Sasha Shahidi

Week 10 Homework: Cryptography Homework: Ransomware Riddles

Riddle 1:

- I used Caesar Cipher to decode “ozcjmz” by going 8 spots back (as suggested in the riddle) in the alphabet on each letter to find the new letter.
- “ozcjmz” became “gruber”.
- Key: 6skd8s

Riddle 2:

- I used a binary to ASCII converter and plugged in the numbers “01000111 01100101 01101110 01101110 01100101 01110010 01101111”
- The ASCII text was “Gennero”
- Key: cy8snd2

Riddle 3:

- I made a nano in Linux called “ciphertexthw10.txt.enc” and put in the cipher text of “4qMOIvwEGXzvkMvRE2bNbg==”
- Then I made a command using openssl, the given key, the given IV, along with some commands such as -aes-256-cbc and -nosalt
- The command was: openssl enc -aes-256-cbc -d -a -nosalt -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED -in ciphertexthw10.txt.enc
- The response was “takagi”
- Key: ud6s98n

Riddle 4:

- Jack would need to use Jill’s public key to send her an encrypted message
- Jill would use her own private key to decrypt Jack’s encrypted message
- (N * (N-1)) / 2 = count of symmetric keys
    - There are 6 total people, so: (6 * 5) / 2 = 15 symmetric keys
- (N * 2) = count of asymmetric keys
    - There are 6 total people, so: (6 * 2) = 12 asymmetric keys
- Tim would need to send the public key of the friend he’s sending the encrypted message to, so in this case, the only option would be Alice’s public key
- Key: 7gsn3nd2

Riddle 5:

- An MD5 hash was given so I used an MD5 hash reverser and entered in the hash “3b75cdd826a16f5bba0076690f644dc7”
- The response was “argyle”
- Key: ajy39d2

Riddle 6:

- I downloaded the mary-lamb.jpg photo into my Downloads folder on Linux, then used steghide by entering the command “steghide extract -sf mary-lamb.jpg” with the passcode that was on the book in the photo, which was “ABC”
- Linux said the data was extracted into “code_is_inside_this_file.txt”, so I typed “cat code_is_inside_this_file.txt”
- The response was “mcclane”
- Key: 7skahd6

Below is the proof that I decrypted the ransomware and saved the hospital.