Week 10 Homework: Cryptography Homework

Riddle #1 – Caesar Cipher

Answer: grubern. 6skd8s

```
Caesar Cipher - Shift by 8
IJKLMNOPQRSTUVWXYZABCDEFGH
ABCDEFGHIJKLMNOPQRSTUVWXYZ
gruber
```

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.

Riddle #2 – Binary to Text

Answer: Gennero. cy8snd2

Convert Binary to Text

web developer and programmer tools

World's simplest bin to text converter. Just paste binary in the form below, press Convert button, and you get plain text. Press button, get text. No ads, nonsense or garbage.

Like 51K

Announcement: We just launched Online Text Tools – a collection of browser-based text processing utilities. Check it out!

Gennero

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

Riddle #3. – openssl

Answer: takagi. ud6s98n

```
645  mkdir cryptohomework
```

```
  649  cd cryptohomework/
  650  nano cyper.txt
  651  openssl enc -pbkdf2 -nosalt -aes-256-cbc -d -in cyper.txt -base64
-K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1
907C5E255F7FC9A6B47B0E789847AED
```

```
sysadmin@UbuntuDesktop:~/cryptohomework$ openssl enc -pbkdf2 -nosalt -aes
-256-cbc -d -in cyper.txt -base64 -K 5284A3B154D99487D9D8D8508461A478C7BE
B67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED
takagi
```

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

Riddle #4a and 4b – Public and Private Keys

Answer: Jill's Public Key, Jill' Private Key, 12 Asymmetric and 15 Symmetric, Alice's Public Key 7gsn3nd2

4a

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?

4b

1)
- Jack's Public Key
- Jack's Private Key
- Jill's Public Key
- Jill's Private Key

2)
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

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? *
- 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

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

Riddle #5 – hashcat

Answer: argyle ajy39d2

```
sysadmin@UbuntuDesktop:~$ echo "3b75cdd826a16f5bba0076690f644dc7" > cryptohomewo
rk.txt
sysadmin@UbuntuDesktop:~$ cat cryptohomework.txt
3b75cdd826a16f5bba0076690f644dc7
```

```
sysadmin@UbuntuDesktop:~$ hashcat -m 0 -a 0 -o solvedcryptohmk.txt cryptohomewor
k.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v4.0.1) starting...
```

```
sysadmin@UbuntuDesktop:~$ cat solvedcryptohmk.txt
3b75cdd826a16f5bba0076690f644dc7:argyle
```

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!

Riddle #6 – Stenography

Answer: mcclane. 7skahd6

```
sysadmin@UbuntuDesktop:~/Downloads$ steghide extract -sf mary-lamb.jpg
Enter passphrase:
wrote extracted data to "code_is_inside_this_file.txt".
sysadmin@UbuntuDesktop:~/Downloads$ cat code_is_inside_this_file.txt
mcclane
```

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.

Ransomware Decrypter – Completed…