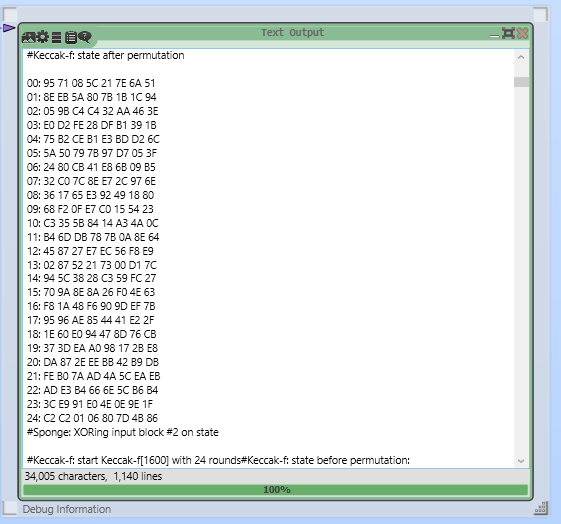


Рисунок 4 – Преобразование первого раунда в CrypTool 2

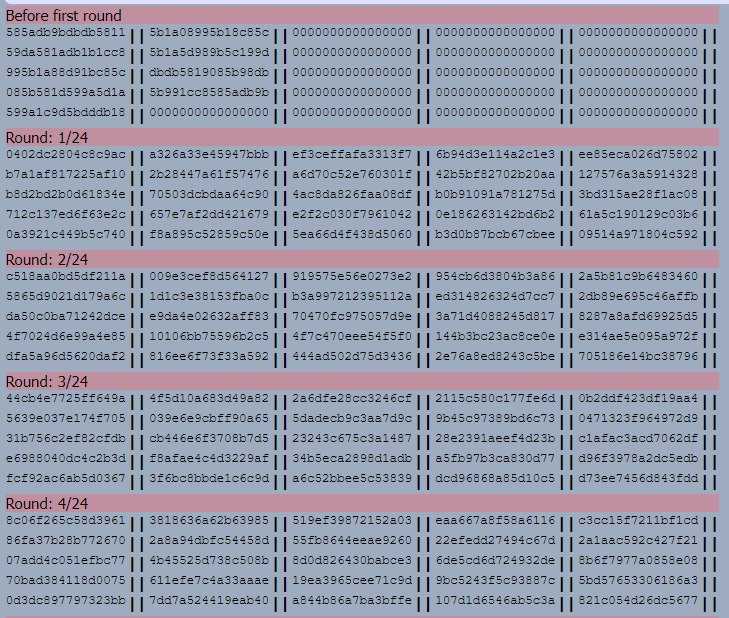


Рисунок 5 – Подробные преобразования в первом раунде

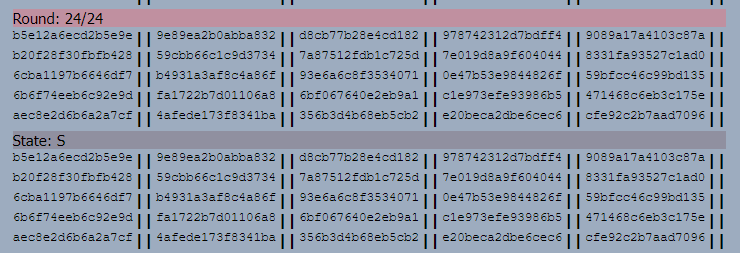


Рисунок 6 – Заключительная фаза преобразований

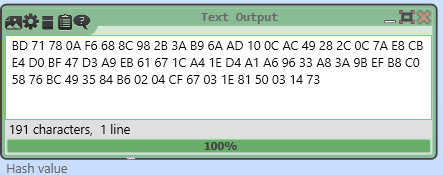


Рисунок 7 – Значение дайджеста

Значение дайджеста:

BD 71 78 0A F6 68 8C 98 2B 3A B9 6A AD 10 0C AC 49 28 2C 0C 7A E8 CB E4 D0 BF 47 D3 A9 EB 61 67 1C A4 1E D4 A1 A6 96 33 A8 3A 9B EF B8 C0 58 76 BC 49 35 84 B6 02 04 CF 67 03 1E 81 50 03 14 73

1. Вычислить значения дайджеста для модифицированных текстов из предыдущего задания

Сведем результат вычислений в таблицу 2.

*Таблица 2 – Значения дайджеста при модификации исходного текста*

|  |  |
| --- | --- |
| ***Тип изменения*** | ***Значение дайджеста*** |
| добавление | A0 17 B7 73 65 4E DB 8C E8 45 00 6A 17 06 4F C6 6E 4B 70 C3 3C 92 55 44 D5 FD F7 49 89 15 36 1B 0B D6 13 BA C3 0D EE D1 DA 89 B6 34 FC BC AA B0 74 13 BE EF 7D E5 20 18 A4 36 37 67 D1 C6 00 5D |
| замена | DB 96 D0 3E 9D A7 24 3E 9D B5 2C ED 4A B4 BF D1 BA 1F CF F9 C6 3A 43 D2 AF 5A E5 73 DD 44 86 C8 B5 40 E1 4F C4 AD A5 BD 5F BB 8C 14 AA A6 0E 73 29 A2 0E 0E CC 27 01 E2 CE CA 3E 99 38 B6 81 DC |
| удаление символа | E7 B8 40 10 93 B3 9F 6D 8A E4 67 AD 48 55 7B 85 BF 35 AC 47 53 AB A9 98 22 F0 FE 9E FD 69 46 62 0E 46 F2 4C 6B 29 AF 2E EE C8 43 E0 1C BB 9B 06 AB A0 5A 36 EA F7 50 FC 25 D4 C8 F1 3D 42 D0 FF |
| Исходное значение | BD 71 78 0A F6 68 8C 98 2B 3A B9 6A AD 10 0C AC 49 28 2C 0C 7A E8 CB E4 D0 BF 47 D3 A9 EB 61 67 1C A4 1E D4 A1 A6 96 33 A8 3A 9B EF B8 C0 58 76 BC 49 35 84 B6 02 04 CF 67 03 1E 81 50 03 14 73 |

1. Подсчитать лавинный эффект с помощью самостоятельно разработанной автоматизированной процедуры

Для подсчета лавинного эффекта воспользуемся встроенным шаблоном Avalanche effect в CrypTool2 и изменим хэш-функцию на Keccak. Представим полученные значения лавинного эффекта в таблице 3 для большей наглядности.

*Таблица 3 – Фактические и усредненные параметры лавинного эффекта*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Хэш-функция*** | ***Тип изменения*** | ***Количество измененных битов в дайджесте*** | ***Среднее количество измененных бит дайджеста*** |
| Keccak Hash (SHA-3) | добавление | 238 бит – 46.5% | 546.6 бит – 48.17 % |
| замена | 252 бит – 49.2 % |
| удаление символа | 250 бит – 48.8% |

**Контроль целостности по коду HMAC.**

1. Выбрать текст на английском языке (не менее 1000 знаков), добавить собственное ФИО и сохранить в файле формата .TXT.

Выбранный и изменённый текст приведен на рис. 8.

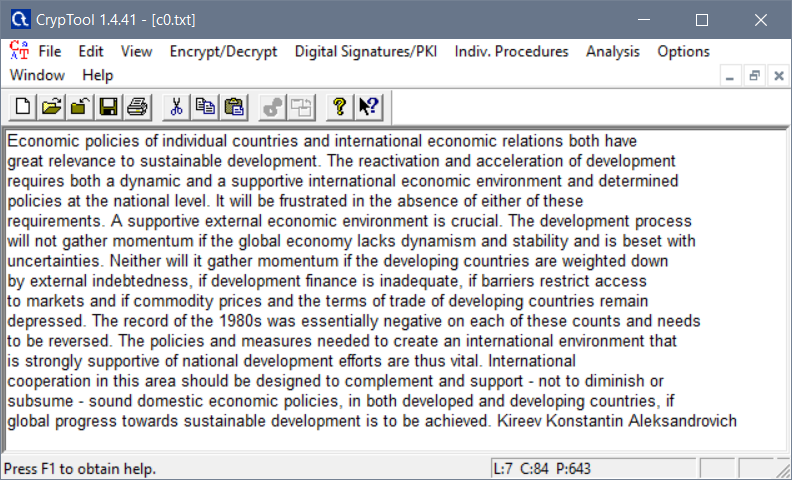


Рисунок 8 – Исходный текст

1. 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.

Пароль: adfknSnfdfMLSnlk34

Параметры генерации:

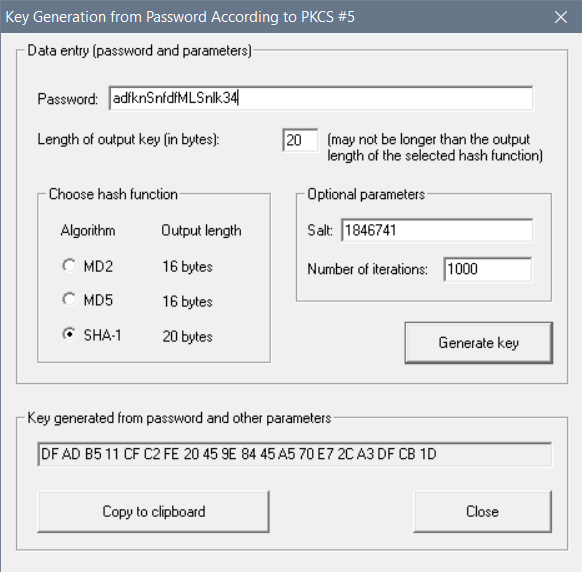


Рисунок 9 – Параметры генерируемого ключа

Сгенерированный секретный ключ:

DF AD B5 11 CF C2 FE 20 45 9E 84 45 A5 70 E7 2C A3 DF CB 1D

1. 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.

Параметры генерации:

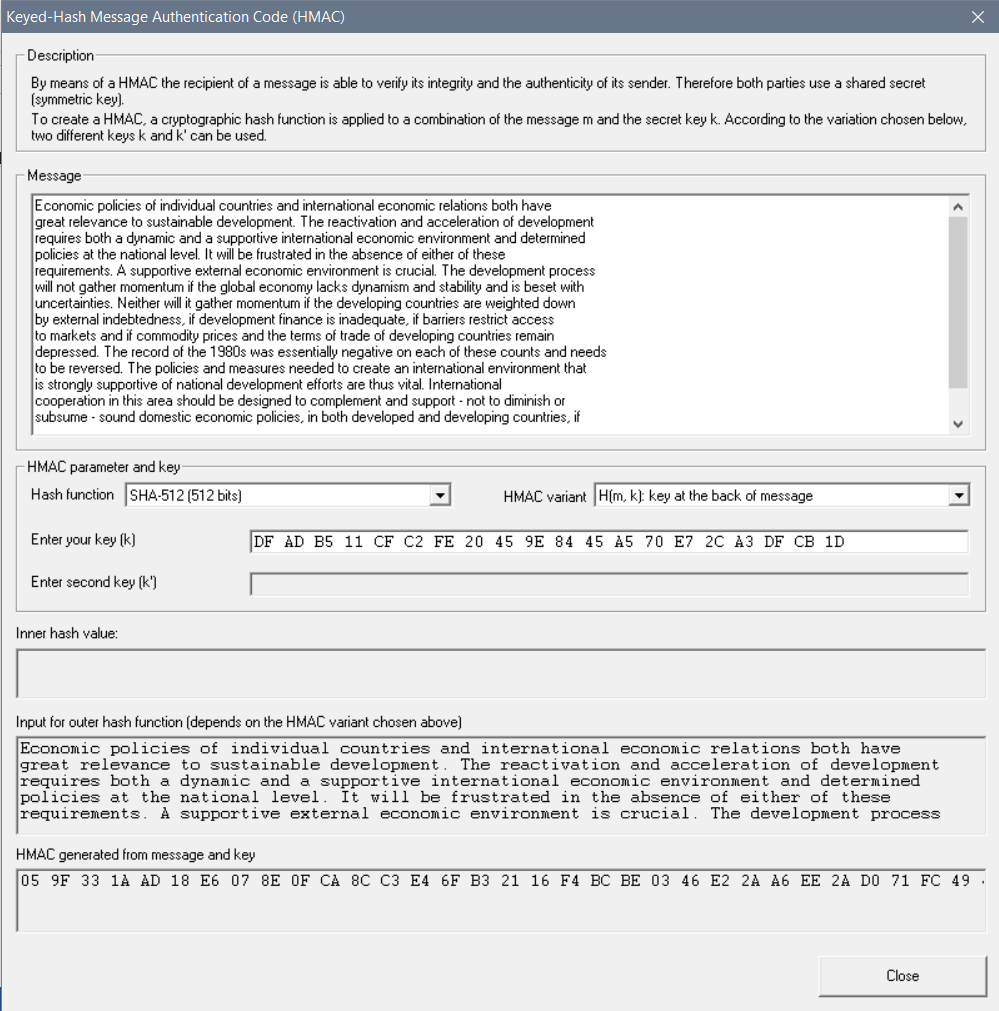


Рисунок 10 – Параметры генерации HMAC

Полученный HMAC: 05 9F 33 1A AD 18 E6 07 8E 0F CA 8C C3 E4 6F B3 21 16 F4 BC BE 03 46 E2 2A A6 EE 2A D0 71 FC 49 4B 5B DC 71 4B 2F B7 A6 32 A5 75 0C 20 3D 02 80 6D B5 E4 FA 5E F1 A4 7D C6 A4 70 2C 57 12 9B 80

1. Передать пароль, HMAC (и его характеристики), исходный текст и модифицированный текст коллеге, не раскрывая, какой текст является корректным. Попросите коллегу определить это самостоятельно.

В таблице 4 представлены полученные значения у коллеги.

*Описание действий передающий стороны на примере выполненного задания:*

Сначала отправитель должен придумать достаточно сложный пароль, далее необходимо настроить достаточно надежную генерацию ключа – CrypTool предлагает использовать по умолчанию seed и 1000 итераций. После этого необходимо определить параметры для HMAC – хэш-функцию и конструкцию добавления. После этого вычисляется сам HMAC и сообщение передаётся получателю.

*Описание действий принимающей стороны на примере выполненного задания:*

Предполагается, что получатель знает характеристики для генерации секретного ключа. Тогда, первым шагом будет сгенерировать секретный ключ по заданным параметрам. Далее, получатель должен вычислить хэш полученного сообщения вместе с секретным ключом. Потом он сравнивает полученное значение хэша с тем, которое он получил. Сообщение является подлинным только в том случае, если два значения хэша равны.

*Таблица 4 – Эксперимент*

|  |  |
| --- | --- |
| Исходный текст:  Economic policies of individual countries and international economic relations both have  great relevance to sustainable development. The reactivation and acceleration of development  requires both a dynamic and a supportive international economic environment and determined  policies at the national level. It will be frustrated in the absence of either of these  requirements. A supportive external economic environment is crucial. The development process  will not gather momentum if the global economy lacks dynamism and stability and is beset with  uncertainties. Neither will it gather momentum if the developing countries are weighted down  by external indebtedness, if development finance is inadequate, if barriers restrict access  to markets and if commodity prices and the terms of trade of developing countries remain  depressed. The record of the 1980s was essentially negative on each of these counts and needs  to be reversed. The policies and measures needed to create an international environment that  is strongly supportive of national development efforts are thus vital. International  cooperation in this area should be designed to complement and support - not to diminish or  subsume - sound domestic economic policies, in both developed and developing countries, if global progress towards sustainable development is to be achieved. Kireev Konstantin Aleksandrovich | Модифицированный текст:  Economic policies of individual countries and international economic relations both havedfgg  great relevance to sustainable development. The reactivation and acceleration of development dfgfd  requires both a dynamic and a supportive international economic environment and determined  policies at the national level. It will be frustrated in the absence of either of these dgdfg  requirements. A supportive external economic environment is crucial. The development process vfgdfg  will not gather momentum if the global economy lacks dynamism and stability and is beset with  uncertainties. Neither will it gather momentum if the developing countries are weighted down  by external indebtedness, if development finance is inadequate, if barriers restrict access dfg  to markets and if commodity prices and the terms of trade of developing countries remain fgfdg  depressed. The record of the 1980s dfgfgdfwas essentially negative on each of these counts and needs gfdgdf  to be reversed. The policies and measures needed to create an international environment that  is strongly supportive of national development efforts are thus vital. International dfgdfg  cooperation in this area shouldg be designed to complement and support - not to diminish or dfgdfg  subsume - sound domestic economic policies, in both developed and developing countries, if global progress towards sustainable development is to be achieved. Kireev Konstantin Aleksandrovich |
| Переданный HMAC:  05 9F 33 1A AD 18 E6 07 8E 0F CA 8C C3 E4 6F B3 21 16 F4 BC BE 03 46 E2 2A A6 EE 2A D0 71 FC 49 4B 5B DC 71 4B 2F B7 A6 32 A5 75 0C 20 3D 02 80 6D B5 E4 FA 5E F1 A4 7D C6 A4 70 2C 57 12 9B 80 | Переданный HMAC:  05 9F 33 1A AD 18 E6 07 8E 0F CA 8C C3 E4 6F B3 21 16 F4 BC BE 03 46 E2 2A A6 EE 2A D0 71 FC 49 4B 5B DC 71 4B 2F B7 A6 32 A5 75 0C 20 3D 02 80 6D B5 E4 FA 5E F1 A4 7D C6 A4 70 2C 57 12 9B 80 |
| Вычисленное получателем значение:  05 9F 33 1A AD 18 E6 07 8E 0F CA 8C C3 E4 6F B3 21 16 F4 BC BE 03 46 E2 2A A6 EE 2A D0 71 FC 49 4B 5B DC 71 4B 2F B7 A6 32 A5 75 0C 20 3D 02 80 6D B5 E4 FA 5E F1 A4 7D C6 A4 70 2C 57 12 9B 80 | Вычисленное получателем значение:  EA DB D6 E3 13 D8 AB 6B 0C CF 91 A5 E0 84 05 E5 D2 F3 AE 7C 9E CF 2B B2 C3 1F DC FE DA 4C C4 8C B8 52 B0 0D 43 13 80 A1 0F A6 34 EE 29 8F 17 42 CE 67 4A 39 14 1D 14 84 A9 64 68 D4 21 32 E5 CF |

**Атака дополнительной коллизии на хэш-функцию.**

***Описание атаки в терминах парадокса «дня рождения».***

Атака строится на парадоксе «дня рождения». Сам парадокс состоит в следующем:

Каково минимальное число k - студентов в аудитории, такое, что с заданной вероятностью по крайней мере два студента имеют тот же самый день рождения? Было вычислено, что если k = 23, то с вероятностью P > 0,5 двое из студентов родились в один день (игнорируя год их рождения).

Суть метода состоит в значительном уменьшении количества передаваемых хеш-функции аргументов, необходимого для обнаружения коллизии, поскольку если хеш-функция генерирует ‑битное значение, то число случайных аргументов хеш-функции, для которого с большой вероятностью будет обнаружена хотя бы одна коллизия хеш-функции (то есть найдётся хотя бы одна пара равных хеш-кодов, полученных на разных аргументах), равно не , а только около .

1. Сформировать два текста на английском языке - один истинный, а другой фальсифицированный. Сохранить тексты в файлах формата \*.txt.

Сформированные тексты представлены на рис. 11 и 12 соответственно.



Рисунок 11 – Истинный текст

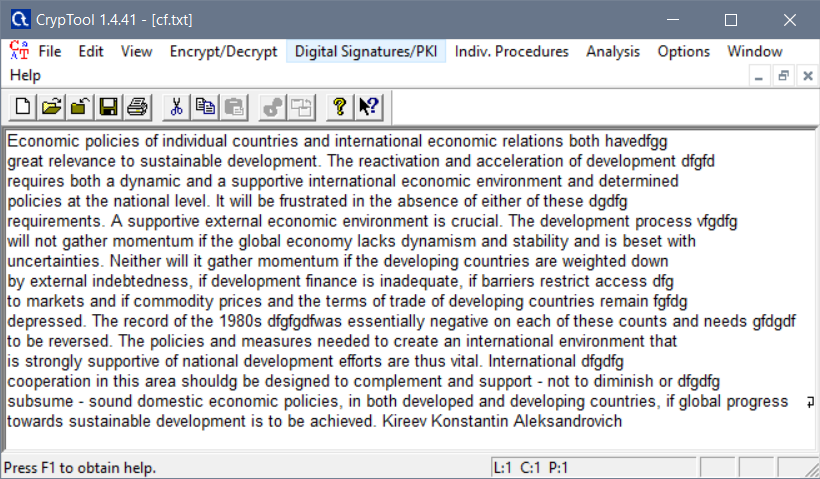


Рисунок 12 – Фальсифицированный текст

1. Утилитой Analysis-> Attack on the hash value... произвести модификацию сообщений для получения одинакового дайджеста. В качестве метода модификации выбрать Attach characters-> Printable characters.

Функция для исследований SHA-1.

1. Проверить, что дайджесты сообщений действительно совпадают с заданной точностью. Проверка на совпадение представлена в Приложении А.
2. Сохранить исходные тексты, итоговые тексты и статистику атаки для отчета. Исходные тексты представлены в пункте 1. Итоговые тексты приведены в приложении А.
3. Зафиксировать временную сложность атаки для 8, 16, 32,40, 48, … бит совпадающих частей дайджестов.

Временная сложность атаки для заданного числа бит приведена в таблице 5.

*Таблица 5 – Временная сложность атаки для n бит совпадающих частей дайджестов*

|  |  |  |
| --- | --- | --- |
| ***Количество значащих бит*** | ***Время атаки*** | ***Количество запусков и число шагов на подбор совпадений*** |
| 8 | 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s) | 2 итерации, 99 обращение к хэш-функции, 35 шагов |
| 16 | 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s) | 2 итерации, 2.424 обращений к хэш-функции, 857 шагов |
| 32 | 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 1.51 second(s) | 1 итерации, 849.980 обращений к хэш-функции, 302.726 шагов |
| 40 | 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 30.57 second(s) | 4 итерации, 16.296.019 обращений к хэш-функции, 5.778.257 шагов |
| 48 | 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 57.48 second(s) | 1 итерация, 28.466.685 обращений к хэш-функции, 10.177.425 шагов |
| 96 | 1.2e+002 years | - |
| 104 | 1.9e+003 years | - |

**Выводы.**

* Проведено исследование лавинного эффекта для представленных хэш-функций.

Для каждой функции замена, добавление, удаление одного символа в прообразе приводило в среднем к изменению 50% битов значения дайджеста. Кроме того, при любом изменении текста хэш-значения модифицированного файла абсолютно не совпадали с исходными. Следовательно, представленные функции обладают лавинным эффектом.

* Проведено исследование лавинного эффекта для хэш-функции Keccak (SHA-3).

Выявлено, что данная функция им обладает – при модификации одного символа в сообщении происходило изменение в среднем 48% бит в хэше. Также, дайджест модифицированного файла не совпадал с исходным. Сравнивания количество измененных бит дайджеста для каждого из типов изменений у всех исследуемых функций, было обнаружено, что наибольший процент получается при замене символа.

* Изучен HMAC – один из механизмов проверки целостности информации. HMAC вычисляется по формуле:

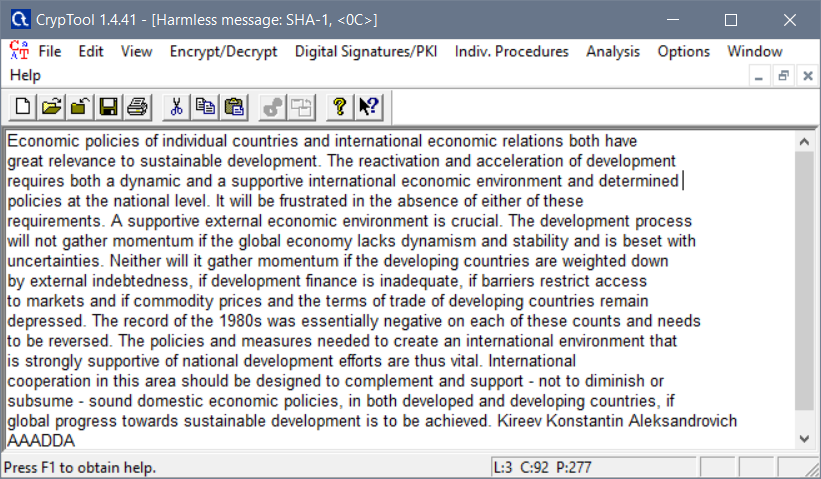
Для создания секретного ключа используется генерация на основе пароля. Секретный ключ – результат повторного использования хэш-функции над заданным паролем. Количество итераций хэша значительно увеличивает количество усилий, необходимых для успешной атаки.

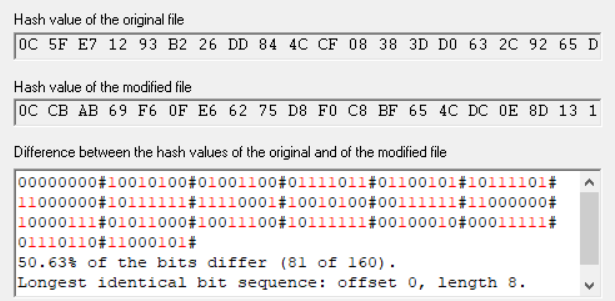
* Изучена атака дополнительной коллизии.

Выявлено, что для двух сообщений и временная сложность атаки вычисления 48 и более бит растет экспоненциально для SHA-1. Цель атаки – получение полностью одинакового дайджеста для двух сообщений (пары ) – занимает 1.9e+003 лет. Следовательно, данные хэш-функции устойчивы к коллизиям.

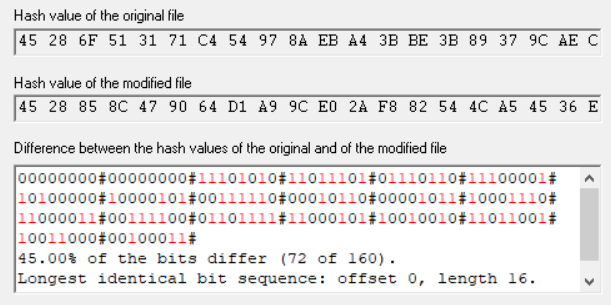
ПРИЛОЖЕНИЕ А

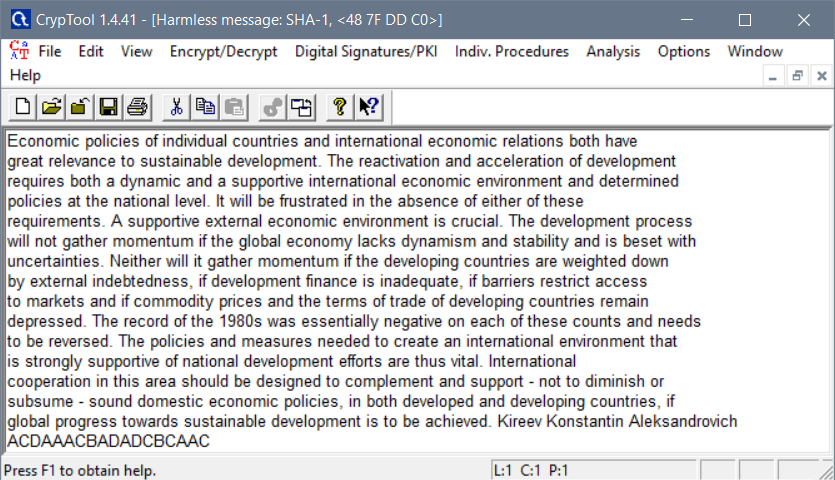
Подробные таблицы для подпункта 6.4

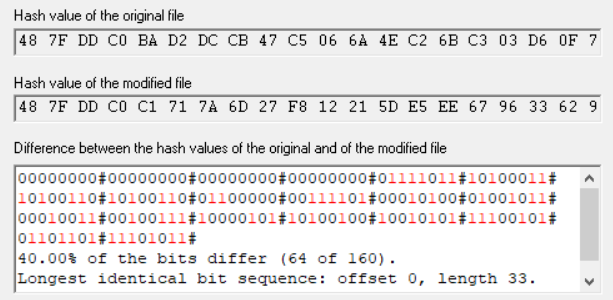
* 8 значащих бит:

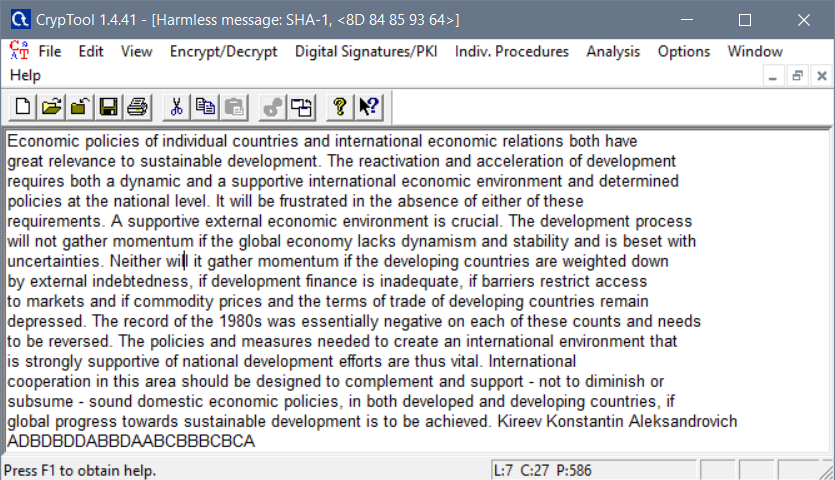


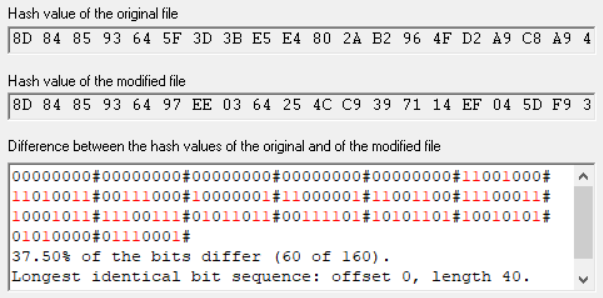
* 16 значащих бит:

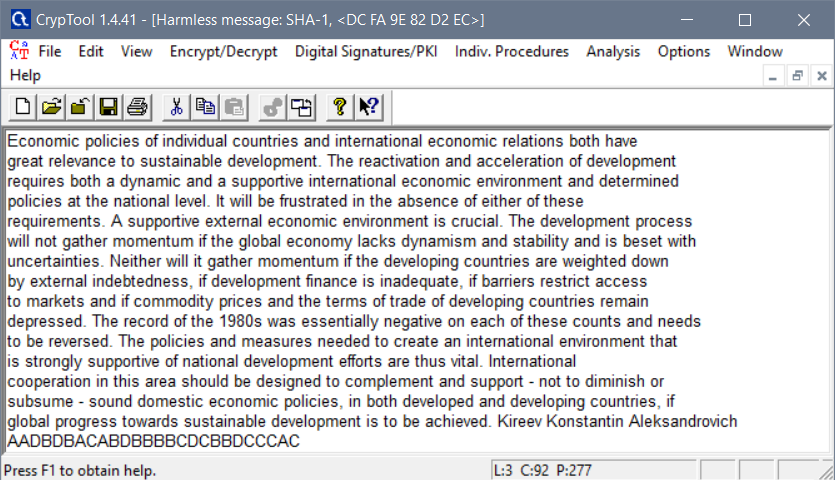


* 32 значащих бит:



* 40 значащих бит:



* 48 значащих бит:

