

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/evp/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/evp/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/evp/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/evp/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.



1	Expenses
2	Phone, \$1.07
3	Office Supplies, \$533.69
4	Maintenance, \$25.23
5	Property Tax, \$9468.35
6	Motor Vehicle, \$87.08
7	Coffee Service, \$55.25
8	Lodging, \$4993.16
9	Loan Interest, \$706.17
10	Insurance, \$51.19
11	Heating, \$5823.78
12	Internet, \$1.98
13	Transportation, \$2.35
14	Advertising, \$606.40
15	Entertainment, \$6518.13
16	Security Alarm, \$864.51
17	Electricity, \$42.20
18	Snacks, \$466.31
19	Bank Fees, \$508.00
20	Mortgage Interest, \$474.21
21	Gas, \$3490.98
22	Depreciation, \$74.71
23	Meals, \$38.98
24	Cooling, \$66.11
25	Software Licenses, \$25.38
26	Entertainment, \$56.57
27	Coffee Service, \$61.73
28	Property Tax, \$861.40

Decoded Spreadsheet

Paste in a fake spreadsheet that you have received:

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

Decode

Decoded Spreadsheet

Your spreadsheet **Expenses Phone, \$1.07 Office Supplies, \$...** decodes to:

Bank account: 112233445500. Use "https://w

Encode

Copyright © 2000-2020 spammimic.com. All rights reserved

(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.

Decrypt: Unhide secret message or secret file from an encrypted image:

Upload encrypted image
Only *.png files
(Max 4 MB) *:

Choose File

funny_image.png

-- Or --

Enter image URL
Only *.png files
(Max 4 MB) *:

Enter password:

.....

To prevent automated submissions an Access Code has been implemented for this tool.

XTb

Please enter the Access Code as displayed above*:
* = required

XTb

Decrypt

Clear

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.