

##10-Cryptography Homework: Ransomware Riddles

Riddle 1 Answer:

gruber

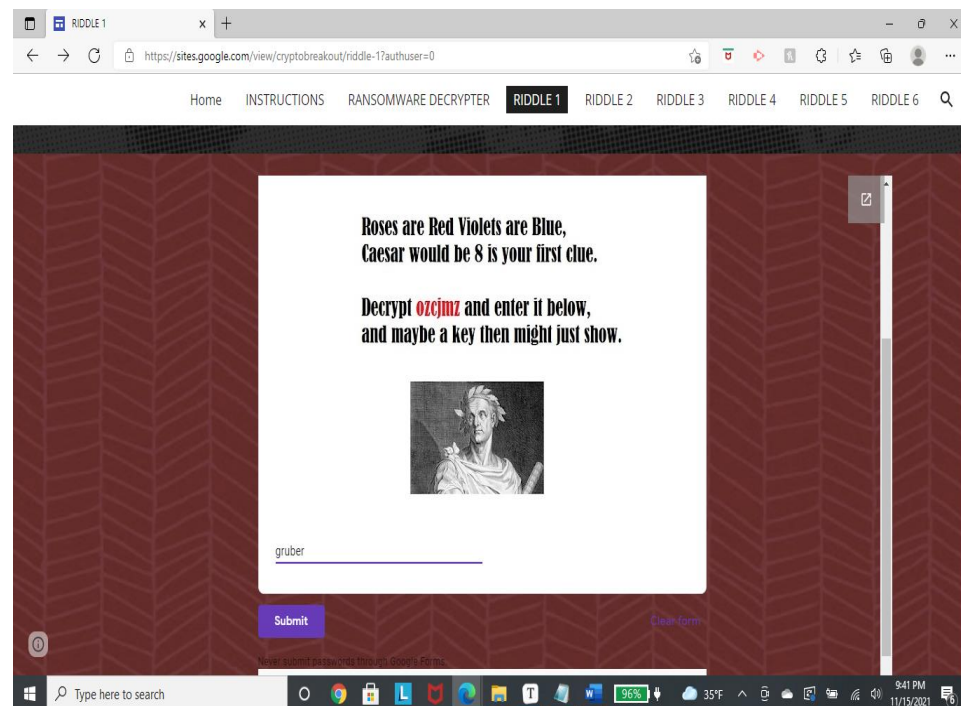
The first key is:

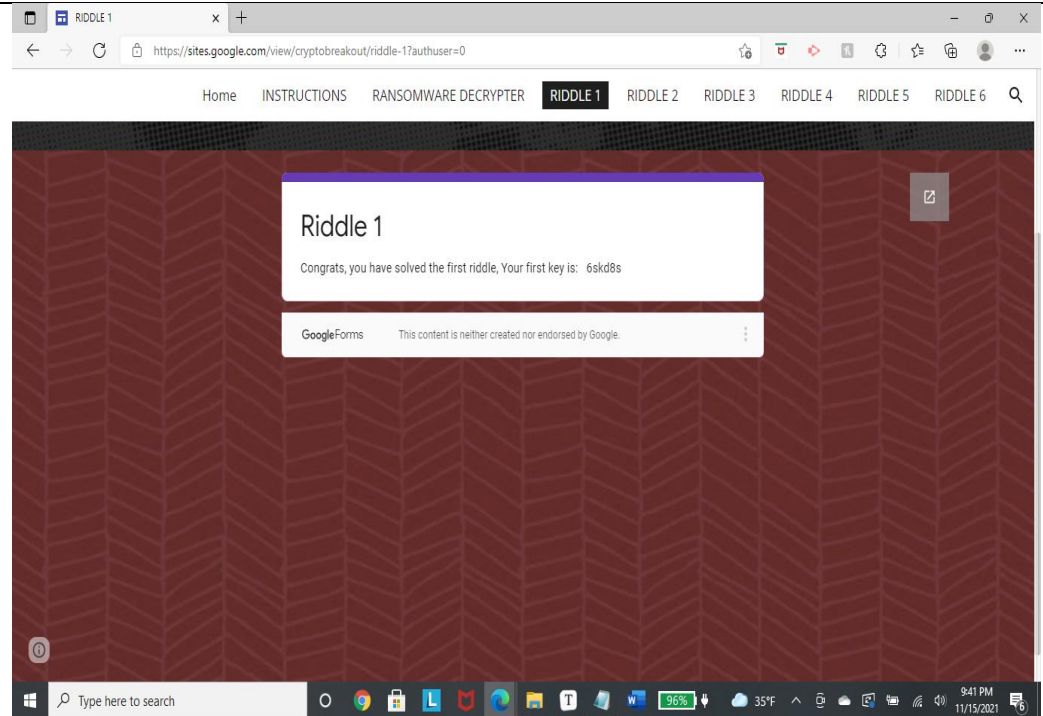
6skd8s

This is how I decrypted the 1st riddle:

o ---> g z ---> r c ---> u j ---> b m ---> e z ---> r
ozcjmz ---> gruber

Below are some captured screenshots:



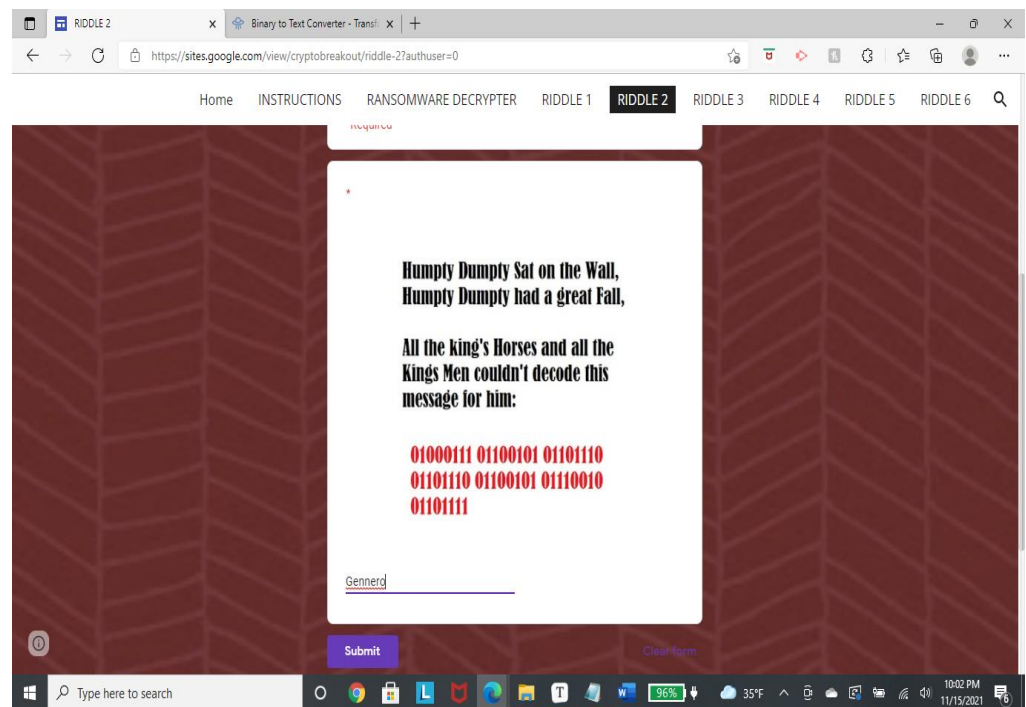


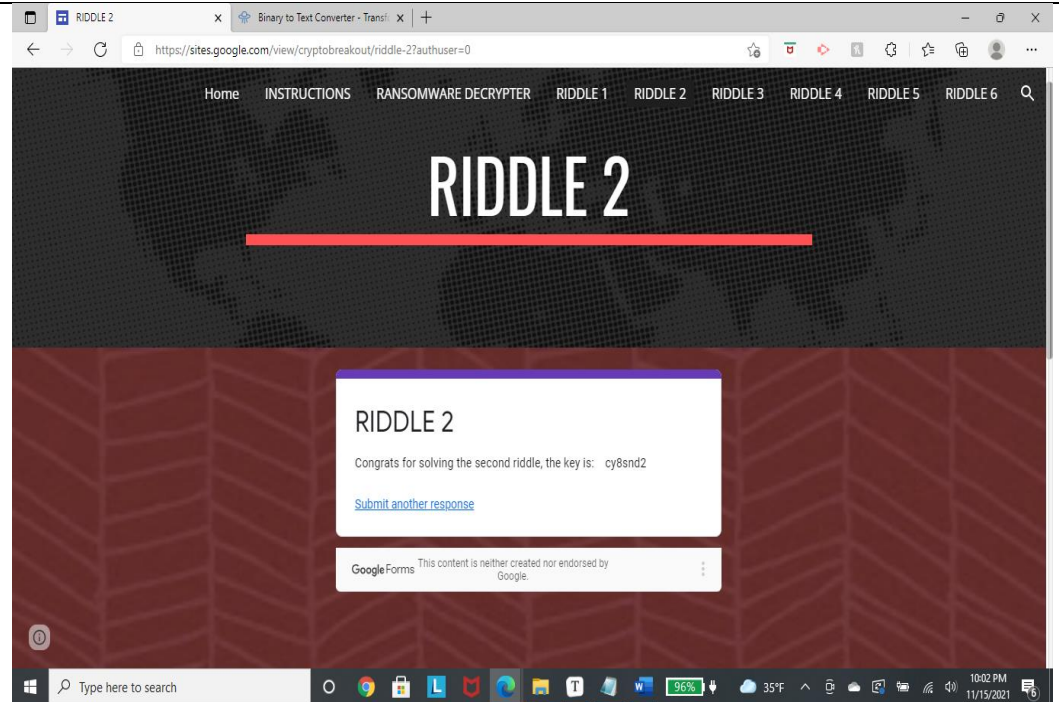
Riddle 2 Answer:

Gennero

**The second key
is: cy8snd2**

Using the below website, I converted the Binary to Text:
[Binary to Text Converter - Transform Binary String to Text - Online - Browserling Web Developer Tools](https://www.browserling.com/tools/binary-to-text-converter)





Riddle 3 Answer:

Takagi

**The third key:
ud6s98n**

Using the below openssl command and the cipher info, vector, key, I solved the 3rd riddle:

```
openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in riddle3ciphertext.txt -base64 -K
```

```
5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED
```

```

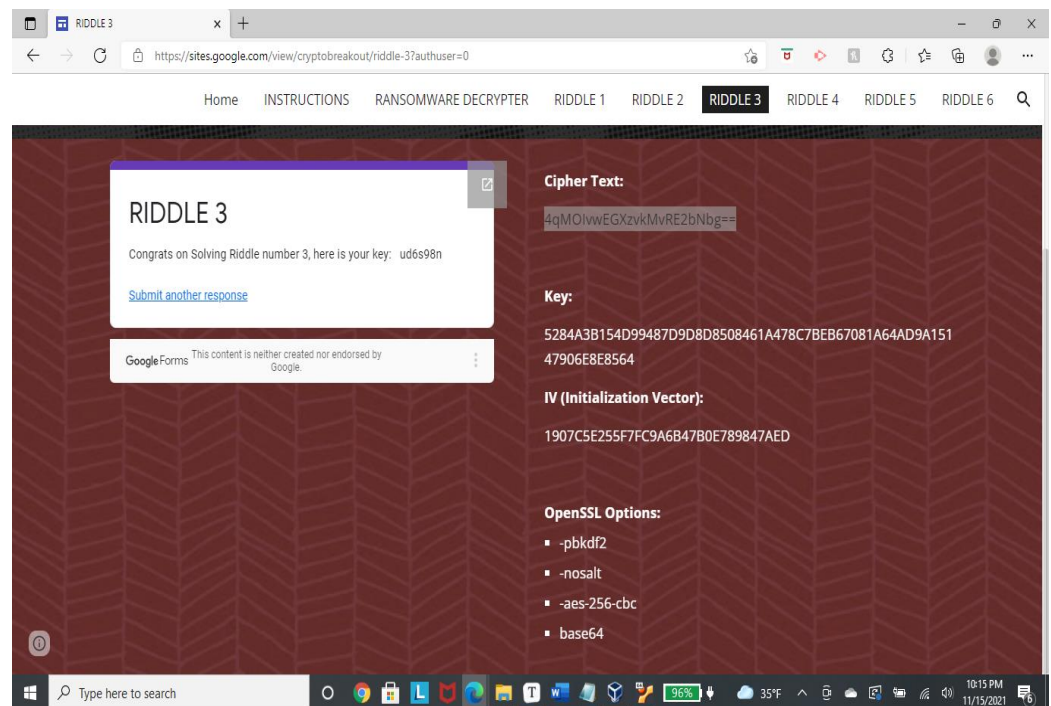
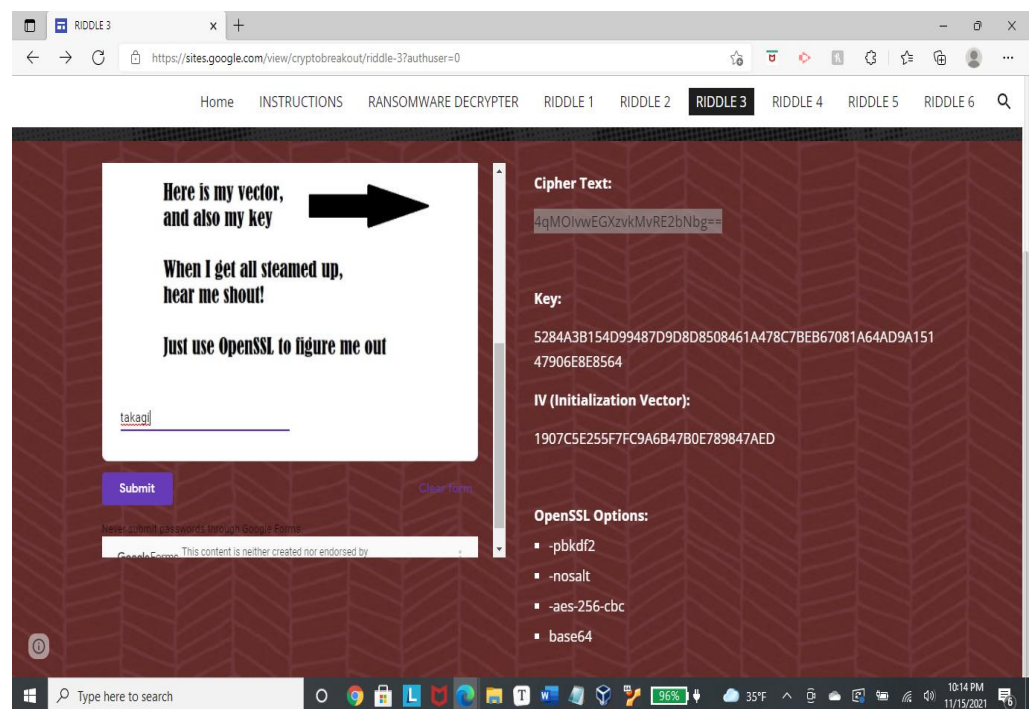
Activities  Terminal
sysadmin@UbuntuDesktop: ~/Documents/openssl/homework

sysadmin@UbuntuDesktop:~$ ls
arp_packets.pcap      Music                synscan.pcapng
Cybersecurity-Lesson-Plans  packetcapTCPclass.pcapng  sys_info.sh
Desktop              Pictures             system.sh
DHCPActivity.pcapng   Projects            Templates
Documents            Public              testk.sh
Downloads            python              today.sh
for_loops.sh         research            Videos
kansascityWEF.pcap   scripts             wireless2.pcapng

sysadmin@UbuntuDesktop:~$ cd Do
bash: cd: Do: No such file or directory
sysadmin@UbuntuDesktop:~$ cd Documents/
sysadmin@UbuntuDesktop:~/Documents$ ls
Darkside.pcap  epscript  openssl  web-vulns
docker_files  missingfiles  setup_scripts

sysadmin@UbuntuDesktop:~/Documents$ cd openssl
sysadmin@UbuntuDesktop:~/Documents/openssl$ ls
activity
sysadmin@UbuntuDesktop:~/Documents/openssl$ mkdir homework
> ^C
sysadmin@UbuntuDesktop:~/Documents/openssl$ mkdir homework
sysadmin@UbuntuDesktop:~/Documents/openssl$ ls
activity  homework
sysadmin@UbuntuDesktop:~/Documents/openssl$ cd homework/
sysadmin@UbuntuDesktop:~/Documents/openssl/homework$ ls
sysadmin@UbuntuDesktop:~/Documents/openssl/homework$ echo "4qM0IvwEGXzvKvMRE2bNbg==" > riddle3ciphertext.txt
sysadmin@UbuntuDesktop:~/Documents/openssl/homework$ ls
riddle3ciphertext.txt
sysadmin@UbuntuDesktop:~/Documents/openssl/homework$ openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in riddle3ciphertext.txt -base64 -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED
takagi
sysadmin@UbuntuDesktop:~/Documents/openssl/homework$

```



Riddle 4 Answers:
Answer 1: Jill's
Public Key

Below are screenshots of the answers to the 4 questions asked:

Answer 2: Jill's

Private Key

Answer 3: 12

Asymmetric and 15

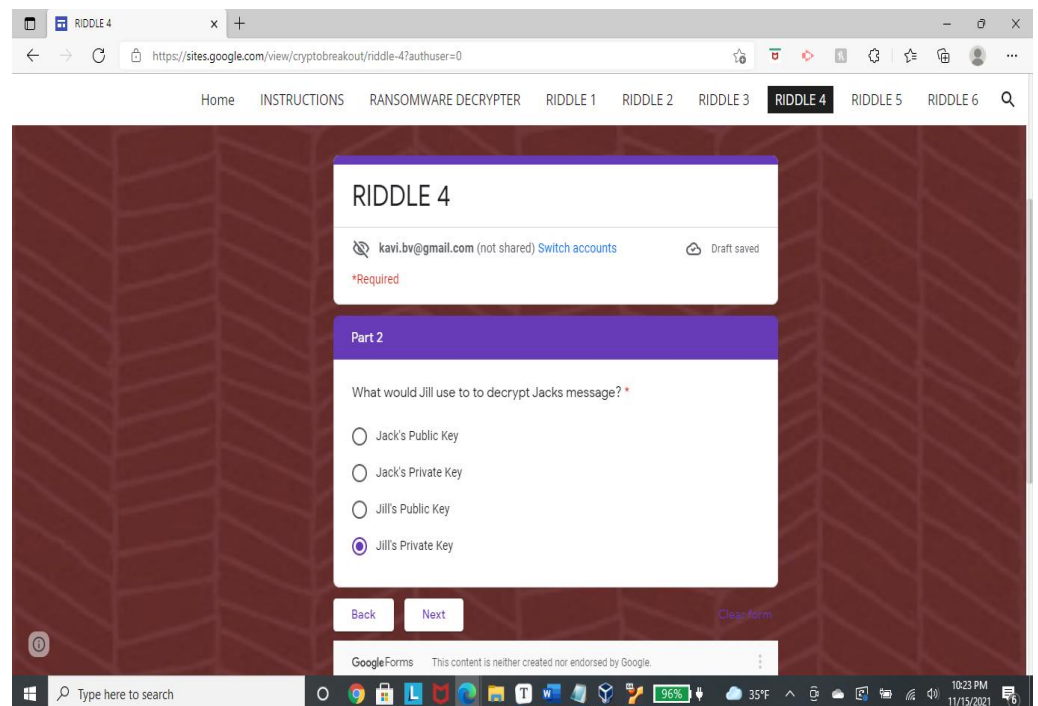
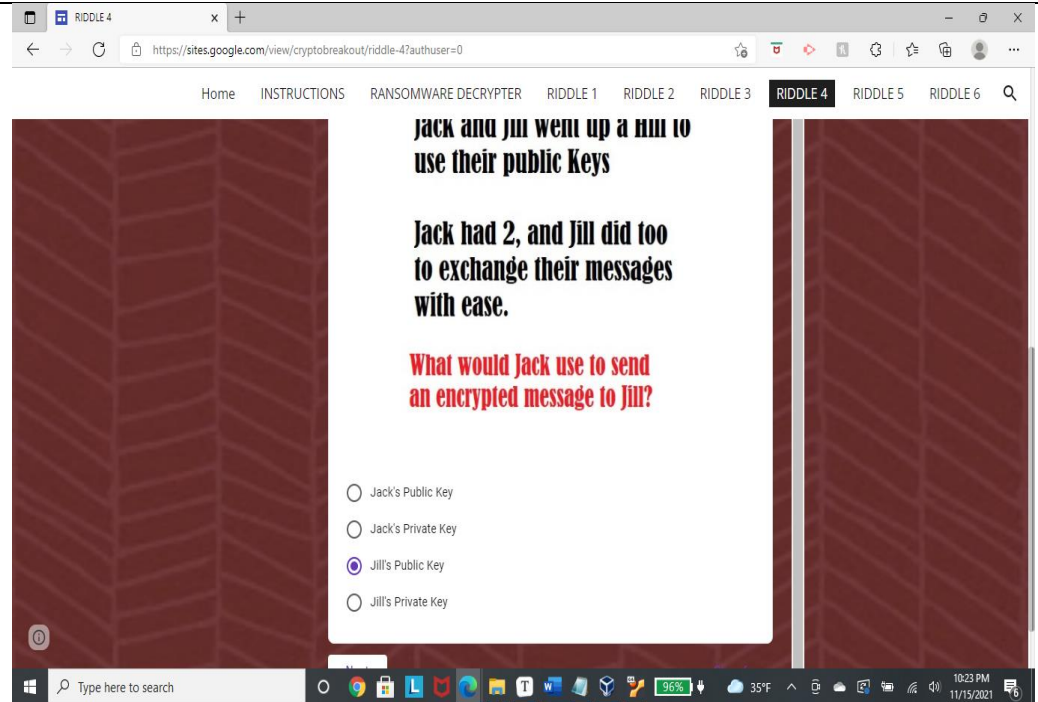
Symmetric

Answer 4: Alice's

Public Key

The fourth Key is:

7gsn3nd2



RIDDLE 4

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

kavi.bv@gmail.com (not shared) [Switch accounts](#) Draft saved

*Required

Part 3

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? *

☐ 15 Asymmetric and 12 Symmetric

☐ 12 Asymmetric and 30 Symmetric

☐ 6 Asymmetric and 15 Symmetric

☐ 10 Asymmetric and 15 Symmetric

☒ 12 Asymmetric and 15 Symmetric

[Back](#) [Next](#) [Clear form](#)

GoogleForms This content is neither created nor endorsed by Google.

RIDDLE 4

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

kavi.bv@gmail.com (not shared) [Switch accounts](#) Draft saved

*Required

Part 4

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

☐ Bob's Private Key

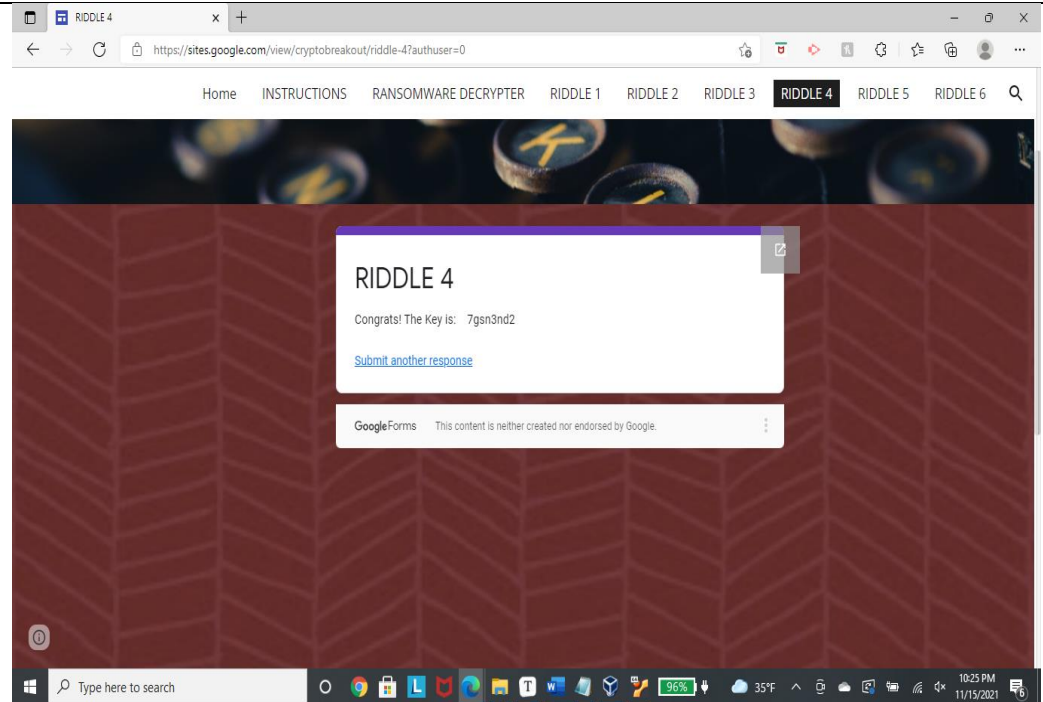
☐ Peter's Private Key

☒ Alice's Public Key

☐ Tim's Private Key

[Back](#) [Next](#) [Clear form](#)

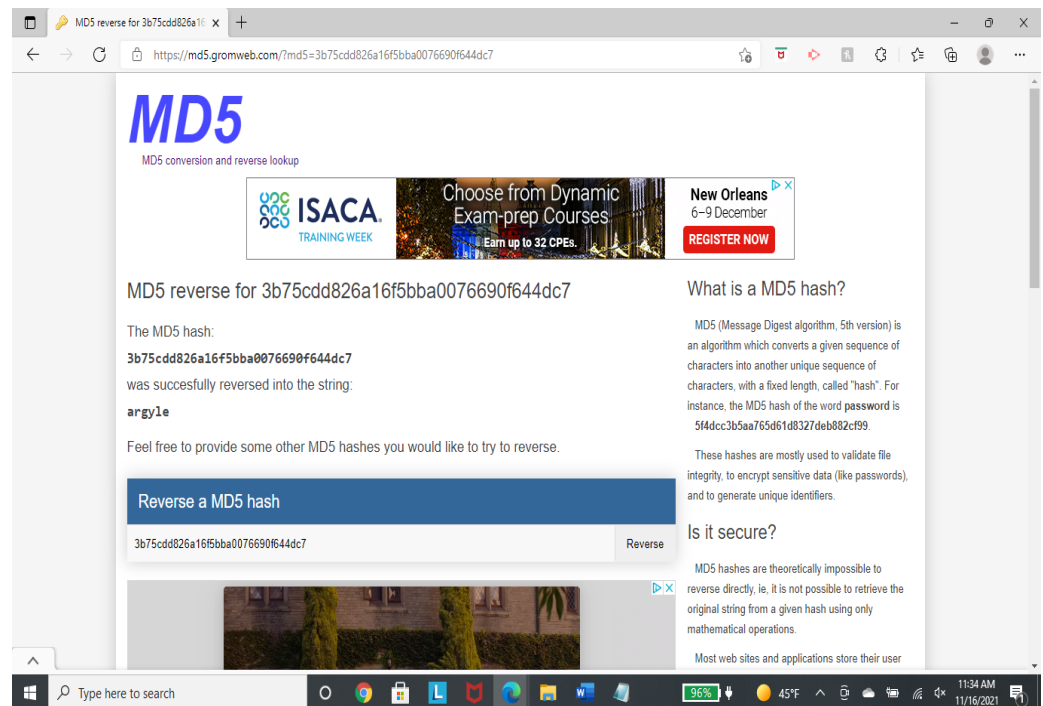
GoogleForms This content is neither created nor endorsed by Google.

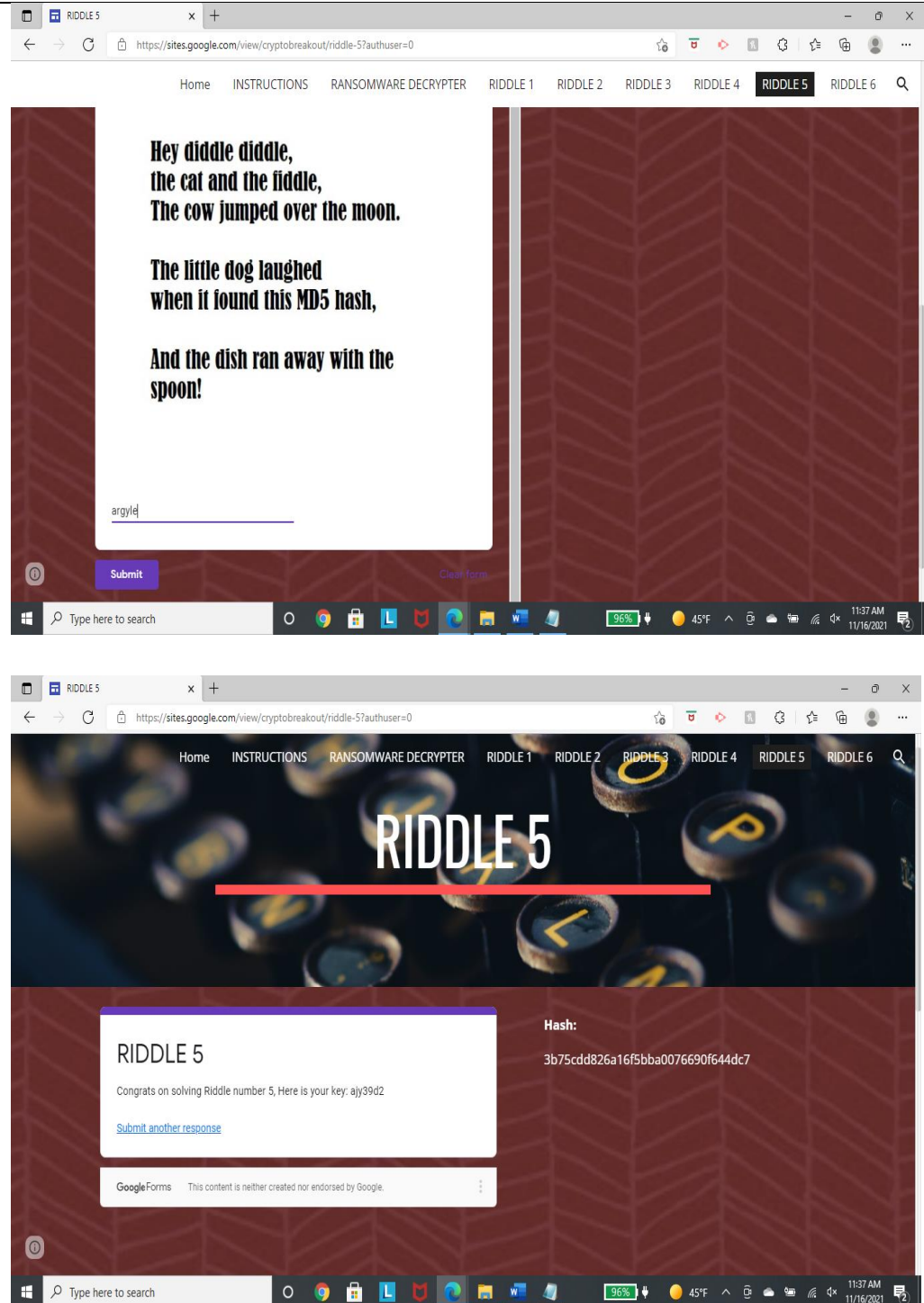


Riddle 5 Answer:

argyle

The fifth key is:
ajy39d2

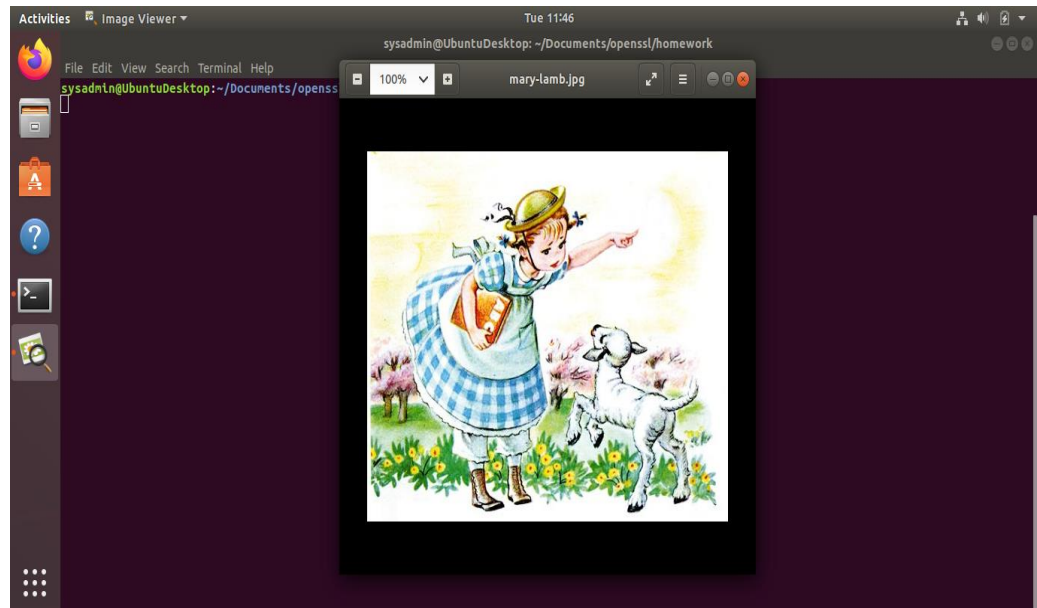




Riddle 6 Answer:
mcclane
The sixth key is:
7skahd6.

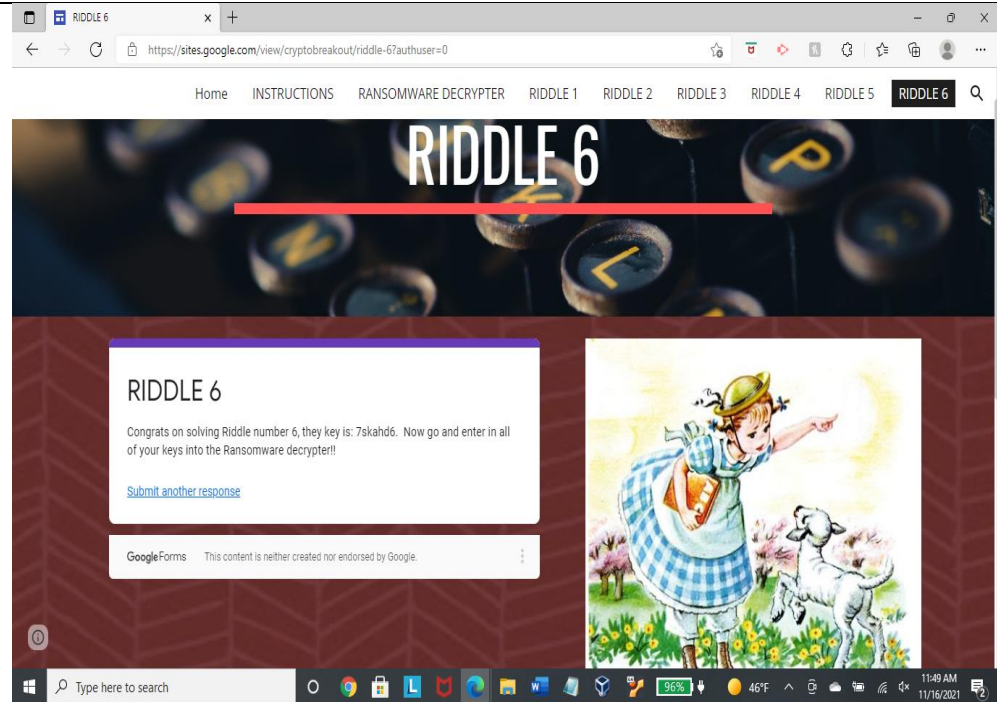
Using below command, I extracted the code from the mary-lamb.jpg file:
`steghide extract -sf mary-lamb.jpg`

The hidden code is extracted into a file - code_is_inside_this_file.txt.
The contents of this file reveal the answer for this riddle.



```
Activities Terminal Tue 11:47
sysadmin@UbuntuDesktop: ~/.Documents/openssl/homework

File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/.Documents/openssl$ eog mary-lamb.jpg
sysadmin@UbuntuDesktop:~/.Documents/openssl/homework$ steghide extract -sf mary-lamb.jpg
Enter passphrase:
wrote extracted data to "code_is_inside_this_file.txt".
sysadmin@UbuntuDesktop:~/.Documents/openssl/homework$ ls
code_is_inside_this_file.txt hash.txt mary-lamb.jpg riddle3ciphertext.txt solved.txt
sysadmin@UbuntuDesktop:~/.Documents/openssl/homework$ cat code_is_inside_this_file.txt
mcclane
sysadmin@UbuntuDesktop:~/.Documents/openssl/homework$
```



Ransomware Decrypter
Congratulations!
You have
decrypted the
Ransomware! All
the Nakatomi
Hospital Records
are now
Decrypted!

After entering all the keys captured by solving the 6 riddles, I got the below screen, indicating Success.

