***CPRE 431***

***Module 2 Lab***

**Assignments will be submitted in PDF format via Canvas.**

Please submit your homework online through Canvas. Late homework will not be accepted.

Important: Your submission must be in .pdf format ONLY!

1. You are the security administrator in the XYZ company, and you noticed some strange traffic on the network of one of the employees sending an encrypted file to someone outside of the company. You want to check if the content doesn’t have any confidential data. The encrypted file is attached with the homework (dont\_smoke\_hash\_it\_can\_md5\_you.zip). From the file name, you guessed that the password could be the md5 hash of the file name with the extension.
   1. Explain with screenshots how to use OpenSSL tool to determine the md5 hash, then use any file decompression tool (WinRAR, Winzip, etc.) to decrypt contents of the attached file. Hint: write the file name in a text file then get the hash for this text file. Note that hash is space sensitive.

*We write the name of the file ‘don’t\_smoke\_hash\_it\_can\_md5\_you.zip’ to notepad. Then hash this text file using ‘md5sum’ to hash. The hash is the password*

*A screenshot of a computer

Description automatically generated*

*A screen shot of a computer

Description automatically generated*

A screenshot of a computer screen

Description automatically generated

* 1. After decryption, you noticed that the content of the attached file was an excel sheet “my\_funny\_expenses.csv”, an image “funny\_image.png” and a text file “funny\_jokes.txt”. This could look normal, however there is a lot of secrets and hidden messages in the content. Depending on your cryptanalysis skills, you started with the text file and you noticed that it only contained random characters but it started with the word “Salted\_\_”. From your experience with OpenSSL tool, this means that this text file is encrypted using Symmetric Cipher (des, des3, aes128, aes192, aes256, etc.). Also, you noticed that all the three files have the word “funny” in their name, maybe this could be the encryption key. Explain with screenshots how to use OpenSSL tool to decrypt the original message in the text file.

*Using openSSL, we can decrypt a text file. Taking our example, we use;*

***openssl enc -d -aes-256-cbc -in funny\_jokes.txt -out decrypted\_jokes.txt -k funny***

*openssl enc: encryption/decryption*

*-d: decryption*

*-aes-256-cbc: encryption algorithm used*

*-in funny\_jokes.txt: input encrypted file*

*-out decrypted\_jokes.txt: decrypted output file*

*-k funny: encryption key*

* 1. The decrypted message of part (a) will contain the instructions for this question. Explain with screenshots how did you solve this secret and get the new key.

*On analysis, we can guess that the password must be ‘funny’, using OpenSSL we can try to decrypt the funny\_jokes.txt file. Now, we must guess what symmetric algorithm it uses and try each one.   
Finally, we find that ‘aes-256-cbc’ gives us sensible data.*

*The decrypted text file gives instructions of decrypting a CSV file called my\_funny\_expenses.csv.*

*A close up of white text

Description automatically generated*

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

* 1. The decrypted message of part (b) will contain the instructions for this question. Explain with screenshots how did you solve this secret and get the final leaked confidential information. Use the file on Canvas instead of the website given from the previous step to complete the final deliverable of the lab.

*Using the decrypted instructions on decrypted\_jokes.txt output file, we open the csv file in notepad and copy its contents and paste it the spammic.com website. Once that is decrypted, we get another message. For readability, we copy this to another txt file. Using the bank account number as password, we use a stenography tool, or in this case the zip file given on Canvas, extract it (password is the account number). Finally we get an image of a supposedly leaked iPhone dimensions.*

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a phone

Description automatically generated

A screen shot of a cell phone

Description automatically generated