



# Cybersecurity

## Module 10 Challenge Submission File

### Cryptography Challenge: Ransomware Riddles

Make a copy of this document to work in, and then for each mission, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

#### Ransomware Riddles

##### 1. Riddle 1:

OZCJMZ = gruber

or a tool

SEARCH A TOOL ON dCODE BY KEYWORDS:

type 'caesar'

BROWSE THE FULL dCODE TOOLS' LIST

Brute-Force mode: the 25 shifts (for the alphabet NOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↓	
→1 (←25)	NYBILY
→2 (←24)	MXAHKX
→3 (←23)	LWZGJW
→4 (←22)	KVYFIV
→5 (←21)	JUXEHU
→6 (←20)	ITWDGT
→7 (←19)	HVCFVS
→8 (←18)	GRUBER

### CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT (?)

OZCJMZ

Test all possible shifts (26-letter alphabet A-Z)

▶ DECRYPT (BRUTEFORCE)

#### MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY (NUMBER): 8

☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)

☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

☐ USE THE ASCII TABLE (0-127) AS ALPHABET

☐ USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

# Riddle 1

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

**Key: 6skd8s**


2. Riddle 2:


From

Binary

To

Text

 Open File

 Open Bin File




Paste binary numbers or drop file:


01000111 01100101 01101110 01101110 01100101 01110010 01101111

Character encoding (optional)

ASCII/UTF-8

 Convert

 Reset

 Swap

Gennero

## RIDDLE 2

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

[Submit another response](#)

Key: cy8snd2

3. Riddle 3:

```
(kali㉿kali)-[~/Desktop]
$ echo 4qM0IvwEGXzvKMvRE2bNbg== > Riddle3.txt

(kali㉿kali)-[~/Desktop]
$ openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in Riddle3.txt -base64 -K 52
84A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255
F7FC9A6B47B0E789847AED
takagi
```

## RIDDLE 3

Congrats on Solving Riddle number 3, here is  
your key: ud6s98n

[Submit another response](#)

Key: ud6s98n

4. Riddle 4:

1. Jills Public Key
2. Jills Private Key
3. 12 Asymmetric and 15 Symmetric
4. Alices Public Key

## RIDDLE 4

Congrats! The Key is: 7gsn3nd2

Key: 7gsn3nd2

5. Riddle 5:

```
(kali㉿kali)-[~/Desktop]  
$ echo 3b75cdd826a16f5bba0076690f644dc7 > Riddle5.txt
```

```
(kali㉿kali)-[~/Desktop]  
$ hashcat -m 0 -a 0 -o Riddle5solved.txt Riddle5.txt rockyou.txt  
hashcat (v6.2.6) starting
```

```
Started: Sun Nov 12 09:18:30 2023  
Stopped: Sun Nov 12 09:18:35 2023
```

```
(kali㉿kali)-[~/Desktop]  
$ cat Riddle5solved.txt  
3b75cdd826a16f5bba0076690f644dc7:argyle
```

## RIDDLE 5

Congrats on solving Riddle number 5, Here is your key:  
ajy39d2

Key: ajy39d2

6. Riddle 6:

```
(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf mary-lamb.jpg
Enter passphrase:
wrote extracted data to "code_is_inside_this_file.txt".

(kali㉿kali)-[~/Desktop]
└─$ cat code_is_inside_this_file.txt
mcclane
```

Passphrase was ABC which was on the book  
Code: mcclane

## RIDDLE 6

Congrats on solving Riddle number 6, they key is: 7skahd6.  
Now go and enter in all of your keys into the Ransomware  
decrypter!!

**Key : 7skahd6**

## Ransomware Screenshot

1. Include a screenshot showing proof that you've decrypted the ransomware:

Riddle 1 Key \*

6skd8s

Riddle 2 Key \*

cy8snd2

Riddle 3 Key \*

ud6s98n

Riddle 4 Key \*

7gsn3nd2

Riddle 5 Key \*

ajy39d2



Riddle 6 Key \*

7skahd6

# RANSOMWARE DECRYPTER

Congratulations! You have decrypted the Ransomware! All the Nakatomi Hospital Records are now Decrypted! Please take a screenshot of this message and submit as your homework!

[Submit another response](#)