

Workshop on

Capture The Flag CTF

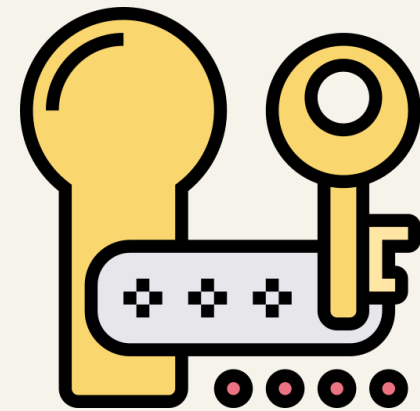
Presented By

RUET Cyber Security Club

Scan It :



On The Menu



Cryptography

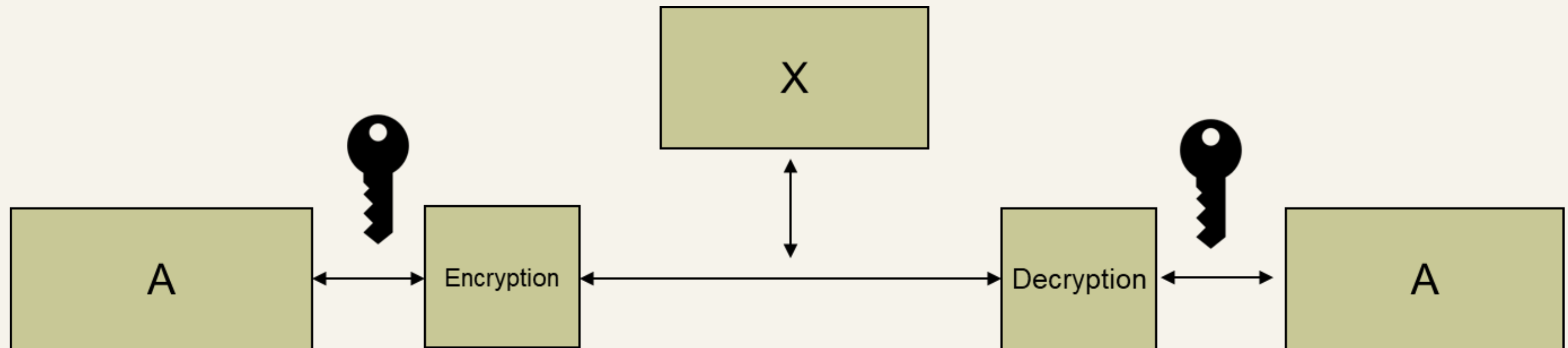


OSINT

Day 3 : 03/10/2024

Cryptography

Sending information in a way that prevents others
from reading it



Types of Cryptography



Symmetric Cryptography

Asymmetric Cryptography

Hash Function

Symmetric Cryptography

Task : MbyBumGuxyOmMnuhxNuffyl,MbyBumGuxyOmZyyfQlcnyl

GENERAL Problems : <https://cryptohack.org/challenges/general/>
(Online Cipher Identifier)

PicoCTF: <https://play.picoctf.org/practice/challenge/307?category=2&page=2>

Online tools

<https://cryptii.com>

<https://www.dcode.fr/>

Task 1:

KZLU42TDNFBFSWJTIFTUSU2BJNKFOTTQJFDTS3LDPFBG2YZSHF4WEU2CGBMTE
WLHLIZE4NTBNZSGSZCTIJEDEV2GNBRTE2DNMQZUKZ2VK5NHIWSHNBVGIV22OZ
NEQWTUJFDVE3KZGNBDMYZSIZXEYZZ5HU=====

Task 2 +3 :

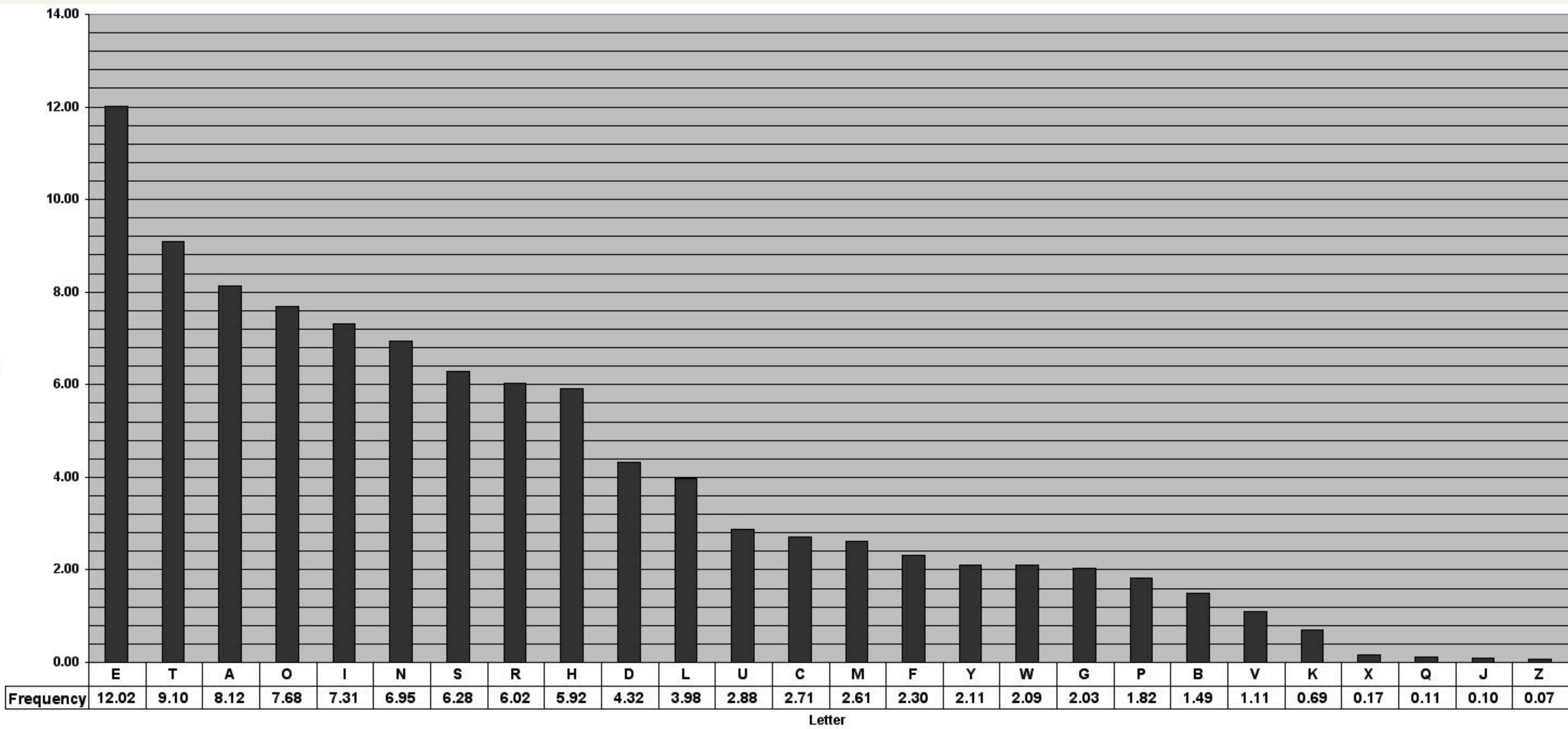
<https://play.picoctf.org/practice/challenge/418?category=2&page=1>

<https://play.picoctf.org/practice/challenge/68?category=2&difficulty=1&page=1>

Frequency Alalysis

<https://play.picoctf.org/practice/challenge/308?category=2&difficulty=2&page=1>

Frequency Alalysis Of English Letters



Frequency Analysis Online Tools

<https://www.dcode.fr/frequency-analysis>

<https://quipqiup.com>

Task 4 :

<https://play.picoctf.org/practice/challenge/309?category=2&difficulty=2&page=1>

OSINT X Cryptography

Task 5:



Drive Link:

https://drive.google.com/file/d/1u6-cJkctCvTHON_5cBK99UGdrrHD0SXB/view?usp=sharing

Hint: FileName

Task 6:



Drive Link:

https://drive.google.com/file/d/1yONznS8tCt-3x95stlyBA7_I8Hd97emG/view?usp=sharing

Symbols Cipher List

<https://www.dcode.fr/symbols-ciphers>

Hash Function

A hash function is a versatile one-way cryptographic algorithm that maps an input of any size to a unique output of a fixed length of bits.

Hash-algorithm Ex: MD5 , SHA1, SHA256 , SHA512

Test Here : <https://v2.cryptii.com/text/md5>

CyberTalents : <https://cybertalents.com/challenges/cryptography>

Task 7:

hash-identifier fd70558ca8ab8e663fd0f88e68d524cb0d208b12

John The Ripper

**Cracking Hashes - My own wordlist
- Johns wordlist**



Syntax :

```
john hash.txt --wordlist=wordlist.txt --format=Raw-Hash_Type
```

Pervious Hash : fd70558ca8ab8e663fd0f88e68d524cb0d208b12

Task 8 :

Hash: e0d00b9f337d357c6faa2f8ceae4a60d

Johns Wordlist

Wordlist Location : `/usr/share/wordlists/rockyou.txt`

```
wc -l /usr/share/wordlists/rockyou.txt
```

```
cat /usr/share/wordlists/rockyou.txt |head -n 10
```

Syntax :

```
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-hash_type
```

Task9

Can You Find My password : `baaa095eff3d03420e3bfd36302363b3`

Mask / Rules on John

Number :

```
john hash.txt --mask=?d?d?d?d?d --format=Raw-Hash_Type
```

Find my roll number : ebc11b64f9dad91128b5c586063bca28

Lower Case

```
john hash.txt --mask=?l?l?l?l?l --format=Raw-Hash_Type
```

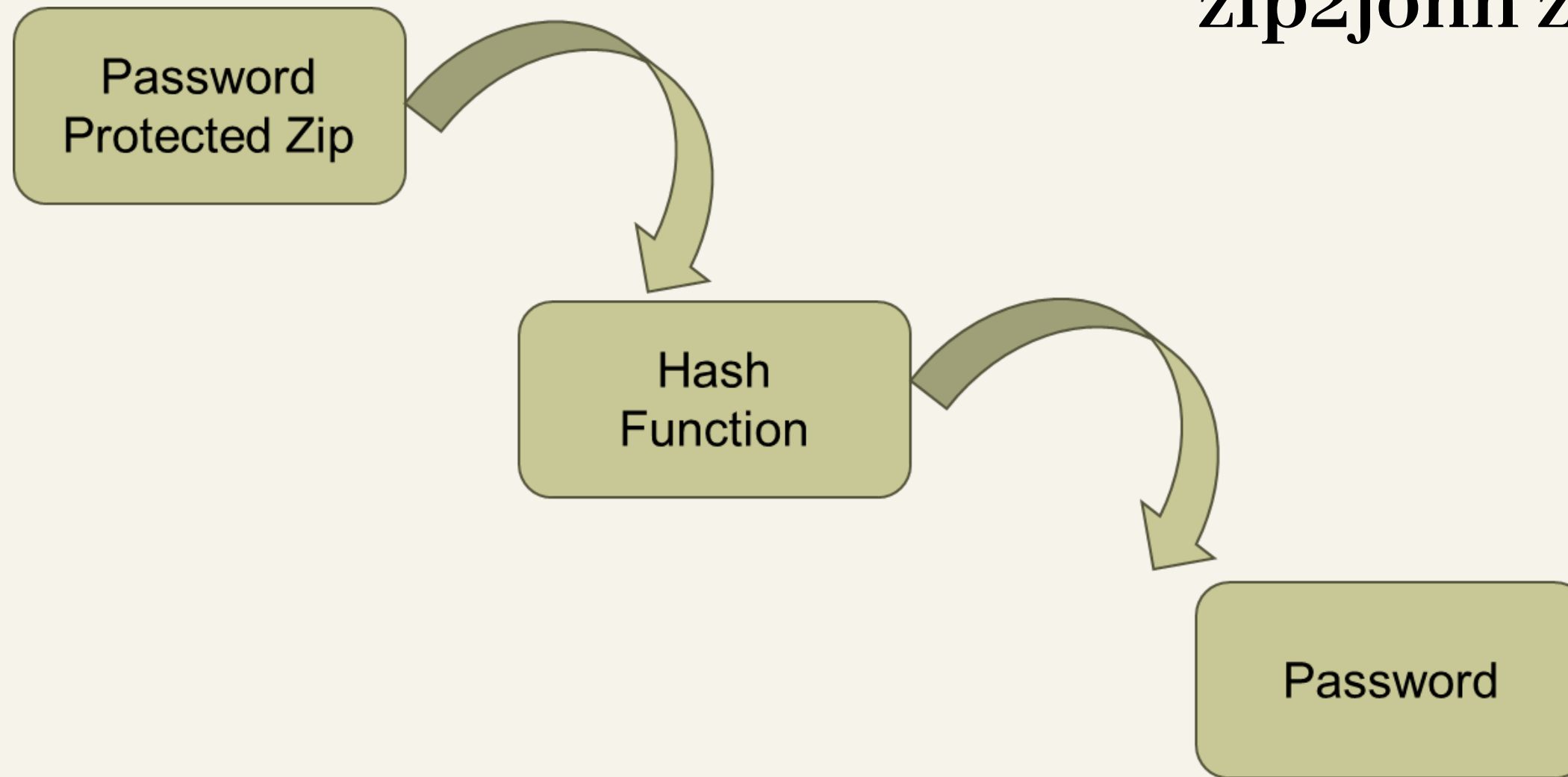
Task10

Can You Find The Key With 6 Letters In It ?(All are in same case)

Hash ad2e11e1e7f59cfcd07837f750ad87811d8b2ee9

Unzip Your Zip

`zip2john zipname.zip>hash.txt`



`john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt`

Task11 :

Zip Link :

https://drive.google.com/file/d/1F_ykQZarXj9-3rt_L4SVp3ik8j0VWYxQ/view?usp=sharing

Hashcat

Syntax :

hashcat **Attack_Mode** **Hash_Type** **Hash_path** **Wordlist_path**

Example: **hashcat -m 0 -a 0 hash.txt wordlist.txt**

Rules Link : <https://www.kali.org/tools/hashcat/>

Hashcat

Combining Two Wordsit

Password : RUETCyber

Hash: 553dba0cf058ed23c9457f639f18d97d

Examplehashcat -m 100 -a 1 hash8.txt wordlist1.txt wordlist2.txt

Hashcat

Task 12:

ee0f8cc4184386a9ea57f2ad391a9a25931db3b2

Hint: Only 2 English Letter Together :)

Asymmetric Cryptography

RSA

Rivest-Shamir-Adleman

1. Choose two large prime numbers p and q .

2. Compute $n = pq$.

3. Calculate $\varphi = (p-1) * (q-1)$.

4. Choose a value of e . [$e < \varphi$ and $\gcd(\varphi, e) = 1$]

5. Calculate $d = e^{-1} \bmod \varphi$

6. Public Key = $\{e, n\}$

7. Private Key = $\{d, n\}$

Encryption : Cipher Text , $Ct = m^e \bmod n$ [$m < n$]

Decryption : Message , $m = Ct^d \bmod n$

Message: 1234

message=1234

p=2089

q=3253

n=p*q

phi=(p-1)*(q-1)

e=113

d=pow(e,-1,phi)

cipherText=pow(message,e,n)

decrypted_Message=pow(cipherText,d,n)

print(decrypted_Message)

Inferius Prime <https://cryptohack.org/challenges/rsa/>

$n = 984994081290620368062168960884976209711107645166770780785733$

$e = 65537$

$ct = 948553474947320504624302879933619818331484350431616834086273$

<https://factordb.com>


Monoprime <https://cryptohack.org/challenges/rsa/>

$n=171731371218065444125482536302245915415603318380280392385291836472299752747934607246$
 $4775085078272840757639102649953260102512684936305019898108554184166433526311024343179$
 $000286979932248686299356572730624725446756933659309433080866342919368465058612039144$
 $49338007760990051788980485462592823446469606824421932591$

$e = 65537$

$ct=1613675503467306044514547561890289389649412803476620987987754660194633756107000748$
 $4010577687379160507009255465019048603036712101157817152575960077473989045841459385770$
 $9994072516290998135846956596662071379067305011746842247628316996977338024343628757374$
 $524136260758515864509435302781735938531030576289086798942$


Explore By Solving



CRYPTOHACK
Learn Modern
Cryptography

RSA challenges

RSA, first described in 1977, is the most famous public-key cryptosystem. It has two main use-cases

 CryptoHack



Task 13:

DESCRIPTION

Me and my friends just finished our final semester of B.Tech, so we decided to have a trip somewhere, but due to some reason, many of them were not available for the trip, but we were all ok as less is more. As the trip was about to end, one of my friends said we should try scuba diving here. I was scared of that, but my friends said, If you don't risk anything, you risk everything. Seriously, why do we have to risk our lives for half an hour? It's impossible for me, I said. But they motivated me all night, and then it was time for the dive. I screamed, Impossible is not a word in my vocabulary, and dived in. After all this, when I came back to my room, I realised I was low on money, so I called and asked my father for some help by singing something like this:

I'd be gone to my dad

And ask for some cash

I ran

All the Hustle towards the trip was worth it, as we enjoyed it a lot and made some awesome memories throughout the trip.

Flag format: RCSCWorkshop{My Name according to story_Amount I got in figures}

Author : Not Me ☒



OSINT

Task 14 :

QR == Quick Response



Flag Formet : RCSCWorkshop{}

Any Question?



Lupôn ☺