Operating Systems Lab

Momina Atif Dar
P18-0030
Section B

System Administration Lab Task 01

SCREENSHOTS:

Lecture 1

```
In [188]: #checking XOR
          bin(0b10 ^ 0b11)

Out[188]: '0b1'

In [189]: #reversing XOR
          bin(0b1 ^ 0b11)

Out[189]: '0b10'
```

In [203]:
```
msg = "The name is Sherlock Holmes and address is 221B Bakers Street."
```

In [204]:
```
for i in msg[:]:
    print(ord(i))
```

```
84
104
101
32
110
97
109
101
32
105
115
32
83
104
101
114
108
111
99
107
32
72
111
108
109
101
115
32
97
110
100
32
97
100

100
114
101
115
115
32
105
115
32
50
50
49
66
32
66
97
107
101
114
115
32
83
116
114
101
101
116
46
```

In [210]:
```
#encryption
def encrypt(msg, key):
    enc_msg = ""

    for i in msg:
        c_bin = ord(i)
        c_enc = c_bin ^ key
        c_enc = chr(c_enc)

        enc_msg += c_enc

    return enc_msg
```

In [211]:
```
key = 76
cypher_txt = encrypt(msg,key)
print(cypher_txt)
```

```
$)l"-!)l%?l$)> #/'l# !)?l-"(l-((>)??l%?l~~}l-')>?l8>))8b
```

In [213]:
```
#decryption
def decrypt(cypher_txt, key):
    dec_msg = ""

    for i in cypher_txt:
        c_bin = ord(i)
        c_dec = c_bin ^ key
        c_dec = chr(c_dec)

        dec_msg += c_dec

    return dec_msg
```

In [214]:
```
print(decrypt(cypher_txt,key))
```

```
The name is Sherlock Holmes and address is 221B Bakers Street.
```

trying to decode hidden msg with hit and try key values

In [215]:
```
key = 2
print(decrypt(cypher_txt,key))
```

```
&+n /#+n'=n&+<"!-%n!"#+=n/ *n/**<+==n'=n||n/%+<=n:<++:`
```

In [217]:
```
for i in range(55,80):
    print(decrypt(cypher_txt,i))
```

```
/[[[[   [3[[[[IIJ9[9[(  U
 TTT'T<TTTTFFE6T6T'Z
!UUU&U=UUUUGGD7U7U&[
"VVV%V>VVVVDDG4V4V%X
#WWW$W?WWWWEEF5W5W$Y
$PPP#P8PPPPBBA2P2P#^
%QQQ"Q9QQQQCC@3Q3Q"_
&RRR!R:RRRR@@C0R0R!\
'SSS S;SSSSAAB1S1S ]
Xdi,bmai,e,_di~`cog,Dc`ai,mbh,mhh~i,e,>>=N,Nmgi~,_x~iix"
Yeh-cl`h-d~-^ehabnf-Eba`h~-lci-liih~~-d~-??<O-Olfh~-^yhhy#
Zfk.`ock.g}.]fk|bame.Fabck}.o`j.ojj|k}}.g}.<<?L.Loek|}.]z|kkz
[gj/anbj/f|/\gj}c`ld/G`cbj|/nak/nkk}j||/f|/==>M/Mndj}|/\{}jj{!
\`m(fiem(a{([`mzdgkc(@gdem{(ifl(illzm{{(a{(::9J(Jicmz{([|zmm|&
]al)ghdl)`z)Zal{efjb)Afedlz)hgm)hmm{lzz)`z);;8K)Khbl{z)Z}{ll}'
^bo*dkgo*cy*Yboxfeia*Befgoy*kdn*knnxoyy*cy*88;H*Hkaoxy*Y~xoo~$
_cn+ejfn+bx+Xcnygdh`+Cdgfnx+jeo+jooynxx+bx+99:I+Ij`nyx+Xynn%
Pla$jeia$mw$Wlavhkgo$Lkhiaw$ej`$e``vaww$mw$665F$Feoavw$Wpvaap*
Qm`%kdh`%lv%Vm`wijfn%Mjih`v%dka%daaw`vv%lv%774G%Gdn`wv%Vqw``q+
Rnc&hgkc&ou&Unctjiem&Nijkcu&ghb&gbbtcuu&ou&447D&Dgmctu&Urtccr(
Sob'ifjb'nt'Tobukhdl'Ohkjbt'fic'fccubtt'nt'556E'Eflbut'Tsubbs)
The name is Sherlock Holmes and address is 221B Bakers Street.
Uid!o`ld!hr!Ridsmnbj!Inmldr!`oe!`eesdrr!hr!330C!C`jdsr!Rusddu/
Vjg"lcog"kq"Qjgpnmai"Jmnogq"clf"cffpgqq"kq"003@"@cigpq"Qvpggv,
Wkf#mbnf#jp#Pkfqol`h#Klonfp#bmg#bggqfpp#jp#112A#Abhfqp#Pwqffw-
```

FOUND IT!

Lecture 2

In [300]:
```
p = 3
q = 11
n = p * q
phi = (p-1)*(q-1)
print(n,phi)
```

```
33 20
```

In [301]:
```
def gcd(a, b):
    while b != 0:
        a, b = b, a%b
    return a
```

In [302]:
```
#co-prime
def get_e(phi):
    e = 2

    while True:
        if gcd(e,phi) == 1:
            break
        e+=1
    return e
```

In [303]:
```
def get_d(init_val = 1):
    d = init_val

    while True:
        if (e*d % phi) == 1:
            break
        d += 1
    return d
```

In [304]:
```
e = get_e(phi)
print(e)
d = get_d()
print(d)
```

```
3
7
```

In [225]:
```
#should be less than n
msg = 31
```

In [226]:
```
#encrypt
enc = msg**e % n
print(enc)
```

```
25
```

In [227]:
```
#decrypt
dec = enc**d % n
print(dec)
```

```
31
```

ADDING SIGNATURE

In [233]:
```
money = 500
```

In [234]:
```
p = 103
q = 100
n = p*q
phi = (p-1)*(q-1)
e = get_e(phi)
d = get_d()
print('n: ',n)
print('e: ',e)
print('d: ',d)
print('phi: ',phi)
```

```
n:  10300
e:  5
d:  6059
phi:  10098
```

In [239]:
```
#encryption with d so decryption with e or do encryption with e and do decryption with d

sign = money**d % n
print(sign)
```

```
8500
```

In [240]:
```
#decryption with d cuz encrypted with e or do decryption with d if encryption with e

dec = sign**e % n
print(dec)
```

```
500
```

In [289]:
```
def hash_fn(msg):
    a = 0
    for i in msg:
        a += ord(i)
    return int(a % 1e5)
```

In [290]:
```
msg2 = "I am going to return you the money I owe you."
```

In [291]:
```
hash_val = hash_fn(msg2)
print(hash_val)
```

```
4051
```

In [292]:
```
#encryption with signature i.e. hidden key
sign = hash_val**d % n
print(sign)
```

```
751
```

In [293]:
```
#made public
print(msg2,sign)
```

```
I am going to return you the money I owe you. 751
```

In [294]:
```
hash_val = hash_fn(msg2)
print(hash_val)
```

```
4051
```

In [295]:
```
#decryption with public key
dec = sign**e % n
print(dec)
```

```
4051
```

In [296]:
```
if dec == hash_val:
    print("The message is sent by right person.")
else:
    print("The message is sent by wrong person.")
```

```
The message is sent by right person.
```

In [297]:
```
#encryption with WRONG KEY
sign = hash_val**10 % n
print(sign)
hash_val = hash_fn(msg2)
print(hash_val)
#decryption with public key
dec = sign**e % n
print(dec)
```

```
7701
4051
7001
```

In [298]:
```
if dec == hash_val:
    print("The message is sent by right person.")
else:
    print("The message is sent by wrong person.")
```

```
The message is sent by wrong person.
```
