

HOME PAGE

Home INSTRUCTIONS RANSOMWARE DECRYPTER RIDDLE 1 RIDDLE 2 RIDDLE 3 RIDDLE 4 RIDDLE 5 RIDDLE 6 Q

The screenshot shows a ransomware interface. On the left, there's a lock icon and two timer boxes: one for a raise and another for file loss. Both timers show 23:59:56. Below them is a Bitcoin payment section with an address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw. Buttons for 'Check Payment' and 'Decrypt' are present. To the right, a large heading 'SCENARIO' is displayed, followed by text about being a Cyber Security Analyst at Nakatomi Hospital who must solve riddles to decrypt patient records.

Instructions:

Home INSTRUCTIONS RANSOMWARE DECRYPTER RIDDLE 1 RIDDLE 2 RIDDLE 3 RIDDLE 4 RIDDLE 5 RIDDLE 6 Q

The screenshot shows a background of binary code with a large red skull icon in the center. Overlaid on the bottom is the word 'RANSOMWARE' in large, bold, red capital letters. To the left of the main text area is a small circular icon with an 'i' symbol. The main text discusses the ransomware providing 6 riddles for decryption, the submission process for solved riddles, and the final step of entering all keys into the Decrypter.

The Ransomware which has encrypted all of the patient records has provided you with 6 different riddles. See above for the link for each riddle. To solve each riddle, cryptography concepts will need to be applied.

Once the riddle has been solved, submit your answer on the bottom of each Riddle Page. If the correct answer is provided, a key will be given.

Once all keys are obtained, select the RANSOMWARE DECRYPTER link above, and enter in all of your keys!

Good Luck and act fast as the Nakatomi Patients are counting on you!

RIDDLE 1:

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

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



Caesar Cipher with a shift value of 8

ANSWER: Gruber KEY: 6skd8s

RIDDLE 2:

**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**

binary -> utf-8

ANSWER: Gennero KEY: cy8snd2

RIDDLE 3:

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

Cipher Text:

4qMOIvwEGXzvkMvRE2bNbG

Key:

5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564

IV (Initialization Vector):

1907C5E255F7FC9A6B47B0E789847AED

OpenSSL Options:

-pbkdf2

-nosalt

-aes-256-cbc

base64

```
echo "4qMOIvwEGXzvkMvRE2bNbg==" | openssl enc -pbkdf2 -nosalt -aes-256-cbc -out  
out.txt -d -base64 -K  
5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv  
1907C5E255F7FC9A6B47B0E789847AED
```

ANSWER: takagi KEY: ud6s98n

RIDDLE 4:

**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

What would Jill use to decrypt Jack's message? *

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

Jack and Jill invited Bob, Alice, Tim and Peter along to exchange some messages. How many keys would they all need for asymmetric vs

Tim just sent an encrypted message to one of his friends, which of the following keys did he likely use to encrypt the message *

- Tim's Public Key
- Alice's Public Key
- Peter's Private Key
- Tim's Private Key
- Bob's Private Key

ANSWER: 7gsn3nd2

RIDDLE 5:

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

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

Hash:

3b75cdd826a16f5bba0076690f644dc7

[hashcat -m 0 temp rockyou.txt](#)

[ANSWER: argyle KEY:ajy39d2](#)

RIDDLE 6:

**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.**

steghide extract -sf mary-lamb.jpg ; #pass : ABC

ANSWER:mcclane KEY: 7skahd6

Image Link:

<https://drive.google.com/file/d/1m9ykscnTGzgkkVet9wmiBCYsbhzbrKR9/view>

The screenshot shows a Mozilla Firefox browser window with the title "RANSOMWARE DECRYPTER - Mozilla Firefox". The address bar displays the URL <https://sites.google.com/view/cryptobreakout/ransomware-decrypter>. The page content is a Google Form titled "RANSOMWARE DECRYPTER". The message in the form states: "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!". Below the message is a link "Submit another response". At the bottom of the form, there is a note: "GoogleForms This content is neither created nor endorsed by Google." The background of the browser window shows a dark-themed interface with various tabs and links related to Kali Linux and security tools.