Week 10 - Cryptography

Topics covered in this assignment:

- Encryption
- Decryption
- Caesar Cipher
- Encoding and Decoding
- Binary
- Symmetric and Asymmetric Encryption
- Open SSL
- Key/IV
- Public/Private Keys
- Key Distribution
- Hashing
- Hashing Algorithms
- Hashcat
- Steganography
- Steghide

Website: https://sites.google.com/view/cryptobreakout/

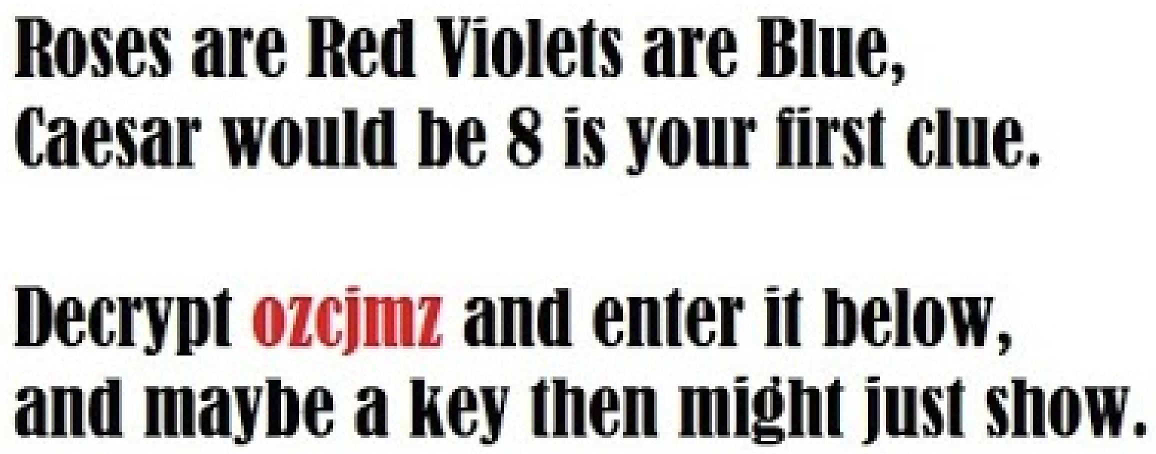
Instructions:

In order to solve each riddle, you will need to apply cryptographic concepts covered in the past three lessons. concepts will need to be applied.

- Once the riddle has been solved, submit your answer on the bottom of each Riddle Page.
- If you are correct, you will receive a key. Save this key in your notes.
- Once you have collected all six keys, select the Ransomware Decrypted header on the website and enter all your keys.
- If all the six keys are correct, the ransomware will be removed and the data will be decrypted.
- You will need to submit a screenshot as proof that the ransomware has been decrypted.

CryptoBreakout Assignment

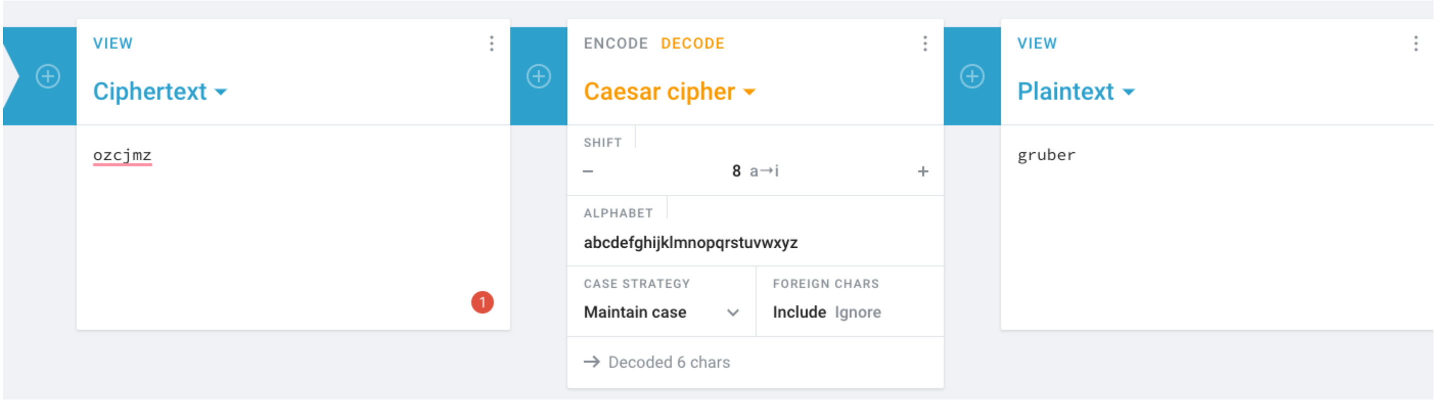
Riddle 1



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.

Used: **https://cryptii.com/pipes/caesar-cipher** - shifted the key to 8.



```
ozcjmz
```

SHIFT: 8 a→i

ALPHABET: abcdefghijklmnopqrstuvwxyz

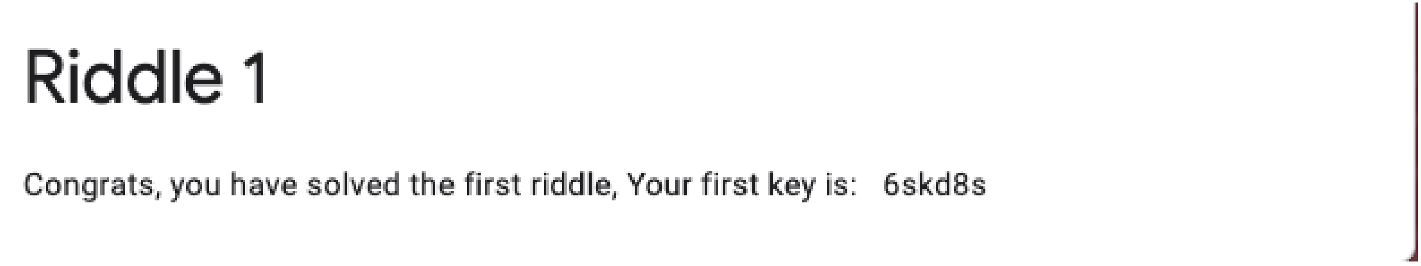
CASE STRATEGY: Maintain case

FOREIGN CHARS: Include Ignore

→ Decoded 6 chars

```
gruber
```

Entered the plaintext and received this answer:

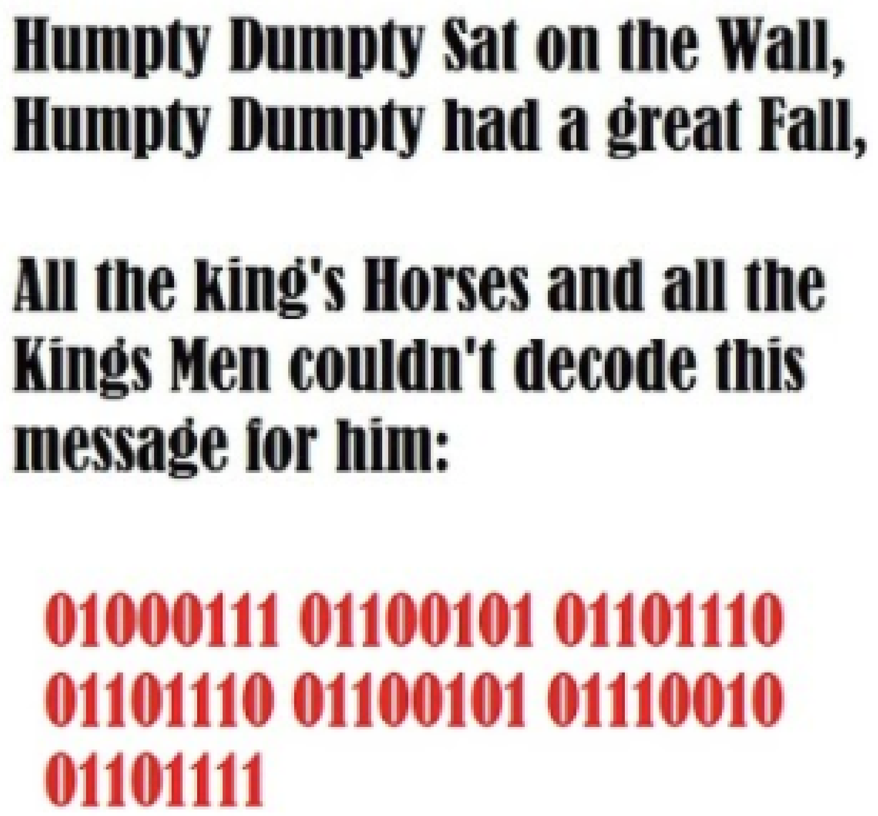


Riddle 1

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

Key 1: 6skd8s

Riddle 2

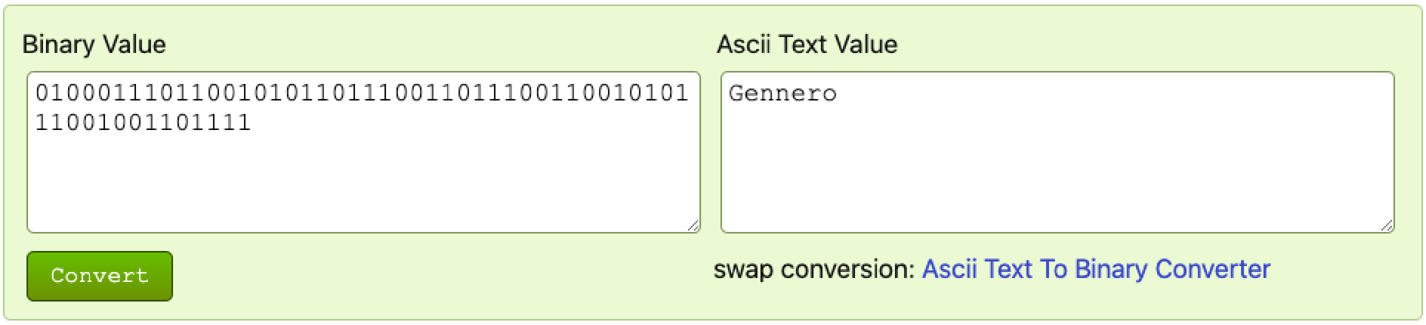


Humpty Dumpty Sat on the Wall,
Humpty Dumpty had a great Fall,

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

01000111 01100101 01101110
01101110 01100101 01110010
01101111

Used: **https://www.binaryhexconverter.com/binary-to-ascii-text-converter**



Binary Value

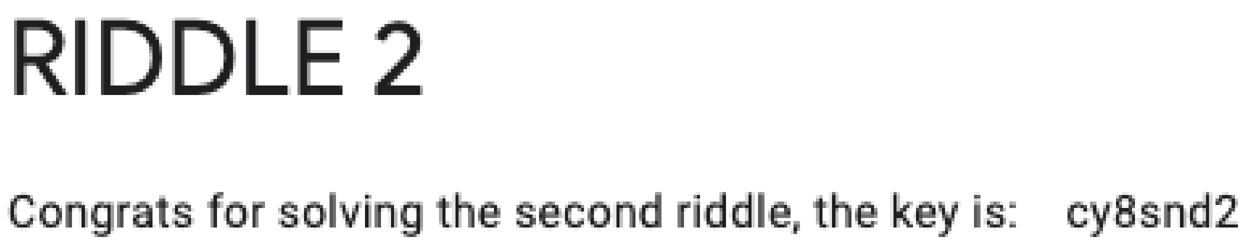
```
010001110110010101101110011011100110010101
11001001101111
```

Ascii Text Value

```
Gennero
```

swap conversion: Ascii Text To Binary Converter

Entered the plaintext and received this answer:

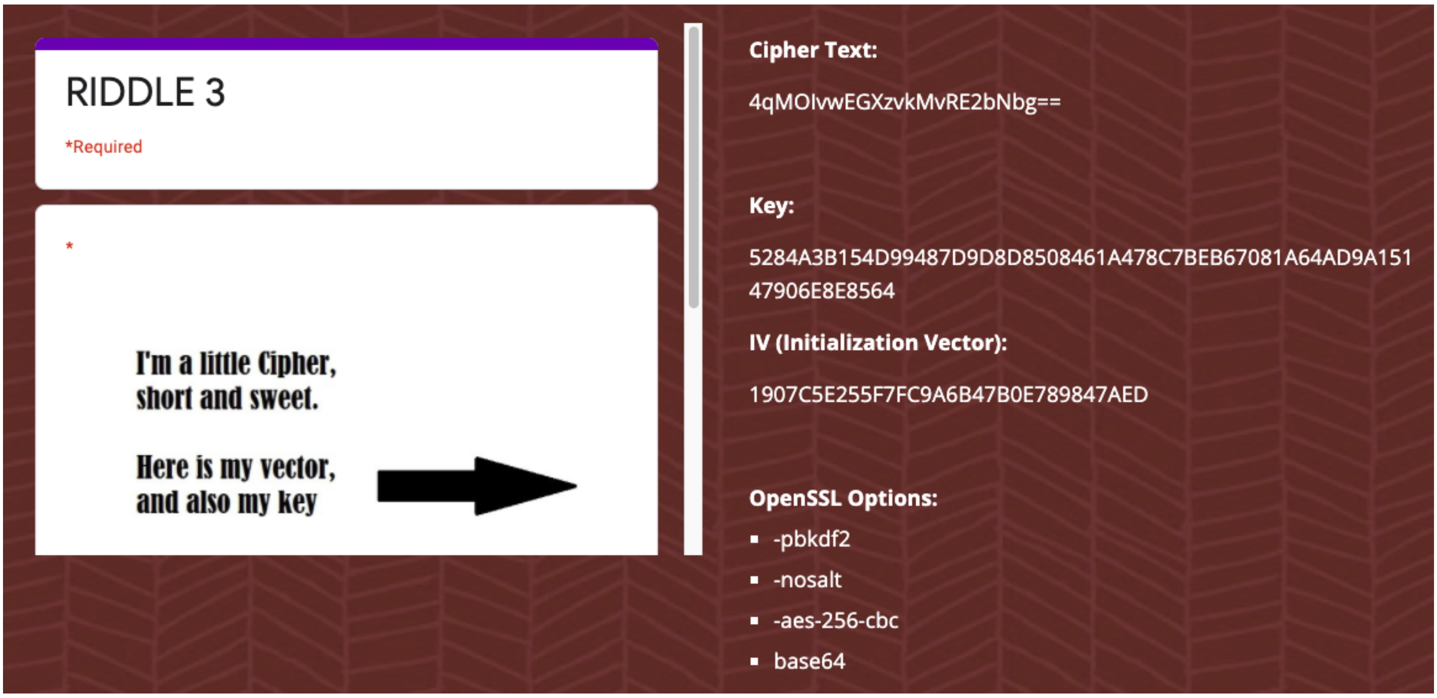


RIDDLE 2

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

Key 2: cy8snd2

Riddle 3



RIDDLE 3

*Required

*

I'm a little Cipher,
short and sweet.

Here is my vector,
and also my key

Cipher Text:

4qMOIvwEGXzvkMvRE2bNbg==

Key:

5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A151
47906E8E8564

IV (Initialization Vector):

1907C5E255F7FC9A6B47B0E789847AED

OpenSSL Options:

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

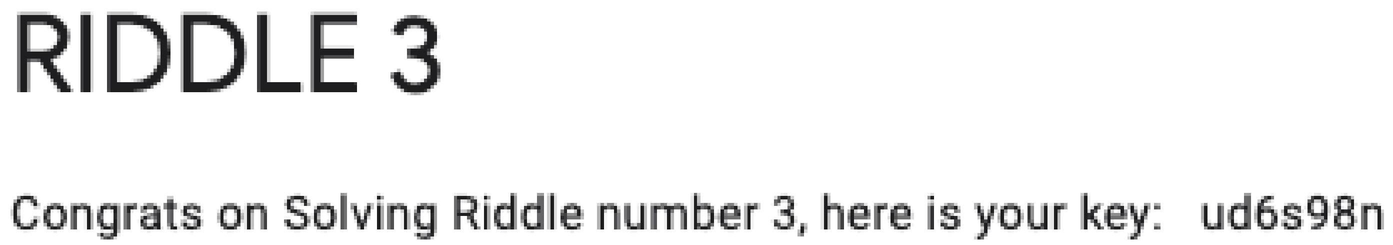
First, I copied the cipher text onto a text file:

```
cristina@kali:~/Desktop$ echo "4qMOIvwEGXzvkMvRE2bNbg==" >>
ciphertext_riddle.txt.enc
cristina@kali:~/Desktop$ cat ciphertext_riddle.txt.enc
4qMOIvwEGXzvkMvRE2bNbg==
```

Second, I used **openssl** to decrypt the message using the options given in the riddle:

```
cristina@kali:~/Desktop$ sudo openssl enc -pbkdf2 -nosalt -aes-256-cbc -in
ciphertext_riddle.txt.enc -d -base64 -K
5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv
1907C5E255F7FC9A6B47B0E789847AED
[sudo] password for cristina:
takagi
```

Entered the plaintext and received this answer:

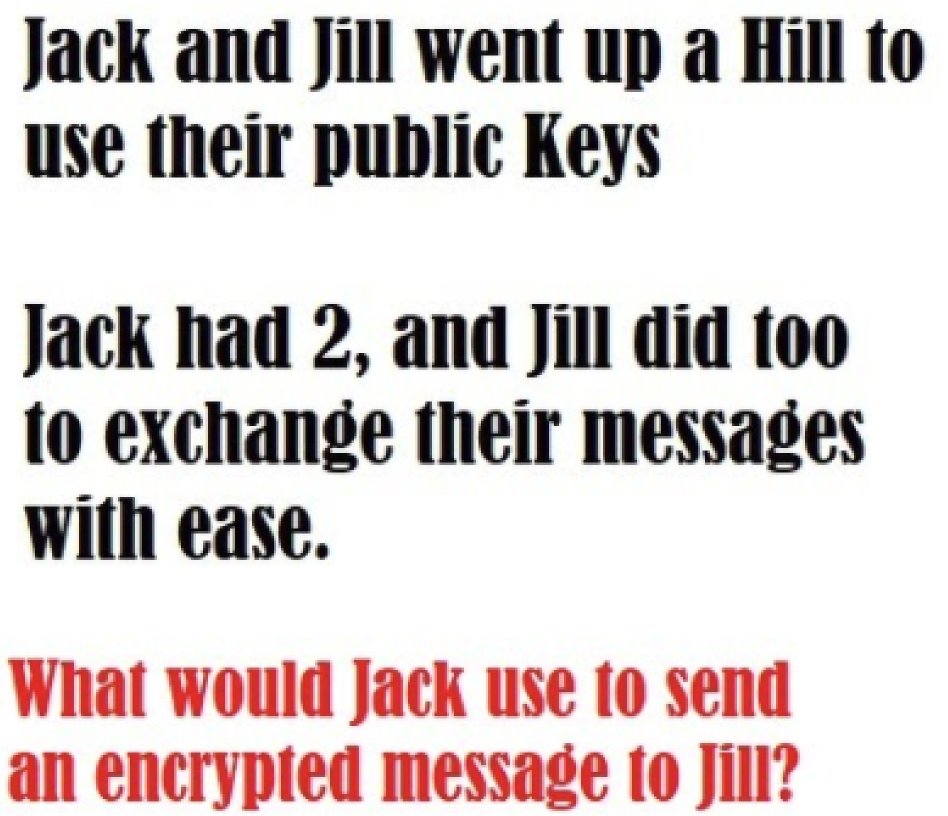


RIDDLE 3

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

Key 3: ud6s98n

Riddle 4

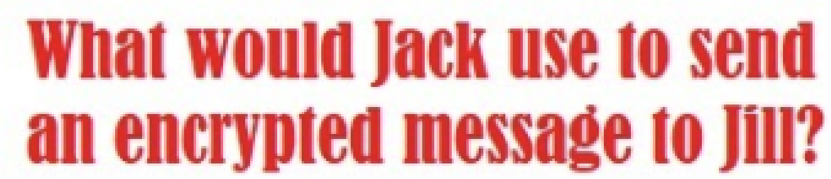


Jack and Jill went up a Hill to use their public Keys

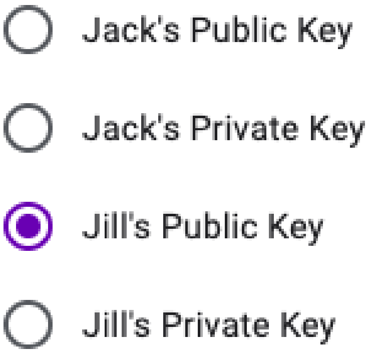
Jack had 2, and Jill did too to exchange their messages with ease.

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

The first answer is:



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



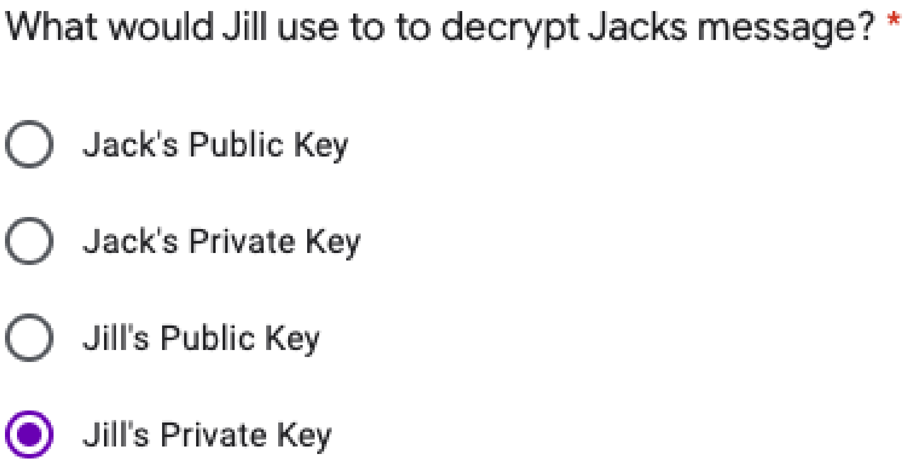
○ Jack's Public Key

○ Jack's Private Key

● Jill's Public Key

○ Jill's Private Key

The second answer is:



What would Jill use to to decrypt Jacks message? *

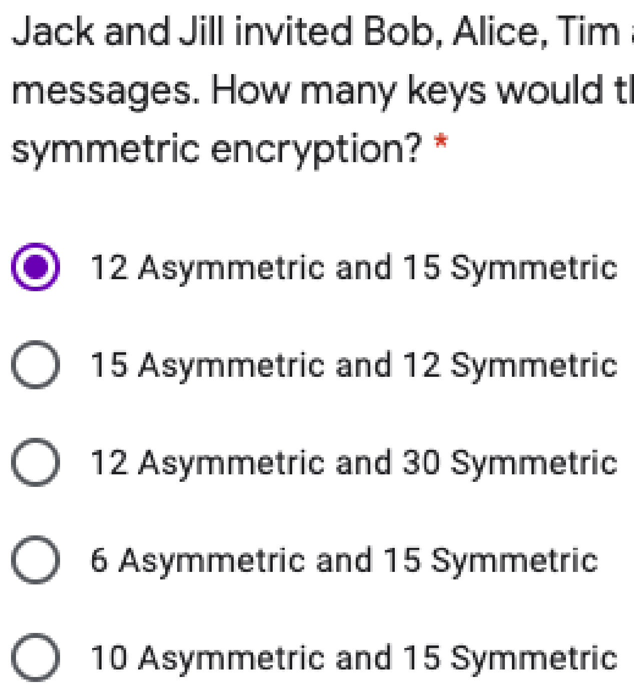
○ Jack's Public Key

○ Jack's Private Key

○ Jill's Public Key

● Jill's Private Key

The third answer is:



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? *

● 12 Asymmetric and 15 Symmetric

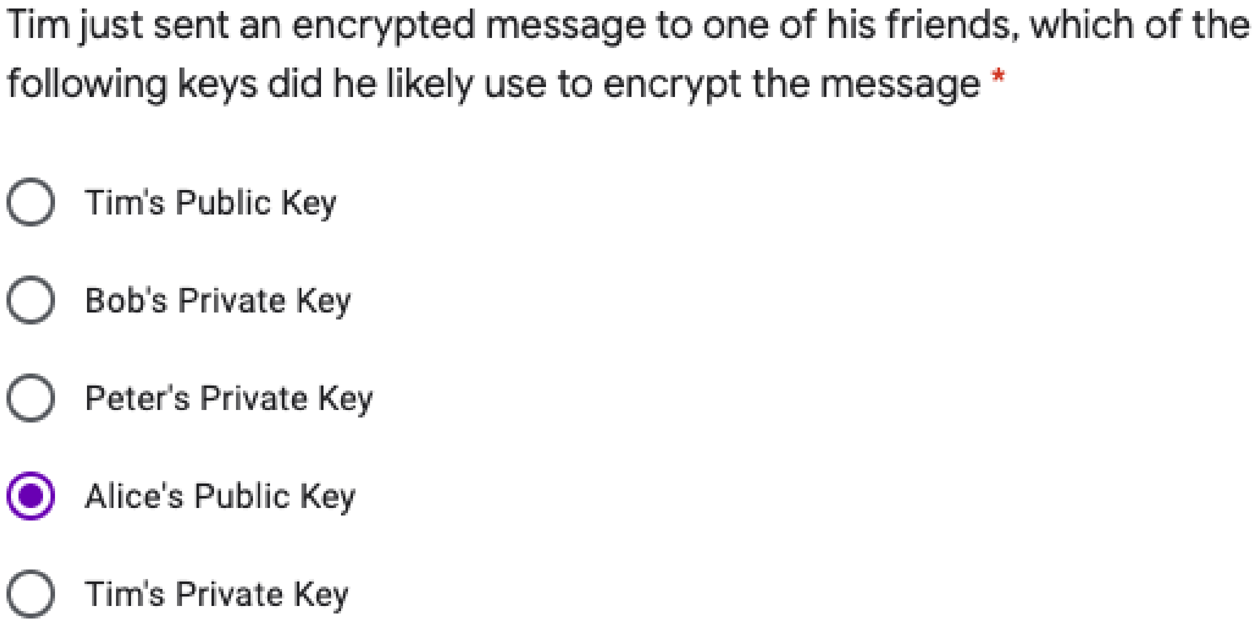
○ 15 Asymmetric and 12 Symmetric

○ 12 Asymmetric and 30 Symmetric

○ 6 Asymmetric and 15 Symmetric

○ 10 Asymmetric and 15 Symmetric

The fourth answer is:



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

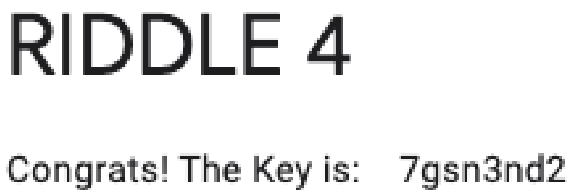
○ Bob's Private Key

○ Peter's Private Key

● Alice's Public Key

○ Tim's Private Key

Received this answer:

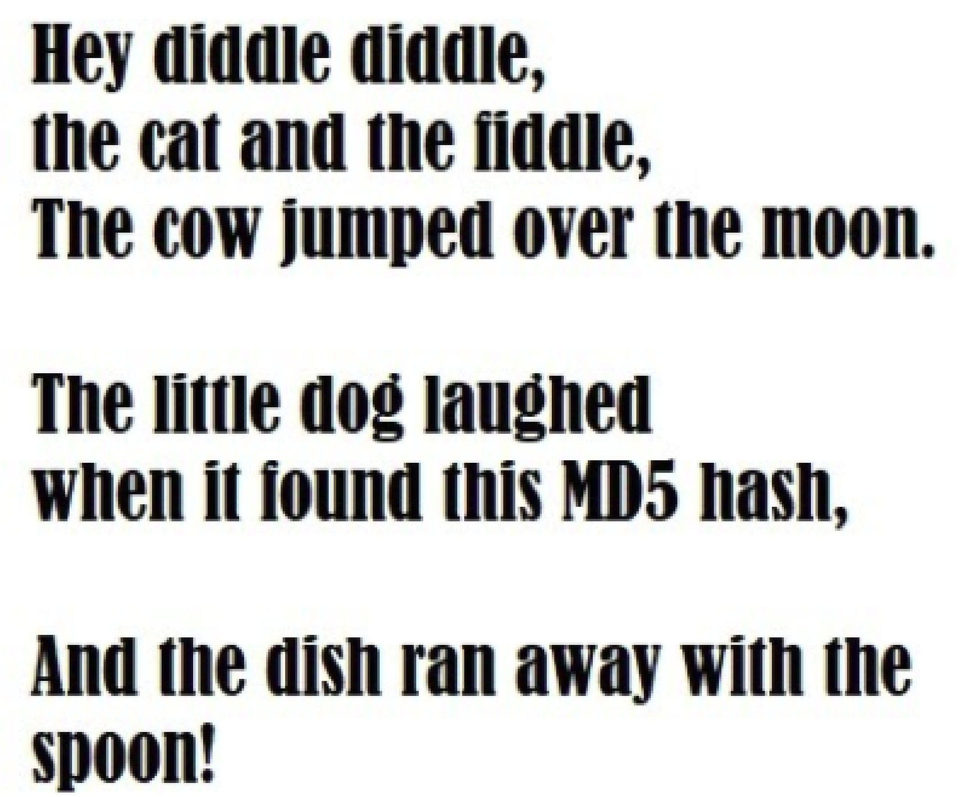


RIDDLE 4

Congrats! The Key is: 7gsn3nd2

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,

And the dish ran away with the
spoon!

First, I copied the hash onto a txt file:

```
cristina@kali:~/Desktop$ echo "3b75cdd826a16f5bba0076690f644dc7" >>
hash_riddle.txt
cristina@kali:~/Desktop$ cat hash_riddle.txt
3b75cdd826a16f5bba0076690f644dc7
```

Second, I used **hashcat** to crack the hash using md5 as the mode:

```
cristina@kali:~/Desktop$ hashcat -m 0 -a 0 -o solved_hash.txt hash_riddle.txt
rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i3-8100B CPU @ 3.60GHz, 512/1472 MB
allocatable, 1MCU

Hashes: 1 digests; 1 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-Hash
* 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.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=8 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
```

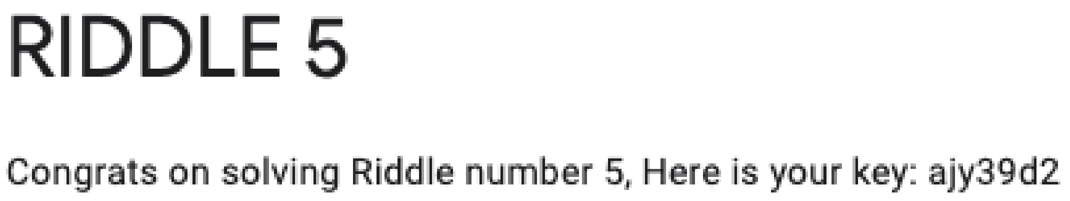
```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 3b75cdd826a16f5bba0076690f644dc7
Time.Started.....: Mon Jun 29 12:39:04 2020 (0 secs)
Time.Estimated...: Mon Jun 29 12:39:04 2020 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   201.3 kH/s (0.17ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 18432/14344385 (0.13%)
Rejected.........: 0/18432 (0.00%)
Restore.Point....: 17408/14344385 (0.12%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: paramedic -> tanika

Started: Mon Jun 29 12:39:02 2020
Stopped: Mon Jun 29 12:39:05 2020
```

Third, I used "cat" on the solved_hash.txt to see the cracked text:

```
cristina@kali:~/Desktop$ cat solved_hash.txt
3b75cdd826a16f5bba0076690f644dc7:argyle
```

I received this answer:

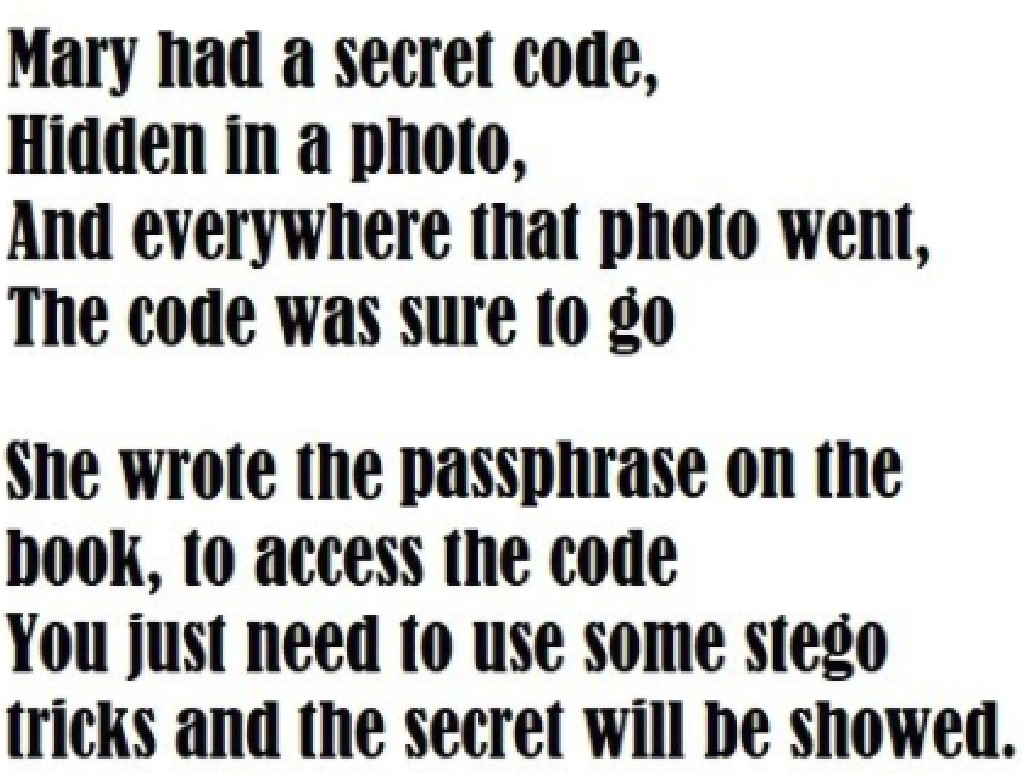


RIDDLE 5

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

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.

Image:

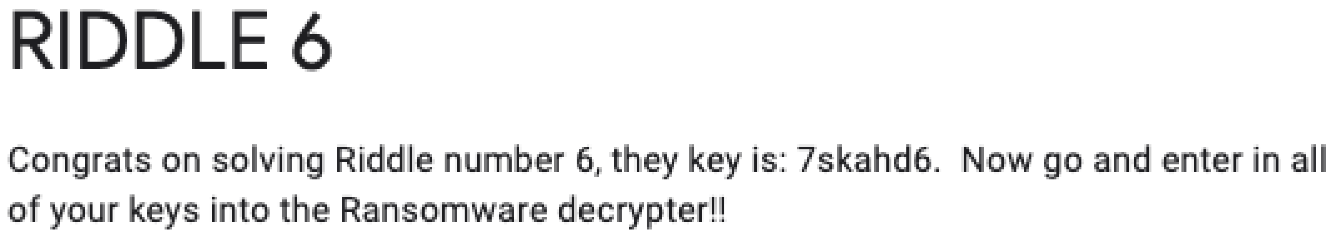
Based on the riddle, I knew I needed to use Steghide and use "ABC" as the passphrase:

```
cristina@kali:~/Desktop$ steghide extract -sf mary-lamb.jpg
Enter passphrase:
wrote extracted data to "code_is_inside_this_file.txt".
```

The passphrase worked! So I used "cat" to view the code in the file:

```
cristina@kali:~/Desktop$ cat code_is_inside_this_file.txt
mcclane
```

I entered the code and got this answer:



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!!

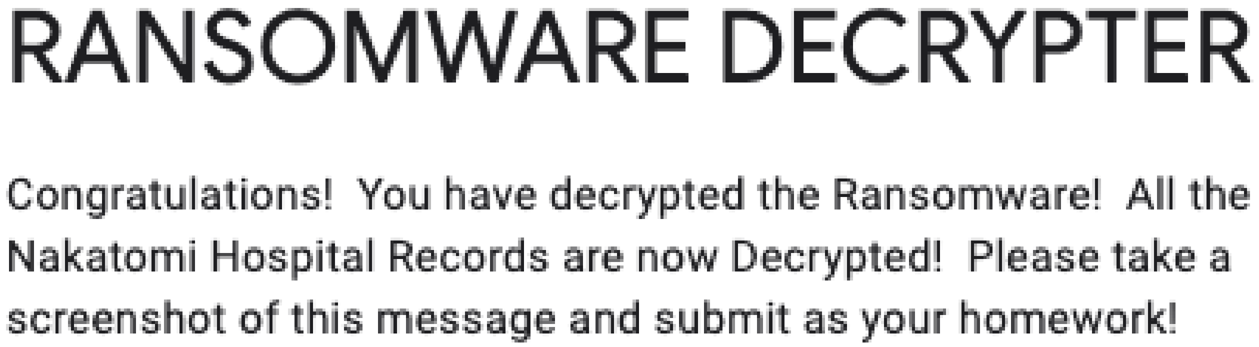
Key: 7skahd6

Ransomware Decrypter

I entered all the keys into the decrypter:

1. 6skd8s
2. cy8snd2
3. ud6s98n
4. 7gsn3nd2
5. ajy39d2
6. 7skahd6

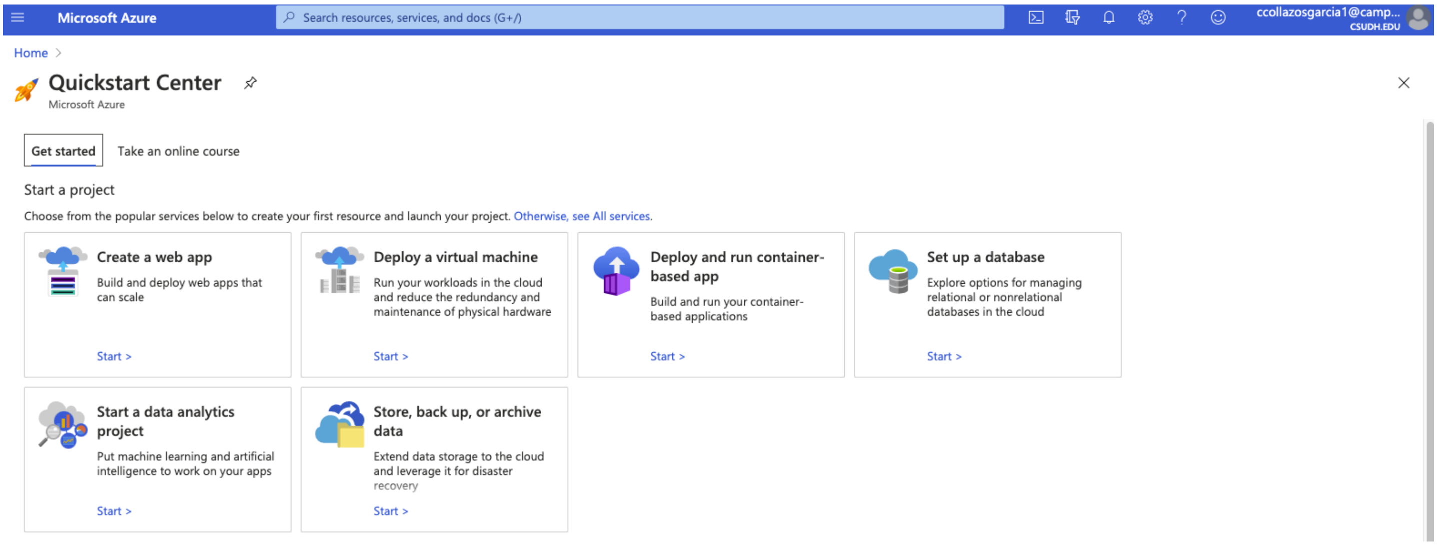
I received this answer:



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!

Azure Account Set-Up



Quickstart Center

Microsoft Azure

Start a project

Choose from the popular services below to create your first resource and launch your project. Otherwise, see All services.

Create a web app

Build and deploy web apps that can scale

Start >

Deploy a virtual machine

Run your workloads in the cloud and reduce the redundancy and maintenance of physical hardware

Start >

Deploy and run container-based app

Build and run your container-based applications

Start >

Set up a database

Explore options for managing relational or nonrelational databases in the cloud

Start >

Start a data analytics project

Put machine learning and artificial intelligence to work on your apps

Start >

Store, back up, or archive data

Extend data storage to the cloud and leverage it for disaster recovery

Start >