Лабораторная работа №5
«ВОССТАНОВЛЕНИЕ И ФОРМИРОВАНИЕ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ»

Цель лабораторной работы:

1) закрепить навыки обучающихся по правильному формированию паролей пользователей путём сравнения эффективности восстановления паролей, имеющих различные параметры;

2) показать, как неправильное использование стойких криптографических алгоритмов может привести к созданию слабозащищённых систем идентификации и аутентификации пользователей.

В ходе выполнения данного лабораторной работы обучающийся получит навыки по самостоятельному формированию различных хэш-функций от паролей пользователей, получит возможность сравнить эффективность двух различных подходов к восстановлению паролей пользователей: на основе методов перебора (полного, по словарю, с мутациями символов и т.д.) и на основе техники криптоанализа по размену «время — память» (с использованием радужных таблиц).

1. Описание RainbowCrack

RainbowCrack является инструментом для восстановления по хэшам исходных открытых сообщений, в роли которых нередко выступают пароли пользователей. Тогда как традиционные методы силового восстановления подразумевают последовательный перебор исходных открытых сообщений с последующим сравнением полученных хэшей, RainbowCrack работает другим способом. Он осуществляет особым образом предварительное вычисление всех возможных пар «открытый текст — зашифрованный текст» и сохраняет их в файле, называемом "rainbow table". Предвычисление таких таблиц занимает длительное время, но по завершении этих предвычислений появляется возможность восстановить открытое сообщение (пароль) в течении секунд. Таким образом осуществляется «размен время — память».

RainbowCrack поддерживает работу с несколькими хэш-функциями: md5, sha1 и др. Неподдерживаемые хэш-функции можно достаточно легко добавить самому, так как данная программа имеет открытые исходные коды.

RainbowCrack работает как под управлением ОС Windows, так и ОС Линукс. Самое главное, в состав программы включена утилита для генерации rainbow-таблиц, что позволяет формировать таблицы для различных наборов символов, например, для русского языка и т.д.

Разработчиками программы предлагается несколько готовых конфигурация для rainbow-таблиц.

Конфигурация #0	
Хэш алгоритм	lm
Набор символов	alpha (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
Диапазон длин открытых сообщений	1 - 7
Объём пространства ключа	26^1 + 26^2 + 26^3 + 26^4 + 26^5 + 26^6 + 26^7 = 8353082582
t	2100
m	8000000

l	5
Использование диска	m * 16 * l = 640000000 B = 610 MB
Вероятность успеха	0.9990
Среднее время криптоанализа	3.7841 s
Среднее время криптоанализа на системах с малым объёмом памяти (свободной памяти менее, чем 122MB)	8.2836 s
Максимальное время криптоанализа	31.1441 s
Команды, используемые для предвычисления таблиц	rtgen lm alpha 1 7 0 2100 8000000 all rtgen lm alpha 1 7 1 2100 8000000 all rtgen lm alpha 1 7 2 2100 8000000 all rtgen lm alpha 1 7 3 2100 8000000 all rtgen lm alpha 1 7 4 2100 8000000 all
Длительность процедуры предвычисления таблиц	2 days 18 hours

Конфигурация #1	
Хэш алгоритм	lm
Набор символов	alpha-numeric(ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789)
Диапазон длин открытых сообщений	1 - 7
Объём пространства ключа	36^1 + 36^2 + 36^3 + 36^4 + 36^5 + 36^6 + 36^7 = 80603140212
t	2400
m	40000000
l	5
Использование диска	m * 16 * l = 3200000000 B = 3 GB
Вероятность успеха	0.9904
Среднее время криптоанализа	7.6276 s
Среднее время криптоанализа на системах с малым объёмом памяти (свободной памяти менее, чем 122MB)	13.3075 s
Максимальное время криптоанализа	40.6780 s
Команды, используемые для предвычисления таблиц	rtgen lm alpha-numeric 1 7 0 2400 40000000 all rtgen lm alpha-numeric 1 7 1 2400 40000000 all rtgen lm alpha-numeric 1 7 2 2400 40000000 all rtgen lm alpha-numeric 1 7 3 2400 40000000 all rtgen lm alpha-numeric 1 7 4 2400 40000000 all
Длительность процедуры предвычисления таблиц	15 days 17 hours

2. Порядок работы с Rainbow_crack

Допустим, мы скопировали (установили) Rainbowcrack в каталог «cd c:\rainbowcrack-1.2-win». После этого запускаем консоль Windows (команда cmd) и осуществляем переход в данный каталог используя команды «**cd ..**» и «**cd c:\rainbowcrack-1.2-win**».

Далее, мы можем воспользоваться командами данного программного продукта.

Для начала необходимо подготовить радужные таблицы (rainbow table). Для этого служит команда «**rtgen.exe**». Вводим её в командной строке и нажимаем «**Enter**». В этом случае на экран будет выведено следующее сообщение, подсказывающее, как пользоваться командой:

```
C:\rainbowcrack-1.2-win>rtgen
RainbowCrack 1.2 - Making a Faster Cryptanalytic Time-Memory Trade-Off
by Zhu Shuanglei <shuanglei@hotmail.com>
http://www.antsight.com/zsl/rainbowcrack/

usage: rtgen hash_algorithm \
plain_charset plain_len_min plain_len_max \
rainbow_table_index \
rainbow_chain_length rainbow_chain_count \
file_title_suffix
rtgen hash_algorithm \
plain_charset plain_len_min plain_len_max \
rainbow_table_index \
-bench

hash_algorithm: available: lm md5 sha1
plain_charset: use any charset name in charset.txt here
use "byte" to specify all 256 characters as the charset of the plaintext
plain_len_min: min length of the plaintext
plain_len_max: max length of the plaintext
rainbow_table_index: index of the rainbow table
rainbow_chain_length: length of the rainbow chain
rainbow_chain_count: count of the rainbow chain to generate
file_title_suffix: the string appended to the file title
add your comment of the generated rainbow table here
-bench: do some benchmark

example: rtgen lm alpha 1 7 0 100 16 test
rtgen md5 byte 4 4 0 100 16 test
rtgen sha1 numeric 1 10 0 100 16 test
rtgen lm alpha 1 7 0 -bench

C:\rainbowcrack-1.2-win>
```

Допустим, нам требуется создать радужную таблицу для хэш-функции SHA1, при этом удовлетворяющую условиям:

1) восстанавливаемые пароли содержат только маленькие латинские буквы и цифры;

2) длина восстанавливаемых паролей от 1-го до 6-и символов;

3) название таблицы — laba.

Для определения того, как указать используемый набор символов, просмотрим содержимое файла «charset.txt»:

```
# charset configuration file for rainbowcrack 1.1 and later
# by Zhu Shuanglei <shuanglei@hotmail.com>

alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

numeric = [0123456789]
loweralpha = [abcdefghijklmnopqrstuvwxyz]
```

```
loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]
lowerrus-numeric = [ёйцукенгшщзхъфывапролджэячсмитьбю0123456789]
```

Как видно из содержимого данного файла, необходимый нам набор символов называется «loweralpha-numeric». В принципе, мы можем сами добавлять в этот файл различные наборы символов, например «lowerrus-numeric».

Следующим важным шагом является определение размерности таблицы, которая зависит от объёма пространства входных сообщений. Данный объём легко вычислить, зная основание алфавита и количетсво используемых символов. Например, набор «loweralpha-numeric» содержит 36 различных символов (т.е. основание равно 36). Для паролей длиной 1 символ объём пространства составляет 36^1 или 36 различных комбинаций, для паролей длиной 2 символа объём пространства составляет 36^2 или 1296 различных комбинаций и т.д. Следовательно, общий объём пространства входных сообщений (паролей) составит:

36^1 + 36^2 + 36^3 + 36^4 + 36^5 + 36^6 = 2.238.976.116 комбинаций.

Объём радужной таблицы задаётся двумя параметрами: длиной цепочки ключей и количеством этих цепочек в таблице. Если мы выберем длину цепочки равной 2400, а количество цепочек равным 1.000.000, то объём радужной таблицы составит 2.400.000.000 ключей (или вариантов перебора). Это значение превышает общий объём пространства входных сообщений, что нам и требуется.

Используя определённые нами параметры запускаем процесс формирования радужной таблицы, используя команду «**`rtgen.exe sha1 loweralpha-numeric 1 6 0 2400 1000000 laba`**»:

```
C:\rainbowcrack-1.2-win>rtgen.exe sha1 loweralpha-numeric 1 6 0 2400 1000000
laba
hash routine: sha1
hash length: 20
plain charset: abcdefghijklmnopqrstuvwxyz0123456789
plain charset in hex: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
7
4 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
plain length range: 1 - 6
plain charset name: loweralpha-numeric
plain space total: 2238976116
rainbow table index: 0
reduce offset: 0

generating...
100000 of 1000000 rainbow chains generated (4 m 15 s)
200000 of 1000000 rainbow chains generated (4 m 17 s)
300000 of 1000000 rainbow chains generated (4 m 15 s)
400000 of 1000000 rainbow chains generated (4 m 16 s)
500000 of 1000000 rainbow chains generated (4 m 16 s)
600000 of 1000000 rainbow chains generated (4 m 16 s)
700000 of 1000000 rainbow chains generated (4 m 15 s)
800000 of 1000000 rainbow chains generated (4 m 14 s)
900000 of 1000000 rainbow chains generated (4 m 14 s)
1000000 of 1000000 rainbow chains generated (4 m 15 s)
```

Подождав более 50 мин. мы получим необходимый файл таблицы, имеющий название «**sha1_loweralpha-numeric#1-6_0_2400x1000000_laba.rt**» Так как в таблице сохраняются только

значения начала и конца цепочек (по 8 байт), то она занимает на диске относительно небольшое место (16.000.000 байт).
Для данной таблицы мы указали значение индекса равным «0». Если мы хотим создать дополнительные таблицы (для увеличения вероятности успешного восстановления пароля), то каждой новой таблице указываем увеличенное на 1 значение индекса.
Следующей процедурой является сортировка таблицы при помощи команды «**rtsort.exe**»:

```
C:\rainbowcrack-1.2-win>rtsort sha1_loweralpha-numeric#1-
6_0_2400x1000000_laba.rt
available physical memory: 2147483647 bytes
loading rainbow table...
sorting rainbow table...
writing sorted rainbow table...
C:\rainbowcrack-1.2-win>
```

Создав полностью готовую радужную таблицу мы можем приступать к процессу восстановления паролей пользователей. Для этого подготовим текстовый файл, содержащий исследуемые значения хэш-функции (например, при помощи «Блокнота»). Ниже приведено содержимое такого файла, хранящего в себе 20 значений хэш-функции SHA1.

```
51E7576A524051D8401D8A1EF12BD65D518B55C7
AE0E3AACF507607DEFDAC37574964384FC18F3AC
D9EB49F41C2363970F99584A697785FDB1A4F7B3
5DD38D3D1C516721B79599B4537BFFB56E97C8B0
655DCAA997C5F5DB69D807971DBBF27A2D46E327
18FD7F9D65029F4E7277EE719F2EF382945BFAEB
8D90FFD60B4C905B72EEFD591C23ADC4577BFF3B
4CF9DFB60A62650CAFC36D1D4EC8B147504A9A54
FE2DB16EBABEDCD16605F1677287E84CBB306146
30080914028E006F45AFAD74A2C524AC9BF80F9F
459cd8a3146de2e46635f24b841a5f25045b50cc
7566becb5f181316fe838cd4c301f59d50ff8ecb
b9d6b72964cea634b2b8c44f7a2fedcaed134025
c37e7c8fd457682199909708cf2da1144178e028
290516b50b2382629f73e1f7497e8cfe1cff0b6a
b82ba51fb1bb6528cd011c92aa79612253c0e387
dac63fcb6cd1322ce7aebaaf4016304b141d7a17
257cd5b35797adfc9ecd073a8512e6c66d998a5d
089af482cde49267862d8b515a1a0655bee1d7ea
bf1451bba3bad13f38fedc18a31487a8aff1ceb2
```

В одной строке указывается только одна хэш-функция, которая записывается в виде последовательности шестнадцатеричхных цифр. Другие символы не допустимы.
Допустим мы назвали файл с хэшами как «passw_sha1.txt». Используя команду «**rcrack.exe**», а именно «**`rcrack sha1_loweralpha-numeric#1-6_0_2400x1000000_laba.rt -l passw_sha1.txt`**» осуществляем попытку восстановления паролей пользователей:

```
C:\rainbowcrack-1.2-win>rcrack sha1_loweralpha-numeric#1-
6_0_2400x1000000_laba.rt -l passw_sha1.txt
sha1_loweralpha-numeric#1-6_0_2400x1000000_laba.rt:
16000000 bytes read, disk access time: 0.03 s
verifying the file...
searching for 20 hashes...
plaintext of ae0e3aacf507607defdac37574964384fc18f3ac is 9qz2
plaintext of 5dd38d3d1c516721b79599b4537bffb56e97c8b0 is 3ege
```

```
plaintext of 18fd7f9d65029f4e7277ee719f2ef382945bfaeb is ukq8
plaintext of 4cf9dfb60a62650cafc36d1d4ec8b147504a9a54 is w7h8
plaintext of fe2db16ebabedcd16605f1677287e84cbb306146 is 7qq7
plaintext of 30080914028e006f45afad74a2c524ac9bf80f9f is hk7n
plaintext of 459cd8a3146de2e46635f24b841a5f25045b50cc is 9e5yf7
plaintext of 7566becb5f181316fe838cd4c301f59d50ff8ecb is 5e48mw
plaintext of 290516b50b2382629f73e1f7497e8cfe1cff0b6a is x8k2g3
plaintext of b82ba51fb1bb6528cd011c92aa79612253c0e387 is 247qar
plaintext of 257cd5b35797adfc9ecd073a8512e6c66d998a5d is 9thu24
plaintext of 089af482cde49267862d8b515a1a0655bee1d7ea is h64r2x
plaintext of bf1451bba3bad13f38fedc18a31487a8aff1ceb2 is 9f43yv
cryptanalysis time: 50.34 s

statistics
----------------------------------------------------------
plaintext found: 13 of 20 (65.00%)
total disk access time: 0.03 s
total cryptanalysis time: 50.34 s
total chain walk step: 33326659
total false alarm: 14935
total chain walk step due to false alarm: 14218079

result
----------------------------------------------------------
51e7576a524051d8401d8a1ef12bd65d518b55c7 <notfound> hex:<notfound>
ae0e3aacf507607defdac37574964384fc18f3ac 9qz2 hex:39717a32
d9eb49f41c2363970f99584a697785fdb1a4f7b3 <notfound> hex:<notfound>
5dd38d3d1c516721b79599b4537bffb56e97c8b0 3ege hex:33656765
655dcaa997c5f5db69d807971dbbf27a2d46e327 <notfound> hex:<notfound>
18fd7f9d65029f4e7277ee719f2ef382945bfaeb ukq8 hex:756b7138
8d90ffd60b4c905b72eefd591c23adc4577bff3b <notfound> hex:<notfound>
4cf9dfb60a62650cafc36d1d4ec8b147504a9a54 w7h8 hex:77376838
fe2db16ebabedcd16605f1677287e84cbb306146 7qq7 hex:37717137
30080914028e006f45afad74a2c524ac9bf80f9f hk7n hex:686b376e
459cd8a3146de2e46635f24b841a5f25045b50cc 9e5yf7 hex:396535796637
7566becb5f181316fe838cd4c301f59d50ff8ecb 5e48mw hex:356534386d77
b9d6b72964cea634b2b8c44f7a2fedcaed134025 <notfound> hex:<notfound>
c37e7c8fd457682199909708cf2da1144178e028 <notfound> hex:<notfound>
290516b50b2382629f73e1f7497e8cfe1cff0b6a x8k2g3 hex:78386b326733
b82ba51fb1bb6528cd011c92aa79612253c0e387 247qar hex:323437716172
dac63fcb6cd1322ce7aebaaf4016304b141d7a17 <notfound> hex:<notfound>
257cd5b35797adfc9ecd073a8512e6c66d998a5d 9thu24 hex:397468753234
089af482cde49267862d8b515a1a0655bee1d7ea h64r2x hex:683634723278
bf1451bba3bad13f38fedc18a31487a8aff1ceb2 9f43yv hex:396634337976

C:\rainbowcrack-1.2-win>
```

После непродолжительного времени ожидания на экран выводится приведённый выше отчёт. Из него следует, что было восстановлено 13 паролей из 20 (65%) и ушло на это 50,34 секунды. Если бы мы использовали метод полного перебора (метод грубой силы), то у нас на обработку ***каждого*** пароля ушло бы более 50 минут! Учитывая при этом, что пароли сформированы случайным образом (нельзя использовать атаки по словарю и т.д.) и их длина составляет 6 символов.

Всё это показывает эффективность метода «размен время — объём памяти», когда заранее осуществляется большое количество операций по вычислению специальной таблицы, а этап восстановления паролей пользователей затем занимает несколько секунд.

Ниже приведена аналогичная последовательность действий по созданию радужной таблицы для хэш-функции MD5 и по восстановлению на её основе паролей пользователей:

```
C:\rainbowcrack-1.2-win>rtgen.exe md5 loweralpha-numeric 1 6 0 2400 1000000
laba

hash routine: md5
hash length: 16
plain charset: abcdefghijklmnopqrstuvwxyz0123456789
plain charset in hex: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
7
4 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
plain length range: 1 - 6
plain charset name: loweralpha-numeric
plain space total: 2238976116
rainbow table index: 0
reduce offset: 0

generating...
100000 of 1000000 rainbow chains generated (3 m 48 s)
200000 of 1000000 rainbow chains generated (3 m 48 s)
300000 of 1000000 rainbow chains generated (3 m 47 s)
400000 of 1000000 rainbow chains generated (3 m 48 s)
500000 of 1000000 rainbow chains generated (3 m 47 s)
600000 of 1000000 rainbow chains generated (3 m 50 s)
700000 of 1000000 rainbow chains generated (3 m 46 s)
800000 of 1000000 rainbow chains generated (3 m 46 s)
900000 of 1000000 rainbow chains generated (3 m 46 s)
1000000 of 1000000 rainbow chains generated (3 m 46 s)

C:\rainbowcrack-1.2-win>rtsort md5_loweralpha-numeric#1-
6_0_2400x1000000_laba.rt

available physical memory: 2147483647 bytes
loading rainbow table...
sorting rainbow table...
writing sorted rainbow table...

C:\rainbowcrack-1.2-win>rcrack md5_loweralpha-numeric#1-
6_0_2400x1000000_laba.rt
-l passw_md5.txt
md5_loweralpha-numeric#1-6_0_2400x1000000_laba.rt:
16000000 bytes read, disk access time: 0.02 s
verifying the file...
searching for 10 hashes...
plaintext of 7e2738461e608bd3cb37c1254abf01e3 is 4q78sw
plaintext of 9b46bc33d4f5488e57809d2e639a74fa is r578fk
plaintext of a171fd24e3b5e58e7dca55adfbfd4a5c is 6dv9y4
plaintext of 225d3dc7ef980c60d5b034befcbf0f6c is 6r8sx4
plaintext of d2ef193311068b8d20bba8b0025f8b10 is tqz235
plaintext of 4b471eee8962c247db66eb6be05bd998 is yq9k72
plaintext of a868905e40cd6bc3108f2744e343ee01 is gp2w78
cryptanalysis time: 20.36 s

statistics
----------------------------------------------------------
plaintext found: 7 of 10 (70.00%)
total disk access time: 0.02 s
total cryptanalysis time: 20.36 s
```

```
total chain walk step: 14869349
total false alarm: 6641
total chain walk step due to false alarm: 6786193

result
------------------------------------------------------
7e2738461e608bd3cb37c1254abf01e3 4q78sw hex:347137387377
9b46bc33d4f5488e57809d2e639a74fa r578fk hex:72353738666b
a171fd24e3b5e58e7dca55adfbfd4a5c 6dv9y4 hex:366476397934
225d3dc7ef980c60d5b034befcbf0f6c 6r8sx4 hex:367238737834
29868768988957f5d34eb3c01e129484 <notfound> hex:<notfound>
d2ef193311068b8d20bba8b0025f8b10 tqz235 hex:74717a323335
69695ae2def03d1b00d10193143fc389 <notfound> hex:<notfound>
d971a9c45c4158b332895940a2b6ee0e <notfound> hex:<notfound>
4b471eee8962c247db66eb6be05bd998 yq9k72 hex:7971396b3732
a868905e40cd6bc3108f2744e343ee01 gp2w78 hex:677032773738

C:\rainbowcrack-1.2-win>
```

Пример варианта задания:

Вариант 1

1. По заданным значениям хэш-функций восстановить пароли пользователей, результаты занести в таблицу. Указать долю правильно восстановленных паролей.
2. Дополнительно сформировать пароли и соответствующие им sha1-хэши, состоящие из русских символов и цифр (длиной не более 6 символов).
3. Сформировать радужную таблицу с использованием символов русского алфавита и набора цифр. Приложить её к отчёту (в электронном виде).
4. Продемонстрировать восстановление паролей, полученных в п.2 используя радужную таблицу, полученную в п.3.

LM-хэш (длина пароля 12 символов):

```
24062F9ABFDF002B79DC190B98842EB7
AAFE7C2888D9722F90044675A76A7AF2
BCC0ABD492B42E84839AF214E797A446
663FE3135116ADD4127BA5C2F43E6AB4
D341284BF612972530D75B03837A8220
```

MD5-хэш (длина пароля 6 символов):

```
2aa1010cc58d6d3fcf6cad27737c8f6e
357b1a263fa0ea406f73f7d16b8532bb
3446a71cc08e28516943567df4676d82
3dc11bbdcb578a8cc28c371430489a48
72cf870a0290c931e39d1c814bbcb0fc
```

SHA1-хэш (длина пароля 6 символов):

```
cbc5446e7dd47a7b82d42e2995edb1df3e5f2db0
```

6a5912c3781eede62390786fbd43d69c9cca3dc9
aaf044a02f19b365db04873cda6481b175c54141
8a058c61af5dd9d91ffa6007f1499a9154113a34
9af733a383a885f7c07325d71a49c9ae857b53f8