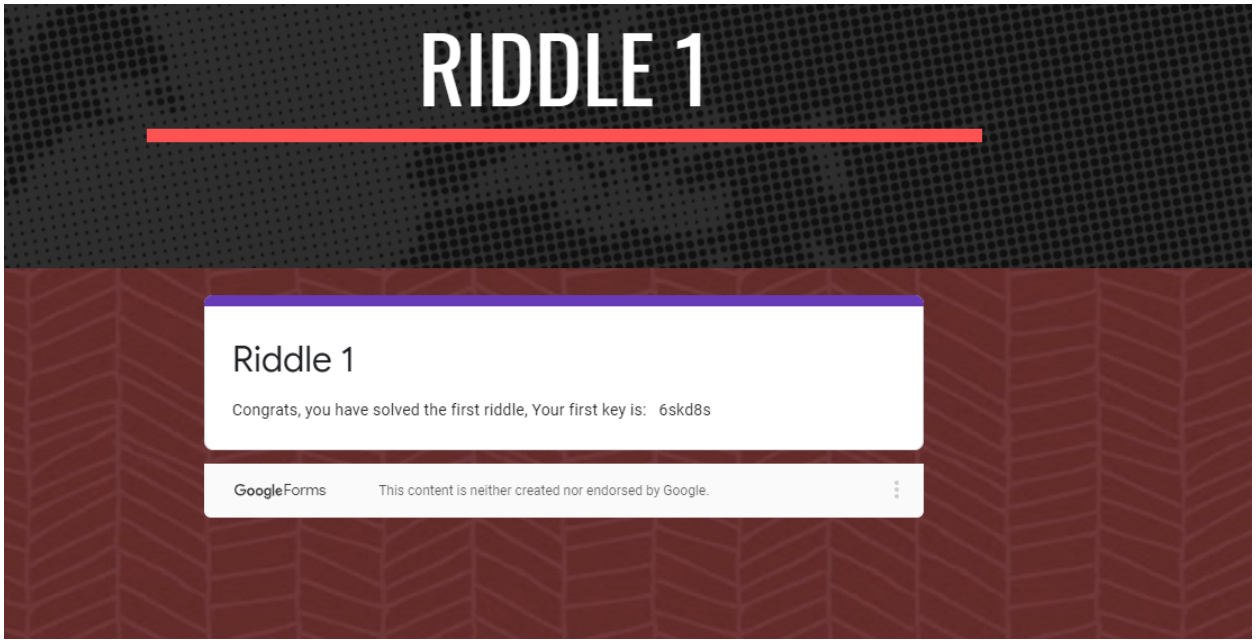
10:Cryptography Project

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.

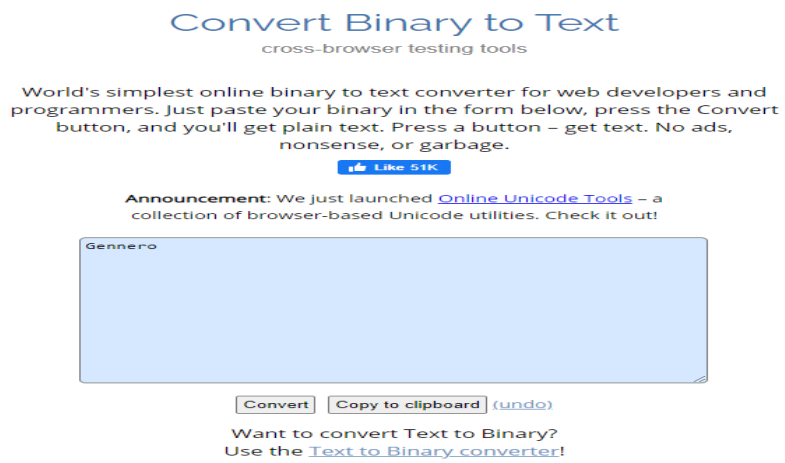
Riddle 1:

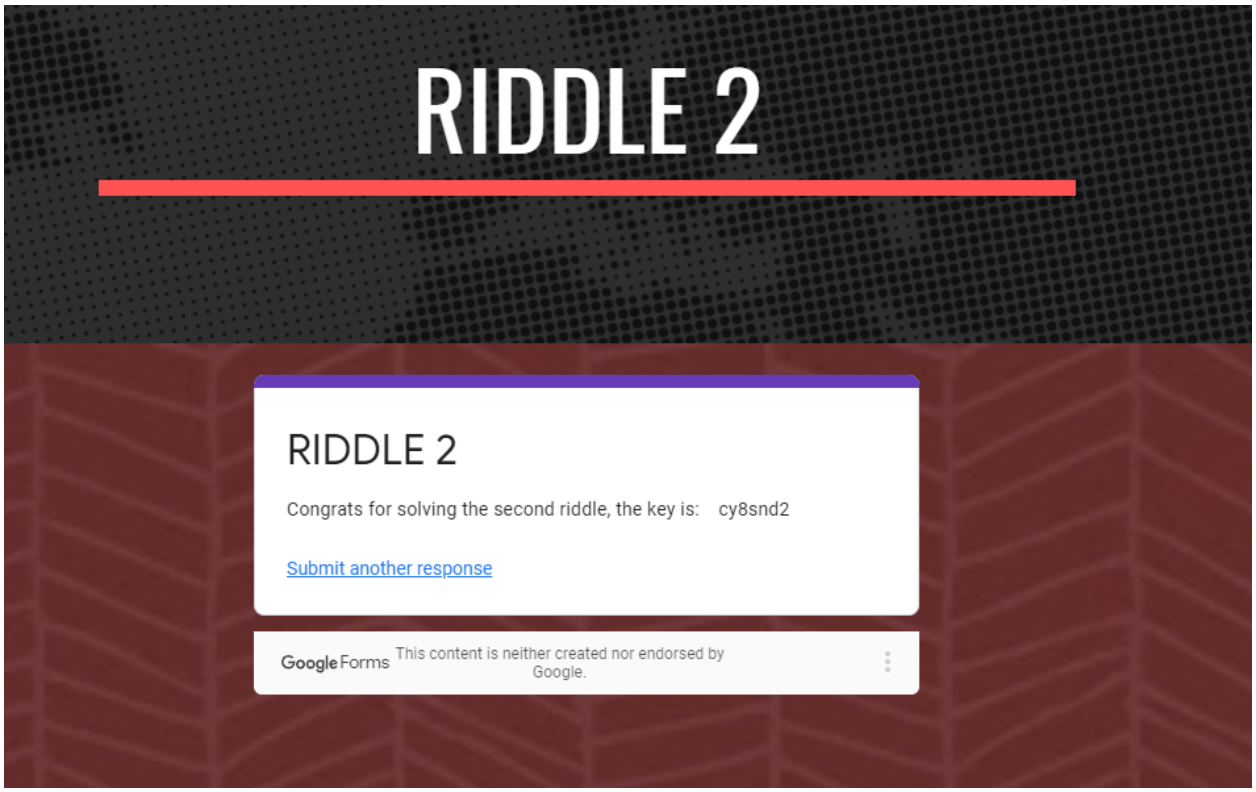
I used Caesar Cipher with a shift value of 8 I was giving (ozcjmz) after i cipher all the words my result turn out to be (gruber) after i solved my cipher, i answer the Riddle. and my riddle one key is (6skd8s).



Riddle 2:

I used Solution binary I was given: (01000111 01100101 01101110 01101110 01100101 01110010 01101111) My Output answer give me (Gennero) After getting my answer, I solved my riddle and get the Key (cy8snd2).





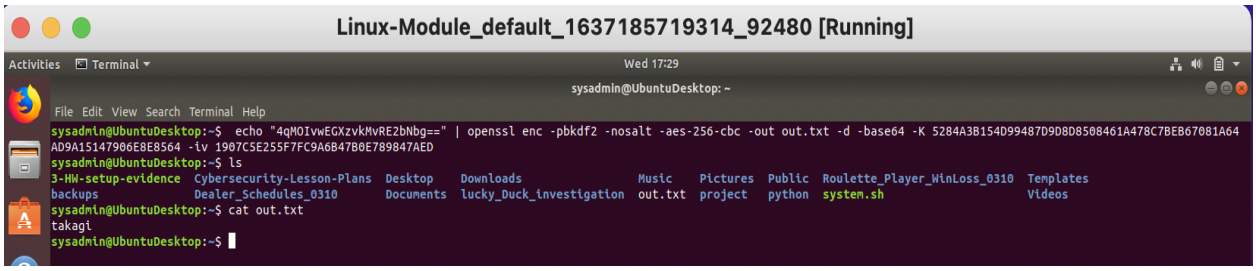
Riddle 3:

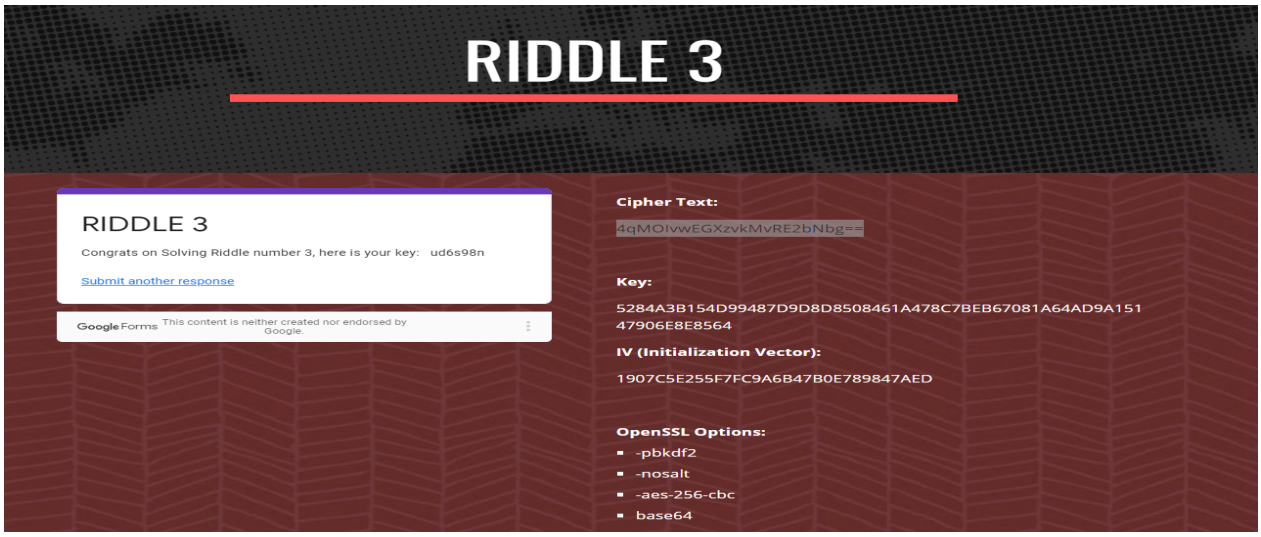
i used my ubuntu machine linux and i used this command:

echo "4qMOIvwEGXzvkMvRE2bNbg==" | openssl enc -pbkdf2 -nosalt -aes-256-cbc -out out.txt -d -base64 -K

5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED

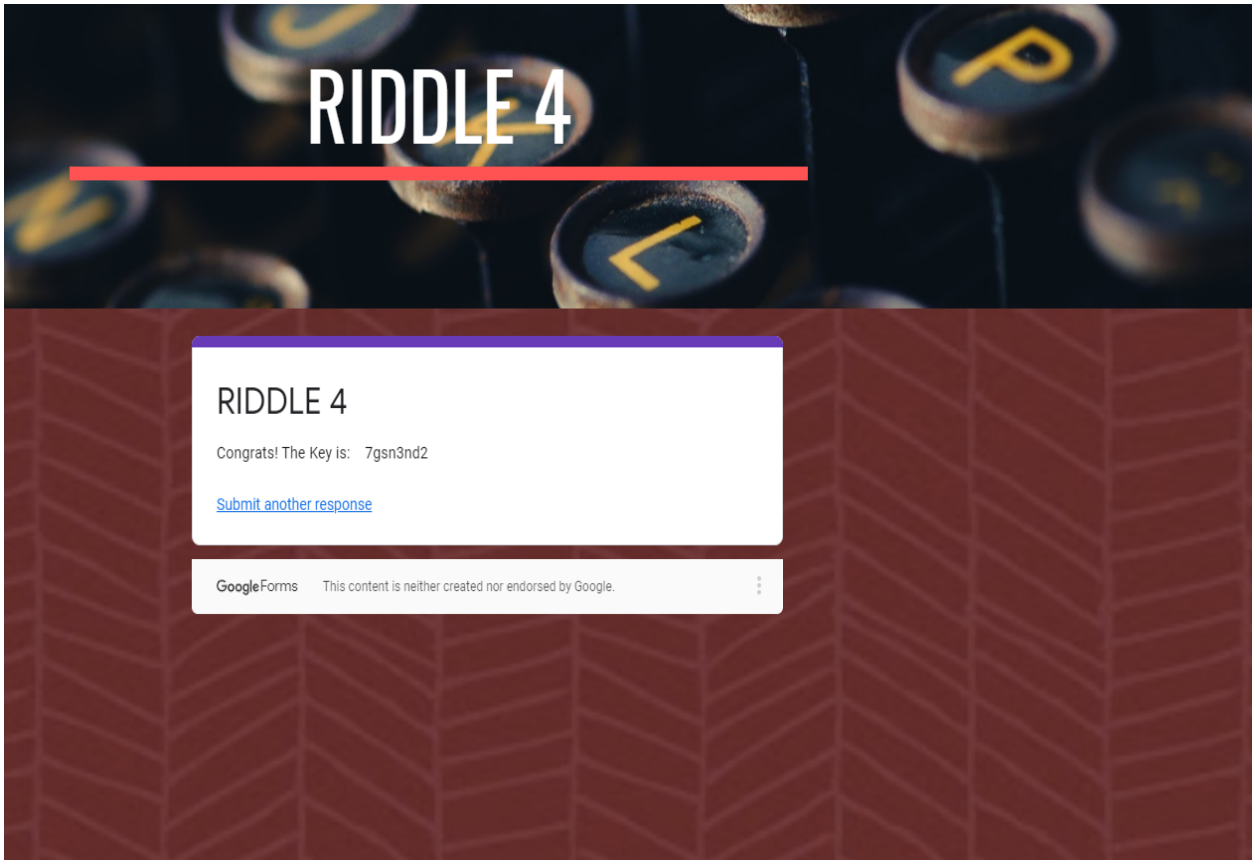
After i decipher 4qMOIvwEGXzvkMvRE2bNbg== I got my answer for my Riddle 3 (takagi) after answering the riddle, the Key was (ud6s98n)





Riddle 4.

The answer was Jill's public key Jill's private key 12 Asymmetric and 15 Symmetric Alice's public key and the key was (7gsn3nd2)



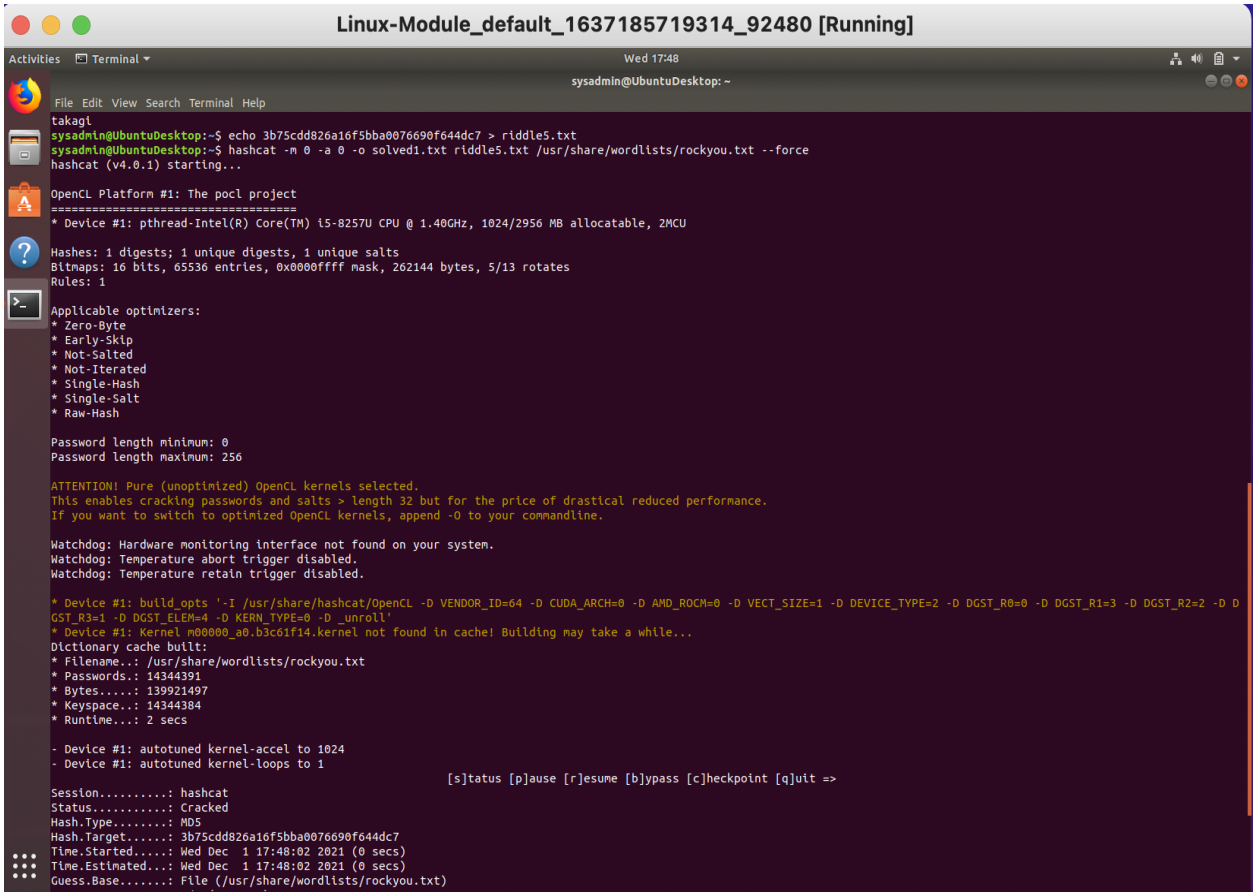
Riddle 5:

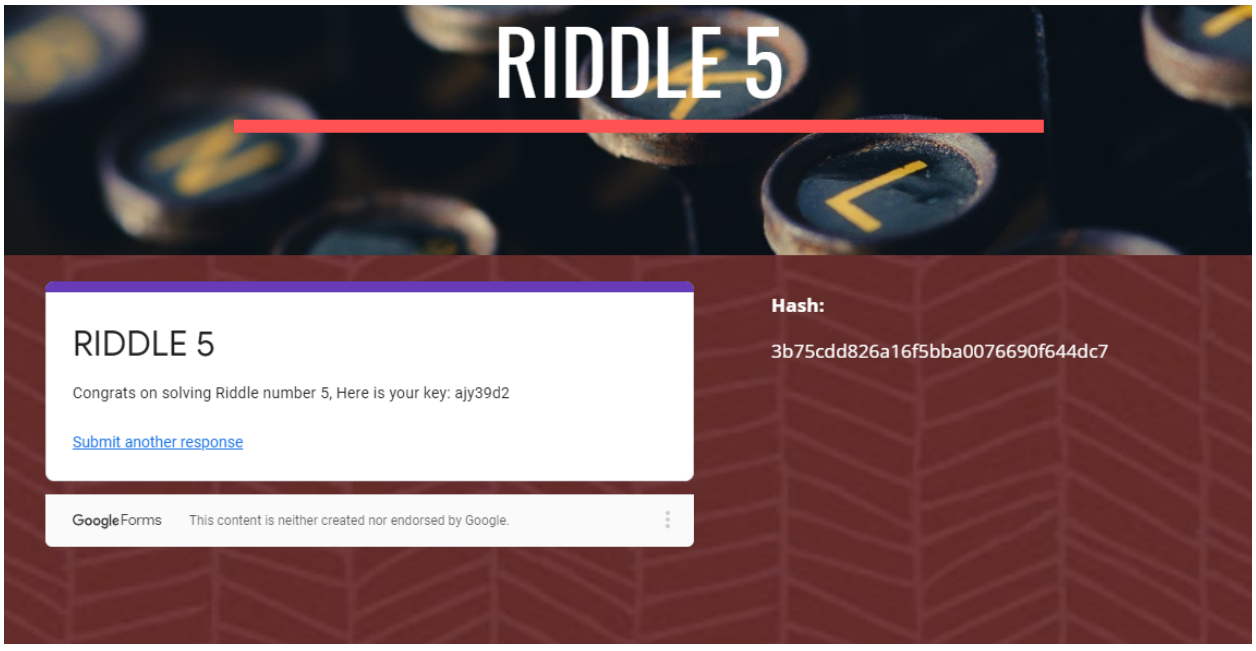
I used my ubuntu machine linux and i used this command:

echo 3b75cdd826a16f5bba0076690f644dc7 > riddle5.txt

hashcat -m 0 -a 0 -o solved1.txt riddle5.txt /usr/share/wordlists/rockyou.txt --force

The riddle gave me this hash to solve (3b75cdd826a16f5bba0076690f644dc7) after deciphering, I got my answer (argyle) and I got my Key (ajy39d2).


Linux-Module_default_1637185719314_92480 [Running]
Activities
Terminal
Wed 17:48
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
takagi
sysadmin@UbuntuDesktop:~$ echo 3b75cdd826a16f5bba0076690f644dc7 > riddle5.txt
sysadmin@UbuntuDesktop:~$ hashcat -m 0 -a 0 -o solved1.txt riddle5.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v4.0.1) starting...
OpenCL Platform #1: The pocl project
* Device #1: pthread-Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz, 1024/2956 MB allocatable, 2MCU
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
Password length minimum: 0
Password length maximum: 256
ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastical 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.
Watchdog: Temperature retain trigger disabled.
* Device #1: build_opts '-I /usr/share/hashcat/OpenCL -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=1 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D D
GST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
* Device #1: Kernel m00000_a0.b3c61f14.kernel not found in cache! Building may take a while...
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs
- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 1
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 3b75cdd826a16f5bba0076690f644dc7
Time.Started.....: Wed Dec 1 17:48:02 2021 (0 secs)
Time.Estimated...: Wed Dec 1 17:48:02 2021 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)

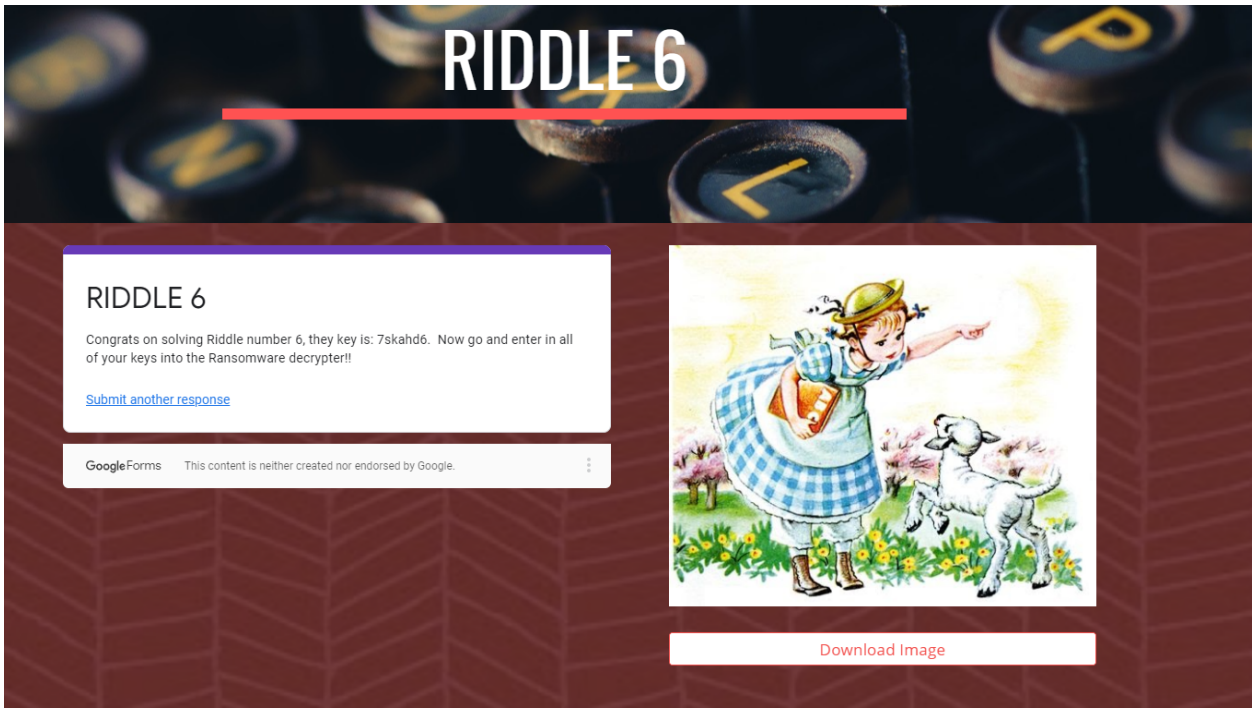

RIDDLE 5
RIDDLE 5
Congrats on solving Riddle number 5, Here is your key: ajy39d2
Submit another response
Google Forms
This content is neither created nor endorsed by Google.
Hash:
3b75cdd826a16f5bba0076690f644dc7

Riddle 6:

I also used my Ubuntu Linux machine. i used this command:

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

After I used the command, I got my riddle six answers (mcclane) and got the Key (7skahd6).



Ransom Decrypted:

After getting all six cryptographic riddles, I went back to the Decrypted header on the website and entered all six keys I solved. and here is my screenshot result.


Home
INSTRUCTIONS
RANSOMWARE DECRYPTER
KIDDLE 1
KIDDLE 2
KIDDLE 3
KIDDLE 4
KIDDLE 5
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
Google Forms
This content is neither created nor endorsed by Google.