4. Demonstrate the working of ECB and CBC modes of AES on plaintext using OpenSSL.

```
touch plain.txt
gedit plain.txt
cat plain.txt

openssl enc -aes-128-cbc -e -in plain.txt -out cipher1.bin -K
00112233445566778899aabbccddeeff -iv 0102030405060708090a0b0c0d0e0f
openssl enc -aes-128-cbc -d -in cipher1.bin -out output1.txt -K
00112233445566778899aabbccddeeff -iv 0102030405060708090a0b0c0d0e0f
xxd cipher1.bin
cat output1.txt

openssl enc -aes-128-ecb -e -in plain.txt -out cipher2.bin -K
00112233445566778899aabbccddeeff
openssl enc -aes-128-ecb -d -in cipher2.bin -out output2.txt -K
00112233445566778899aabbccddeeff
xxd cipher2.bin
cat output2.txt
```

5. Demonstrate the workings of the ECB and CBC modes of AES on a bitmap image using OpenSSL.

```
openssl enc -aes-128-ecb -e -in pic_original.bmp -out pic_ecb.bmp -K
0123456789abcdeffedcba9876543210

openssl enc -aes-128-cbc -e -in pic_original.bmp -out pic_cbc.bmp -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff

head -c 54 pic_original.bmp > header

tail -c +55 pic_ecb.bmp > body_ecb
cat header body_ecb > new_ecb.bmp

tail -c +55 pic_cbc.bmp > body_cbc
cat header body_cbc > new_cbc.bmp

eog new_ecb.bmp
eog new_cbc.bmp
```

6. Demonstrate the effects of padding in AES using OpenSSL.

```
echo -n 12345 > f1.txt
echo -n 1234567890 > f2.txt
echo -n 1234567890abcdef > f3.txt

ls -l f*.txt

openssl enc -aes-128-cbc -e -in f1.txt -out f1.bin -K 0123456789abcdeffedcba9876543210 -iv
00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f1.bin -out f1_dec.txt -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f1.bin -out f1_nopad.txt -nopad -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff

openssl enc -aes-128-cbc -e -in f2.txt -out f2.bin -K 0123456789abcdeffedcba9876543210 -iv
00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f2.bin -out f2_dec.txt -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f2.bin -out f2_nopad.txt -nopad -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff

openssl enc -aes-128-cbc -e -in f3.txt -out f3.bin -K 0123456789abcdeffedcba9876543210 -iv
00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f3.bin -out f3_dec.txt -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff
openssl enc -aes-128-cbc -d -in f3.bin -out f3_nopad.txt -nopad -K
0123456789abcdeffedcba9876543210 -iv 00112233445566778899aabbccddeeff

ls -l f*.bin
xxd f1.txt
xxd f1_nopad.txt
```

7. Demonstrate the effects of error propagation in different modes of AES. Also, demonstrate the usage and effects of the initialization vector on AES.

----- 7 A-----

touch plain.txt
gedit plain.txt
ls -l plain.txt

openssl enc -aes-128-ecb -e -in plain.txt -out error_prop.bin -k
00112233445566778899aabbccddeeff

ghex error_prop.bin

openssl enc -aes-128-ecb -d -in error_prop.bin -out error_prop.txt -k
00112233445566778899aabbccddeeff

gedit error_prop.txt

openssl enc -aes-128-cbc -e -in plain.txt -out error_prop_cbc.bin -k
00112233445566778899aabbccddeeff -iv 01020304050607080 90a0b0c0d0e0f

ghex error_prop_cbc.bin

openssl enc -aes-128-cbc -d -in error_prop_cbc.bin -out error_prop_cbc.txt -k
00112233445566778899aabbccddeeff -iv 01020304050607080 90a0b0c0d0e0f

gedit error_prop_cbc.txt

--------7B--------

openssl enc -aes-128-cbc -e -in plain.txt -out cipher1.bin -k
00112233445566778899aabbccddeeff -iv 01020304050607080 90a0b0c0e0f
openssl enc -aes-128-cbc -e -in plain.txt -out cipher2.bin -k
00112233445566778899aabbccddeeff -iv 102030405060708090a0b0c0d0e0f0
xxd cipher1.bin
xxd cipher2.bin

8. Demonstrate the key generation, encryption, and decryption procedure of the RSA algorithm using OpenSSL. Also demonstrate the encryption of a secret key using an RSA keypair.

```
openssl genrsa -out key.pri 2048
cat key.pri

openssl rsa -in key.pri -noout -text

openssl rsa -in key.pri -out key.pub -pubout
cat key.pub

touch Earth.txt
gedit Earth.txt

openssl rsautl -encrypt -inkey key.pub -pubin -in Earth.txt -out Earth.enc
openssl rsautl -decrypt -inkey key.pri -in Earth.enc -out Earth.dec
cat Earth.dec

openssl rand -hex 32 > encryption.key

openssl rsautl -encrypt -inkey key.pub -pubin -in encryption.key -out encryption.key.enc
openssl rsautl -decrypt -inkey key.pri -in encryption.key.enc -out encryption.key.dec

cat encryption.key
cat encryption.key.dec
```

10. Demonstrate the usage of tcpdump to capture packets based on different filters and protocols. Also demonstrate storing and retrieving data from files.

```
tcpdump -D

sudo tcpdump -i any
Ctrl + C

sudo tcpdump -i any -w capture.pcap
Ctrl + C

# open new terminal
ping google.com
Ctrl + C

# back to first terminal
sudo tcpdump -i any tcp
Ctrl + C

sudo tcpdump -i any icmp
Ctrl + C

sudo tcpdump -i any port 80
Ctrl + C

sudo tcpdump -n -i any 'tcp[tcpflags] & tcp-syn != 0'
Ctrl + C

sudo tcpdump -n -i any 'tcp[tcpflags] & tcp-syn != 0' -w tcpsyn.pcap
Ctrl + C

sudo tcpdump -n -i any 'tcp[tcpflags] & tcp-ack != 0'
Ctrl + C

sudo tcpdump -n -i any 'tcp[tcpflags] & (tcp-syn|tcp-ack) != 0'
Ctrl + C

sudo tcpdump -n -i any 'tcp[tcpflags] & tcp-fin != 0' -w tcpfin.pcap
Ctrl + C

sudo tcpdump -r capture.pcap

sudo tcpdump -A -r capture.pcap

sudo tcpdump -xx -r capture.pcap

sudo tcpdump -xx -r tcpsyn.pcap

sudo tcpdump -xx -r tcpfin.pcap
```