STUDENT REPORT

DETAILS

Name

ANUMALLA CHARAN RAJ

Roll Number

20R01A6602

EXPERIMENT

Title

WEEK 2

Description

Implementation of Cryptanalysis using RSA.

Procedure and Overvation:

```
┌──(kali㉿kali)-[~/Desktop/6602]
└─$ ls
enc.txt  pubkey.pem

┌──(kali㉿kali)-[~/Desktop/6602]
└─$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+SO2Emjj8Ro4lt5FdLO6WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0VyyO0zQ
owIDAQAB
-----END PUBLIC KEY-----

┌──(kali㉿kali)-[~/Desktop/6602]
└─$ openssl 6602 -pubin -inform PEM -text -noout <pubkey.pem
Invalid command '6602'; type "help" for a list.

┌──(kali㉿kali)-[~/Desktop/6602]
└─$ openssl rsa -pubin -inform PEM -text -noout <pubkey.pem
Public-Key: (576 bit)
Modulus:
    00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
    96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
    22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
    14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:
    4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
Exponent: 65537 (0x10001)

┌──(kali㉿kali)-[~/Desktop/6602]
└─$ touch pubhex.txt

┌──(kali㉿kali)-[~/Desktop/6602]
└─$ nano pubhex.txt

┌──(kali㉿kali)-[~/Desktop/6602]
```

```
└─$ touch exploit.py



┌──(kali㉿kali)-[~/Desktop/6602]

└─$ nano exploit.py



┌──(kali㉿kali)-[~/Desktop/6602]

└─$ cat exploit.py

from Crypto.PublicKey import RSA

from Crypto.Util.number import inverse

import base64

n = 188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

e = 65537

p = 39807508642406493739712550055038649119906436234252670840638518957594638895726176858331 7

q = 472772146107435302536223071973048224632914695302097116459852171130520711256363590397527

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

d = inverse(e, phi_n)

key = RSA.construct((n, e, d, p, q))

fn = "private.pem"

with open(fn, "wb") as f:

        f.write(key.exportKey())




┌──(kali㉿kali)-[~/Desktop/6602]

└─$ pip install pycrypto

Defaulting to user installation because normal site-packages is not writeable

Collecting pycrypto

  Downloading pycrypto-2.6.1.tar.gz (446 kB)

     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 446.2/446.2 kB 7.2 MB/s eta 0:00:00

  Preparing metadata (setup.py) ... done

Building wheels for collected packages: pycrypto

  Building wheel for pycrypto (setup.py) ... done

  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp310-cp310-linux_i686.whl size=531509 sha256=9aace0001179edf49ddebf93f696607c6e80e5aeee574593a1f6776f818261fd

  Stored in directory: /home/kali/.cache/pip/wheels/e8/4b/5b/b10a6fc885057b6ff9fbd5691d7e700d0a9408f80b7e6f12e0

Successfully built pycrypto

Installing collected packages: pycrypto

Successfully installed pycrypto-2.6.1



┌──(kali㉿kali)-[~/Desktop/6602]
```

```
└─$ python exploit.py


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ ls
enc.txt  exploit.py  private.pem  pubhex.txt  pubkey.pem


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ cat private.pem
-----BEGIN RSA PRIVATE KEY-----
MIIBXwIBAAJJAMLLsk/b+SO2Emjj8Ro4lt5FdLO6WHMMvWUpOIZOIiPu63BKF8/Q
jRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0VyyO0zQowIDAQABAkgyAw5Cxp1O
d95+I5exPbouUvLFeiBfWXP+1vh2MvU8+IhmCf9j+hFOK13x22JJ+Orwv1+iatW4
5It/qwUNMvxXS0RuItCLp7ECJQDM6VRX8SfElUbleEECmsavcGBMZOgoEBisu1OC
M7tX83puaJUCJQDzXLgl8AM5bxHxSaWaD+c9tDFiyzBbjr/tpcqEC+JMU2tqrlcC
JQCjGt8+GQD0o3YJVc05i4W3RBYC+RcqPJXHeFyieRcYjP/ZPnkCJQDVUULBTl8l
KuzJWcrk/metuJNJi925g6lMwHSBxoD4cm7HtkUCJFqWTOzCIODw7eoypcJYjm2O
/ohEsSjEXsg6Bh8mY3LunBaqiA==
-----END RSA PRIVATE KEY-----


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ touch dec.txt


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ openssl rsa -decrypt -in enc.txt -out dec.txt -inkey private.pem
rsa: Use -help for summary.


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ openssl rsautl -decrypt -in enc.txt -out dec.txt -inkey private.pem
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ openssl pkeyutl -decrypt -in enc.txt -out dec.txt -inkey private.pem


┌──(kali㉿kali)-[~/Desktop/6602]
└─$ cat dec.txt
RSAisEasy
```

```
┌──(kali㉿kali)-[~/Desktop/6602]
└─$


RSAisEasy
```

VIVA RESPONSES

Q) In Asymmetric-Key Cryptography, the two keys, e and d, have a special relationship to

Each other

Q) One commonly used public-key cryptography method is the --- algorithm

RSA

Q) Public key encryption is also known as

Asymmetric encryption

Q) Which command is used to display the operating system name

uname

Q) Which of the following command is used to count the total number of lines, words, and characters contained in a file?

wc