

Module 10 Challenge ~ Ransomware Riddles

Riddle 1: Caesar decypher

**Roses are Red Violets are Blue,
Caesar would be 8 is your first clue.**

Decrypt **ozcjmz and enter it below,
and maybe a key then might just show.**

When I run the above encrypted code through the Caesar Cipher Tool, it displays an answer of **gruber**

The image shows a web-based 'Caesar Cipher Tool'. At the top, the title 'Caesar Cipher Tool' is displayed. Below it, a text input field contains the encrypted string 'ozcjmz'. Underneath the input field are three buttons: 'Copy', 'Paste', and 'Text Options...'. Below these buttons is a section for settings, including a key input field with the value '8' and a language dropdown menu set to 'English'. Below the settings are three buttons: 'Decode', 'Encode', and 'Auto Solve (with...)'. Below these buttons is a section titled 'Auto Solve Options' with two sub-sections: 'Max Results' with a value of '10' and 'Spacing Mode' with a dropdown menu set to 'Automatic'. Below the 'Auto Solve Options' section is a 'Results' section. In the 'Results' section, there is a label 'Decoded message.' and a text input field containing the decoded string 'gruber'.

When gruber is entered into the answer field, the below key is:

key 1 = **6skd8s**

Riddle 1

Congrats, you have solved the first riddle, Your first key is: 6skd8s

Riddle 2: Binary challenge

**Humpty Dumpty Sat on the Wall,
Humpty Dumpty had a great Fall,**

**All the king's Horses and all the
Kings Men couldn't decode this
message for him:**

**01000111 01100101 01101110
01101110 01100101 01110010
01101111**

Let's decode the binary.

Enter the binary text to decode, and then click "Convert!":

01000111011001010110111001101110011001010111001001101111

Convert!

The decoded string:

Gennero

Gennero is entered into the answer field, and key is given:

key 2 = **cy8snd2**

RIDDLE 2

Congrats for solving the second riddle, the key is: cy8snd2

Riddle 3: OpenSSL

**I'm a little Cipher,
short and sweet.**

**Here is my vector,
and also my key** →

**When I get all steamed up,
hear me shout!**

Just use OpenSSL to figure me out

ur answer

Cipher Text:
4qMOlwEGXzvKmvRE2bNbg==

Key:
5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564

IV (Initialization Vector):
1907C5E255F7FC9A6B47B0E789847AED

OpenSSL Options:

- -pbkdf2
- -nosalt
- -aes-256-cbc
- base64

We are given some cipher text, a key, a IV and some OpenSSL options. I need to switch over to my VM Apache to run this and figure it out.

- Step 1: echo cipher text into a cipher.txt.enc text file
- Step 2: use openssl and options to decipher the text file.

Command:

```
openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in cipher.txt.enc -base64 -K  
5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv  
1907C5E255F7FC9A6B47B0E789847AED
```

Displays output: takagi

```
sysadmin@vm-image-ubuntu-dev-1:~/module_10_challenge$ openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in cipher.txt.enc -base64 -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED  
takagi
```

When takagin entered into answer, key is given.

key 3 = **ud6s98n**

Riddle 4: Keys

**Jack and Jill went up a Hill to
use their public Keys**

**Jack had 2, and Jill did too
to exchange their messages
with ease.**

**What would Jack use to send
an encrypted message to Jill?**

- ☐ Jack's Public Key
- ☐ Jack's Private Key
- ☐ Jill's Public Key
- ☐ Jill's Private Key

- Part 1: Jill's public key
- Part 2: Jill's private key
- Part 3: 12 asym, 15 sym
 - o *In asymmetric encryption, 12 keys would be needed because each of the six people needs a unique pair of keys (a public and a private key). For symmetric encryption, 15 keys are required for secure communication between every pair out of the six people*
- Part 4: Alice's public key

Upon hitting submit, key is given:

key 4 = **7gsn3nd2**

Riddle 5: HashCatcd ..

**Hey diddle diddle,
the cat and the fiddle,
The cow jumped over the moon.**

**The little dog laughed
when it found this MD5 hash,**

**And the dish ran away with the
spoon!**

- Step 1: nano hash into the hashes.txt file in the VM apache
- Step 2: run hashcat command to create a solved txt file. Ran against the rockyou.txt wordlist.
 - o **hashcat -m 0 -a 0 -o riddle_5_solved.txt hashes.txt rockyou.txt --force**

```
sysadmin@vm-image-ubuntu-dev-1:~$ hashcat -m 0 -a 0 -o riddle_5_solved.txt hashes.txt rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2048/5891 MB allocatable, 2MCU

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance
```

- Step 3: Then I could cat the solved txt file and got the answer as **argyle**

```
sysadmin@vm-image-ubuntu-dev-1:~$ cat riddle_5_solved.txt
3b75cdd826a16f5bba0076690f644dc7:argyle
```

Once I entered the answer of argyle into the field, it gave me the key.

key 5 = **ajy39d2**

Riddle 6: Steghide

**Mary had a secret code,
Hidden in a photo,
And everywhere that photo went,
The code was sure to go**

**She wrote the passphrase on the
book, to access the code
You just need to use some stego
tricks and the secret will be showed.**



Downloaded the image to the VM Apache. Need to run steghide command to find secret code.

Command: `steghide extract -sf mary-lamb.jpg`

Passphrase: `ABC`

Extracted data to "code_is_inside_this_file.txt"

```
sysadmin@vm-image-ubuntu-dev-1:~/Downloads$ steghide extract -sf mary-lamb.jpg
Enter passphrase:
wrote extracted data to "code_is_inside_this_file.txt".
sysadmin@vm-image-ubuntu-dev-1:~/Downloads$
```

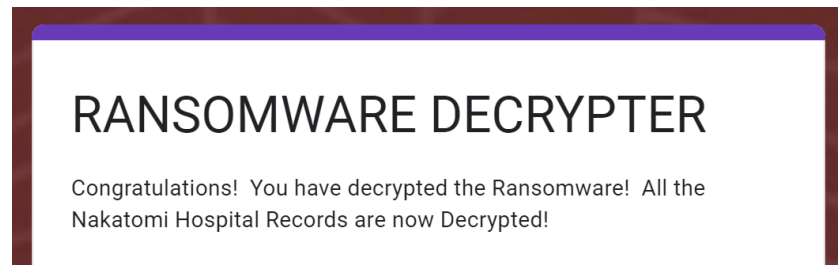
When I cat the file, it displays **mcclane**

```
sysadmin@vm-image-ubuntu-dev-1:~/Downloads$ cat code_is_inside_this_file.txt
mcclane
sysadmin@vm-image-ubuntu-dev-1:~/Downloads$
```

I enter mcclane in the answer field, and a key is given.

key 6 = **7skahd6**

When I enter all keys into the decrypter section of website, it says all data has now been decrypted. The mission was a success!!



QUIZ.

Question 1 15 / 15 pts

What is the first key (Riddle 1)?

6skd8s

Correct. The answer to the riddle was **gruber**

Question 2 20 / 20 pts

What is the second key (Riddle 2)?

cy8snd2

Correct. The answer to the riddle was **Gennero**

Question 3 15 / 15 pts

What is the third key (Riddle 3)?

ud6s98n

Correct. The answer to the riddle was **takagi**

Question 4

15 / 15 pts

What is the fourth key (Riddle 4)?

7gsn3nd2

Correct.

1. Jack would use Jill's public key to encrypt a message that he will send to Jill.
2. Jill would decrypt this message with her private key.
3. Six people total:
 - **Asymmetric** = $6 * 2 = 12$ Keys
 - **Symmetric** = $(6 * (6 - 1)) / 2 = (6 * 5) / 2 = 30 / 2 = 15$ Keys
4. Tim would only use someone else's public key to encrypt a message. The only other person's public key is Alice.

Question 5

20 / 20 pts

What is the fifth key (Riddle 5)?

ajy39d2

Correct. The answer to the riddle was **argyle**

Question 6

15 / 15 pts

What is the sixth key (Riddle 6)?

7skahd6

Correct. The answer to the riddle was **mcc lane**