UNIVERSITY OF MARYLAND
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ENEE 457
Computer Systems Security
Instructor: Charalampos Papamanthou

Programming Project 3: Rainbow Tables

Out: 10/10/18 Due: 10/24/18 11:59pm

Instructions

1. Strictly adhere to the University of Maryland Code of Academic Integrity.
2. Submit your solutions as a pdf document at Canvas. Include your full name in the solutions document. Name the solutions document as x-project3.pdf, where x is your last name.

Rainbow Tables

Assume the following scheme is being used to hash passwords: An n-bit password p is padded to the left with $128 - n$ zeros and used as an AES-128 key to encrypt the all-0 plaintext; the result is the "hashed password", i.e.

$$h(p) = \mathsf{AES}_{0_{128-n}||p}(0^{128}).$$

So for the 12-bit password $p = \mathsf{0xABC}$, the result should be

$$h(p) = \mathsf{970fc16e71b75463abafb3f8be939d1c}.$$

You may assume n is a multiple of 4.

The scenario is that you are given $h(p)$ and n and need to recover p. Your attack should use a rainbow table with $2^{n/2}$ chains of $2^{n/2}$ length each. You may wish to visit this page for an example of a reduction function that you can use.

1. Write two programs, called GenTable and Crack. The first of these corresponds to the pre-processing phase in which you generate a rainbow table, while the second corresponds to the on-line phase in which you are given $h(p)$ and need to recover p.
   - GenTable should take one command-line argument and generate output to a file rainbow. The argument will be n, the password length (in bits). The bound on the size of rainbow must be no larger than $3 \cdot 128 \cdot 2^{\frac{n}{2}}$ bits. Failure to meet this space bound will result in 0 points. You can use `ls -l` to check the size of your file.
   - Crack should take two command-line arguments and generate output to standard output. The first command-line argument is the same as above. The second argument is $h(p)$ in hex. When you run Crack n $h(p)$, you may assume that GenTable n was just run to give rainbow. The output of crack should include two items: the password p or "failure", and the number of times AES was evaluated. Failure to report the number of AES evaluations accurately will be considered cheating, and will result in 0 points.

- So running
  GenTable 12
  Crack 12 970fc16e71b75463abafb3f8be939d1c
  should give output "password is ABC, AES evaluated 191 times" (assuming that in this execution of crack AES was evaluated 191 times).

2. Include a 1-2-page writeup that describes your implementation.
3. Use your programs to recover the passwords from the challenges here:

$$http://enee457.github.io/homeworks/code/rainbow.txt$$

   Include the answers at the end of your writeup.

Submit your source code for your programs and your writeup.