Отчет по лабораторной работе.

Изначально по заданию лабораторной работы нам дан текст:

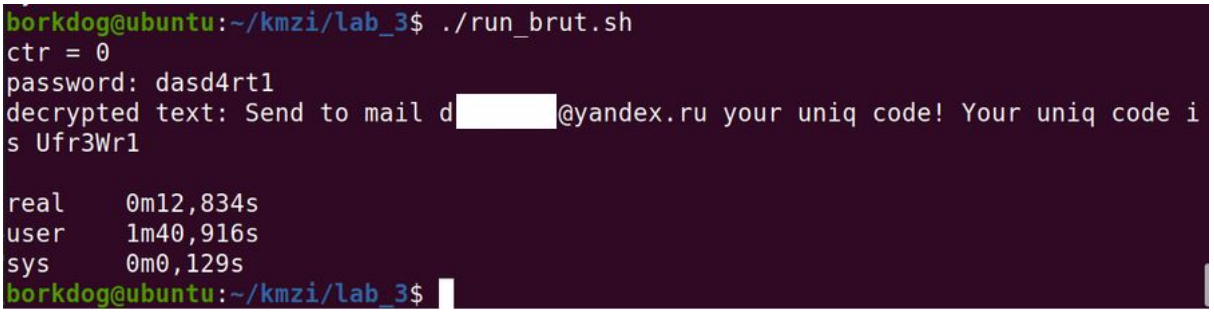
“*4B4B533031370100000140000004CB213E6352856C414D74B8F7C238680D5074A9F30000000DD59AC338EA1ECB99E91FEB71C13F2FF709F85E8334EF430168DD8274ADEAD1992DC5AF12CFB3D48470B2D12118F5F3F269B5EDB91362AA2A109D680A87B9F7197A94F5BFE25A7854AF47DF5BED7BF351DA543957C5E988814196A7C52096D7090BA2C97491DC93D8A623FAC725CA5E7F4260D13*”

Рассмотрим его структуру, которую мне удалось восстановить:

- группа: 4B4B53303137 (‘KKSO17’)
- длина (в байтах) количества раундов: 01000000 (0x1=1)
- длина (в байтах) соли: 14000000 (0x14=20)
- соль: 4CB213E6352856C414D74B8F7C238680D5074A9F
- счетчик: 30000000 (0x30=48)
- iv: DD59AC338EA1ECB99E91FEB71C13F2FF
- шифрованный текст: 709F85E8334EF430168DD8274ADEAD1992DC5AF12CFB3D48470B2D12118F5F3F269B5EDB91362AA2A109D680A87B9F7197A94F5BFE25A7854AF47DF5BED7BF351DA543957C5E988814196A7C52096D70
- хэш: 90BA2C97491DC93D8A623FAC725CA5E7F4260D13

Для развертки ключа для AES-cbc использована функция PBKDF2 с PRF HMAC SHA1. Хэш в конце файла - SHA1.

Нам известна маска пароля: da****t1 и то, что пароль содержит 6 символов английского алфавита нижнего регистра и две цифры. Это означает, что по рассчетам нам нужно перебрать чуть больше 700 тысяч ключей. Для генерации ключей нужно запустить скрипт **./run_gen_keys.sh**, а для запуска брута нужно запустить файл **./run_brut.sh**. Брутфорс использует многопоточность, реализованную на OpenMP, а также библиотеку Openssl для PBKDF2 и библиотеку Crypto++ для реализации AES-CBC. Проверка на читаемость производится с помощью самописной функции is_printable(), которая выводит ключ и расшифрованный текст в том случае, если в нем содержится больше чем один блок, который целиком состоит из печатаемых символов. Результат работы брутфорса:



Программа запускалась на процессоре Intel Core i7 8th gen, который содержит 8 логических ядер, что позволило ускорить брутфорс в 8 раз. Брутфорс написан на C++, генератор ключей написан на Python3. Подробная информация о ходе работы программы складывается в файл log.txt.