Matthew Kachar

COSC4931

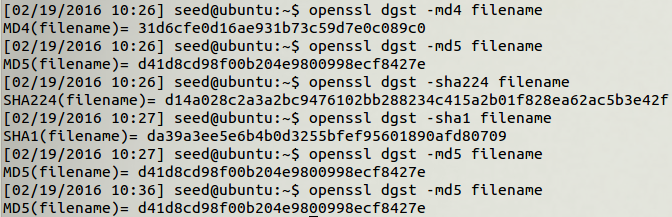
2/19/16

Homework 4 Crypto Lab – One-way Hash Function and MAC

Lab Objective:

Familiarity with one-way hash functions and Message Authentication Code.

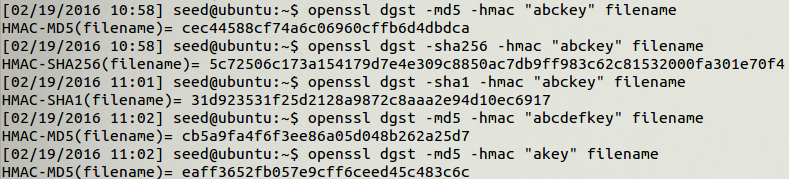
Generating a hash value for a blank file using the *dgst* command with several hashing algorithms, the output is as follows;



Just to understand what is happening, I ran the *md5* algorithm consecutively to verify the digest command would return the same value.

Generating a keyed hash value using the *–md5* *–hmac*, the *–sha256 –hmac*, and the *–sha1*

*–hmac* and passing through different key sizes for the same blank file.



As for using a fixed size key, the algorithm is not changed by the size of the key and seems to give a random hash value for all different keys. The length of the hash value is different between each of the crypto algorithms since the output seems to be truncated.

To understand the properties of the one-way hash function, I used a text file with the string,

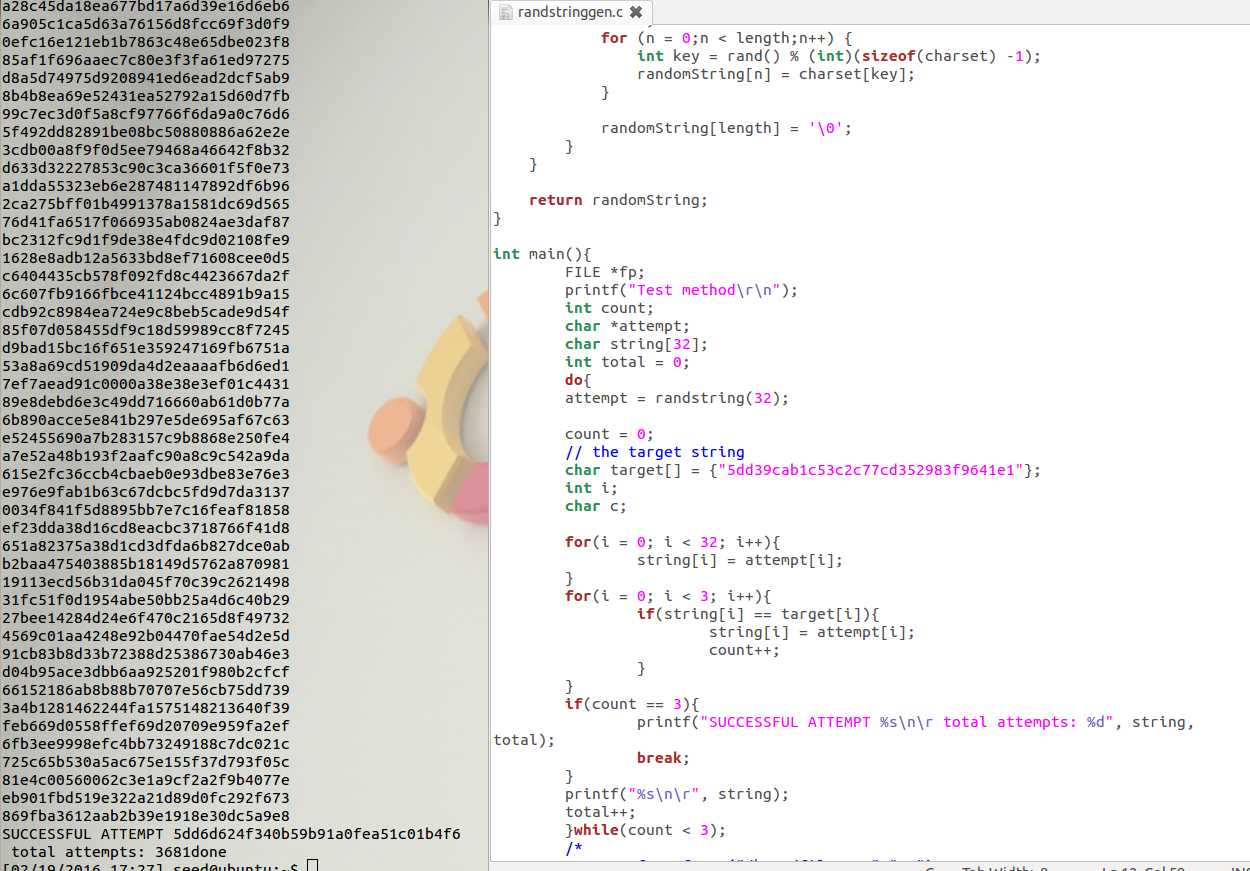
“This is a test file.”

Running the *–md5* algorithm on the file the output is:

MD5(filename)= 5dd39cab1c53c2c77cd352983f9641e1

Then I changed the ‘i’ in the word “is” to an ‘h’ which changes the last bit; from 01101001 to 01101000. The output is completely different:

MD5(filename)= cfb47749ac888fd43ba604d6f357356d



The brute force method is not very efficient and somewhat complicated to implement since it requires passing the random files over and over through the openssl and the random string generator takes on average over 3000 attempts before success. While trying to complete the first few attempts Ubuntu crashed a couple of times from perhaps reading and rewriting the same file several thousand times.