Q1 Let's assume that someone does triple encryption by using EEE with CBC on the inside. Suppose an attacker modfies bit x of ciphertext block n. How does this affect the decrypted plaintext?

Q2 From the Reading List, read "What's wrong with WEP?" and write a half a page executive summary explaining how to break into a wireless LAN that is secured with WEP. (This type of exercise is very useful, as you will be writing memos and how-to documents frequently during your IT career.)

Programming Problem To be implement in Python (2.7). First install the Python cryptographic library:

```
pycrypto 2.6.1
```

It can be downloaded from

```
https://pypi.python.org/pypi/pycrypto
```

Now consider the following example, shown in the Python interactive mode. This example is an application of DES in ECB mode to a plaintext that is exactly 8 characters long.

```
>>> from Crypto.Cipher import DES
>>> obj=DES.new('amalgams', DES.MODE_ECB)
>>> plaintext="8 chars."
>>> ciphertext=obj.encrypt(plaintext)
>>> ciphertext
'(\xdc\xa5|\x025\xaa\\'
>>> obj.decrypt(ciphertext)
'8 chars.'
```

Your assignment is to implement CBC on a plaintext of arbitrary length; your program should be called as follows:

```
python des-cbc key plaintext.txt
```

and it should output `ciphertext.txt` using DES in ECB as a building block to implement DES in CBC. Essentially you need to loop over the characters in `plaintext.txt` in groups of 8 characters at a time, applying a modification of the above snippet each time.

Propose a solution for the case that the length of plaintext is not divisble by 8.