

HOMework #10 – Gavin Faught

[Home](#)
[INSTRUCTIONS](#)
[RANSOMWARE DECRYPTER](#)
[RIDDLE 1](#)
[RIDDLE 2](#)
[RIDDLE 3](#)
[RIDDLE 4](#)
[RIDDLE 5](#)
[RIDDLE 6](#)

The screenshot shows a ransomware message titled "Ooops, your files have been encrypted!". It explains that important files are encrypted and offers two options to recover them: solving 6 riddles or paying 100 Bitcoins. A Bitcoin payment address is provided, and a "Check Payment" button is visible.

SCENARIO

You are a Cyber Security Analyst at Nakatomi Hospital. Unfortunately, one of your Doctors opened up an email which contained Ransomware.

This Ransomware spread throughout the hospital and encrypted all of the Hospital Patient records. The Ransomware has given you two options to decrypt and retrieve your patient records:

- 1) Pay 100 Bitcoins
- 2) Solve 6 Riddles

Since you refuse to pay off any ransom, you need to act fast to solve the 6 riddles from the Ransomware as the Doctors need to access the patient records as lives are at stake!

Instructions:

[Home](#)[INSTRUCTIONS](#)[RANSOMWARE DECRYPTER](#)[RIDDLE 1](#)[RIDDLE 2](#)[RIDDLE 3](#)[RIDDLE 4](#)[RIDDLE 5](#)[RIDDLE 6](#)[?](#)

The image shows a digital interface for a ransomware decryption tool. It features a dark background with a grid of numbers in various colors (blue, green, yellow, red). In the center, there is a large, stylized skull icon with a white outline and a red interior. Below the skull, the word "RANSOMWARE" is written in large, bold, red capital letters. The overall aesthetic is high-tech and ominous.

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



Shifting characters 8 to the left gets: "gruber"
FIRST 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**

Using the Browserling Binary-to-Test converter gives us: Gennero
Second 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

Key:

5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564

IV (Initialization Vector):

1907C5E255F7FC9A6B47B0E789847AED

OpenSSL Options:

☐ -pbkdf2

☐ -nosalt

☐ -aes-256-cbc

☐ base64

echo "4qMOIvwEGXzvKMrE2bNbg==" > plainmessage.txt.enc

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

SOLUTION: 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

Jill's Public Key

What would Jill use to to decrypt Jacks message? *

- ☐ Jack's Public Key
- ☐ Jack's Private Key
- ☐ Jill's Public Key
- ☐ Jill's Private 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 symmetric encryption? *

- ☐ 6 Asymmetric and 15 Symmetric
- ☐ 15 Asymmetric and 12 Symmetric
- ☐ 10 Asymmetric and 15 Symmetric
- ☐ 12 Asymmetric and 30 Symmetric
- ☐ 12 Asymmetric and 15 Symmetric

Symmetric: $(6)(5)/2 = 15$

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

Asymmetr
ic: $6*2 = 12$

Alice's Public Key
Key: 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

Using: <http://reverse-hash-lookup.online-domain-tools.com/> 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

→ **Passphrase:** ABC

Data extracted to "code_is_inside_this_file.txt"

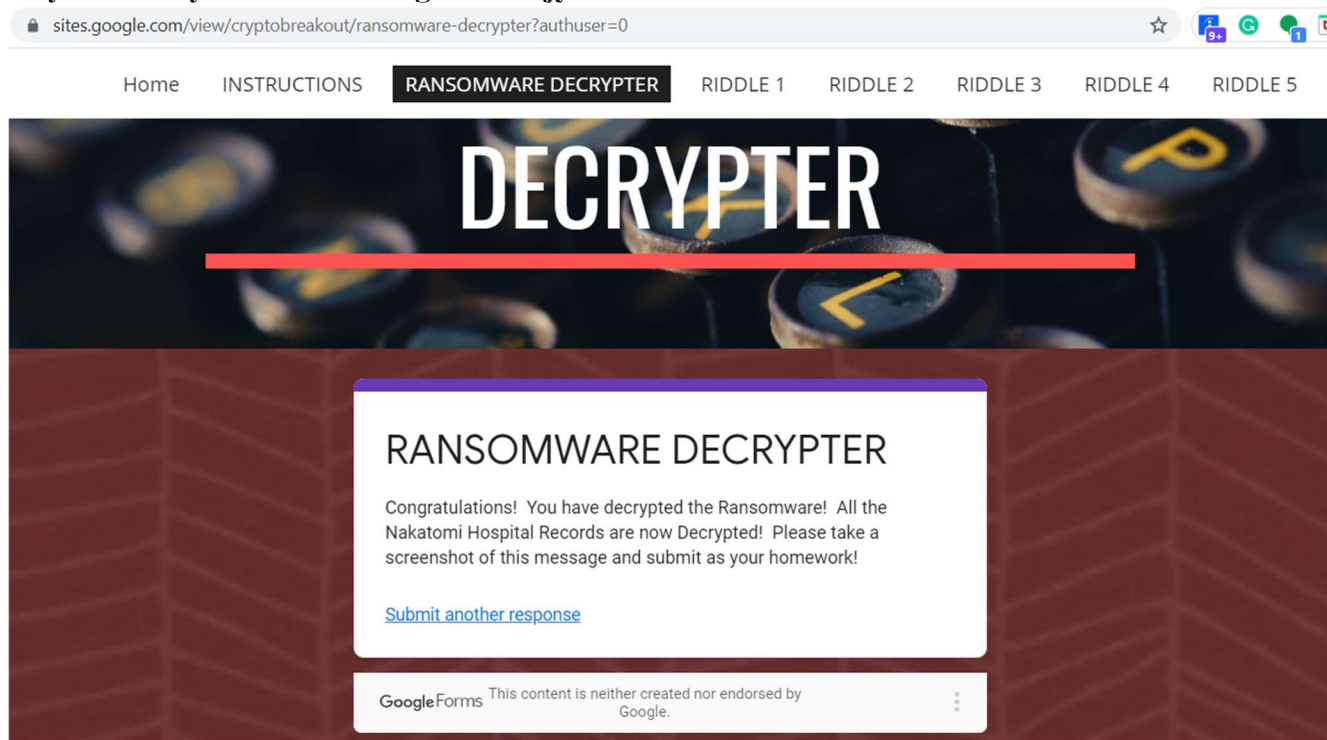
ANSWER: mcclane

Key: 7skahd6

Image Link: <https://drive.google.com/file/d/1m9ykscnTGzgkVet9wmiBCYsbhzbrKR9/view>

RANSOMWARE DECRYPTER

Key: 6skd8scy8snd2ud6s98n7gsn3nd2ajy39d27skahd6



Gavin's Corner – Cryptography Not Covered in Class

Cryptography comes in many forms. One such form is called the substituted word form, sometimes known as the "lesser cipher". The two parties agree on a word or phrase to act as a "key." This key is a word, ideally from a book that is acquired by both parties. They could contact each other at any time to change the key (instead of the fifth word in the body on page 4, let's use the tenth word in the body on page 11.) Here it is in action:

Encrypted message: (A=1, B=2, C=3...)

G i g G f v l c

R u b B e d r u the key "rubbed" is repeated until the end of the message → page 123 word #2 (from the book Dune)

where u minus a = t, c minus n = o, g minus r = o, etc... The decrypted message is on the next page.

Decrypted message: One Earth