Sean Gordon

CprE 431

Module 2 Lab

(a) Using Cygwin command prompt, enter the following command:

```
$ md5sum dont_smoke_hash_it_can_md5_you.txt
d6192fc25d86eeecb9b4e8a54da0fdd2 *dont_smoke_hash_it_can_md5_you.txt
```

The hash key (D6192FC25D86EEECB9B4E8A54DA0FDD2) can then be used to open the zip file.

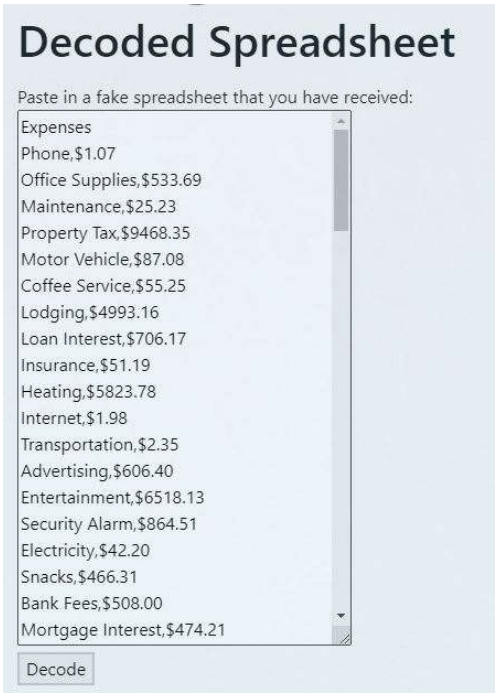
(b) The last (most secure and more commonly used) algorithm was the correct one, outputting a text file with the secret message decoded inside.

```
$ openssl des -d -salt -in funny_jokes.txt -out jokes_decrypted.txt
enter des-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
34359738384:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:crypto/e
vp/evp_enc.c:583:

Sean@GamingPC /cygdrive/c/Users/Sean/Documents/-=-   School    -=-/7th_Semester/CprE_431/Labs
/Module 2 Lab/For Windows Users_ dont_smoke_hash_it_can_md5_you.zip/dont_smoke_hash_it_can_md
5_you
$ openssl des3 -d -salt -in funny_jokes.txt -out jokes_decrypted.txt
enter des-ede3-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
34359738384:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:crypto/e
vp/evp_enc.c:583:

Sean@GamingPC /cygdrive/c/Users/Sean/Documents/-=-   School    -=-/7th_Semester/CprE_431/Labs
/Module 2 Lab/For Windows Users_ dont_smoke_hash_it_can_md5_you.zip/dont_smoke_hash_it_can_md
5_you
$ openssl aes128 -d -salt -in funny_jokes.txt -out jokes_decrypted.txt
enter aes-128-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
34359738384:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:crypto/e
vp/evp_enc.c:583:

Sean@GamingPC /cygdrive/c/Users/Sean/Documents/-=-   School    -=-/7th_Semester/CprE_431/Labs
/Module 2 Lab/For Windows Users_ dont_smoke_hash_it_can_md5_you.zip/dont_smoke_hash_it_can_md
5_you
$ openssl aes192 -d -salt -in funny_jokes.txt -out jokes_decrypted.txt
enter aes-192-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
34359738384:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:crypto/e
vp/evp_enc.c:583:

Sean@GamingPC /cygdrive/c/Users/Sean/Documents/-=-   School    -=-/7th_Semester/CprE_431/Labs
/Module 2 Lab/For Windows Users_ dont_smoke_hash_it_can_md5_you.zip/dont_smoke_hash_it_can_md
5_you
$ openssl aes256 -d -salt -in funny_jokes.txt -out jokes_decrypted.txt
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

(c) Using the instructions found within the decoded message, I went to www.spammimic.com and used their spreadsheet decoder to find the message hidden within the excel file.

my_funny_expenses.csv

```
Expenses
Phone,$1.07
Office Supplies,$533.69
Maintenance,$25.23
Property Tax,$9468.35
Motor Vehicle,$87.08
Coffee Service,$55.25
Lodging,$4993.16
Loan Interest,$706.17
Insurance,$51.19
Heating,$5823.78
Internet,$1.98
Transportation,$2.35
Advertising,$606.40
Entertainment,$6518.13
Security Alarm,$864.51
Electricity,$42.20
Snacks,$466.31
Bank Fees,$508.00
Mortgage Interest,$474.21
Gas,$3490.98
Depreciation,$74.71
Meals,$38.98
Cooling,$66.11
Software Licenses,$25.38
Entertainment,$56.57
Coffee Service,$61.73
Property Tax,$861.40
```



(d) Using the instructions decoded from the excel file, I went to https://www.mobilefish.com/services/steganography/steganography.php and inserted the attached photograph and, with the bank account number as the password, decoded the image.

P.S. If I paid a guy to covertly leak iPhone design files and that jpeg is what I got in return, I think I would break cover and stab him lol.