Q1 Finish reading chapter 3 in the textbook; answer the following question: "Why is each DES semi-weak key the inverse of another semi-weak key?" (Problem 9 on page 94 of the textbook.)

Q2 Read the following article from the reading list: *The State of Phishing Attacks*, by Jason Hong, and write a summary — one page long max!

Programming Problem Implement in Python (2.7) a password breaker for the function `crypt()`. The assumption is that the password is a dictionary word, so you have to write a Python script that checks all the words in a dictionary file until it finds the one with a given `crypt()` hash.

There are many free dictionaries out there, i.e., word lists given as text files. If you have a Mac OS X, or most UNIXes for that matter, there is a dictionary file in `/usr/share/dict/words` . It works for this assignment.

In order to implement `crypt()` in Python use this type of code:

```
import crypt
print crypt.crypt(password, salt)
```

Your program should be invoked as follows:

```
python breakcrypt.py saltedhash
```

and it should output the corresponding password. For example, on input

```
python breakcrypt.py 3zJVde6E76qRo
```

it should output `acorn` which is the corresponding dictionary password. Note that the salt in the salted hash is always the first two characters, `3z` in this case.

As part of this programming assignment you should break the following `crypt()` salted hash:

```
eYSv7jHPDWf/A
```

that is, provide the corresponding password (a.k.a., clear word).