Cryptography-Challenge-Ransomware-Riddles Execution

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
Shift right didn't work
Shift Left 8 position
ozcjmz =
o=g
z=r
c=u
j=b
m=e
z=r

Encrypt txt =gruber
Key= 6skd8s

Riddle 2 =

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

01000111=G
01100101=e
01101110=n
01101110=n
01100101=e
01110010=r
01101111=o
Solution=Gennero
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.

Cipher Text: 4qMOIvwEGXzvkMvRE2bNbg==

Key: 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564

IV (Initialization Vector): 1907C5E255F7FC9A6B47B0E789847AED

OpenSSL Options:

- **-pbkdf2** : This is the command-line tool for OpenSSL, a widely-used open-source cryptographic library.
- **-nosalt** :This option indicates that no random salt should be used. A salt is typically a random value that is combined with the password before hashing to enhance security.
- **-aes-256-cbc**: This specifies the encryption algorithm and mode. AES-256-CBC uses the Advanced Encryption Standard (AES) with a 256-bit key in Cipher Block Chaining (CBC) mode.
- **Base64**:This indicates that the output should be encoded using the BASE64 encoding scheme. BASE64 is commonly used to represent binary data as text.
- **-out** : If you want to specify the output file
- **-d**: If you want to decrypt data
- **-K**: is used to specify the actual encryption key

Command

1) openssl version
   OpenSSL 3.0.11 19 Sep 2023 (Library: OpenSSL 3.0.11 19 Sep 2023)

1) echo "4qMOIvwEGXzvkMvRE2bNbg==" | openssl enc -pbkdf2 -nosalt -aes-256-cbc -out out.txt -d -base64 -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED
2) Cat out.txt

Encrypt txt= takagi
key: ud6s98n

```
┌──(ladyoscar㉿kali)-[~]
└─$ echo "4qMOIvwEGXzvkMvRE2bNbg==" | openssl enc -pbkdf2 -nosalt -aes-256-cbc -out out.txt -d -base64 -K 5284A3B154D99487D9D8D8508461A478C7BEB67081A64AD9A15
147906E8E8564 -iv 1907C5E255F7FC9A6B47B0E789847AED

┌──(ladyoscar㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  decode.sh  encode.sh  file1  flag.txt  out.txt  tmp  tor.dark.bear

┌──(ladyoscar㉿kali)-[~]
└─$ cat out.txt
takagi

┌──(ladyoscar㉿kali)-[~]
└─$
```

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

What would Jill use to decrypt Jack's message?

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

Explanation:

- Public keys are used for encryption, and anyone can use the public key to encrypt a message.
- Private keys are used for decryption, and only the owner of the private key should have access to it.

So, Jack uses Jill's public key to send an encrypted message that only Jill, with her private key, can decrypt

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

- Jack would use Jill's Public Key to encrypt the message

What would Jill use to decrypt Jack's message?

- Jill would use Jill's Private Key to decrypt Jack's message

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?

Explanation:

- Asymmetric Encryption:
  - Each participant need a unique pair of public and private keys.
  - For n participant, you would need n pairs of keys.

    1 participant = 2 Asymmetric Keys. (multiply x number or participants)

- Symmetric Encryption:
  - For each pair of participants, you need a unique symmetric key. This is because symmetric keys are shared between two parties.

  Now, imagine the participants: A,B,C,D,E,F.
- To form unique pairs for symmetric keys, you pair each person with every other person exactly once

  Participants A and B = 1 Symmetric key
  Participants C and D = 1 Symmetric key
  Participants E and F = 1 Symmetric key
  1 participant = 2 Symmetric Keys.)
  1 pair of participants = 1 Symmetric Key.
  Total keys used = 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

Tim just sent an encrypted message to one of his friends, which of the following keys did he likely use to encrypt the message

In asymmetric encryption, the sender uses the recipient's public key to encrypt the message, and the recipient uses their private key to decrypt
are private keys, and messages are not typically encrypted using the recipient's private key in asymmetric encryption

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!
Hash:
3b75cdd826a16f5bba0076690f644dc7

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 show.

Image Link:
https://drive.google.com/file/d/1m9ykscnTGzgkkVet9wmiBCYsbhzbrKR9/view

The command steghide extract -sf mary-lamb.jpg is using the Steghide tool to extract hidden data from the image file "mary-lamb.jpg." Here's a breakdown of the command:

steghide: This is the main command for the Steghide tool, which is used for steganography.

extract: This is the subcommand that tells Steghide to extract hidden data.

-sf mary-lamb.jpg: These are options and arguments:

-sf: Specifies the steganography file (the image from which you want to extract hidden data).
mary-lamb.jpg: The name of the image file from which you want to extract hidden information.
So, in summary, the command is telling Steghide to extract any hidden data from the image file "mary-lamb.jpg." If the data was embedded using Steghide, it will attempt to extract and reveal the hidden information.

If there's a passphrase associated with the embedded data, Steghide may prompt you to enter the passphrase during the extraction process.

Encrypt txt= mcclan
Key= 7skahd6

Key= ajy39d2
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!!


DECRYPTER
RANSOMWARE DECRYPTER
Congratulations! You have decrypted the Ransomware! All the Nakatomi Hospital Records are now Decrypted!
Submit another response
Google Forms
This content is neither created nor endorsed by Google.