1. You are encouraged to work in groups of two or three. If you cannot find partners, you may work alone.
2. Please submit **one** copy of the assignment using `subversion`; if you are working with a partner, both names should appear on the assignment.
3. Note that you will get a grade of zero if your program does not run.

Write a Python program that implements DES, the "Data Encryption Standard," following the description of DES in section 3.3 in the textbook.

Note that the S-boxes given in figures 3-9 to 3-16 can also be found on the web, so you do not have to copy them by hand; but make sure that your source is correct!

Your program should work as follows:

```
> des.py
> Enter 64-bit string (plaintext):
> Enter 56-bit string (key):
```

and it should output a 64-bit string, which is the DES ciphertext obtained from the plaintext and the key.

Make sure that you test your program before you submit it. Also note that you are not required to do *Cipher-Block Chaining (CBC) mode*; only encrypt one block of 64 bits, which is called *Electronic-Code Book (ECB) mode*.

To test your program, you may use OpenSSL, which has an implementation of DES in ECB mode. Create a file of 64 bits, for example by using the command (in UNIX):

```
echo -n '12345678' > plaintext.txt
```

and now you can compute the DES encoding of this file with the command:

```
openssl des-ecb -base64 -nosalt -nopad -K 0 -iv 2011 -in plaintext.txt
```

to which the output (in `Base64`) is `Yt2OSmFOGvk=`. To see the binary output omit `-base64` in the above command, but you should "pipe" it to `xxd -b`, i.e.,

```
openssl des-ecb -nosalt -nopad -K 0 -iv 2011 -in hello.txt | xxd -b
```

and the output is

```
0000000: 01100010 11011101 10001110 01001010 01100001 01001110  b..JaN
0000006: 00011010 11111001
```

which gives you the bits.

Note that the switch `-iv 2011` is superfluous, as we are not doing CBC, but it is required by the command (if you change the values of the switch, the output remains the same). The `-K 0` switch is the key, which is assumed to be a number in hexadecimal, in this case it is just 0 (zero).

Please include a text write up of your program. That is, write a short report (a few paragraphs, included as a comment at the beginning of your code) describing how you solved the problem, how was your program tested, any problems you encountered, and a sample run of the program (and an output dump of the sample run). The intention is to have a basic "manual" for your program.