# Lab 2: Symmetric Key and Hashing

You will be allocated an instance of the Cloud. It is recommended that you use Linux Kali for the following, but you can also use the Windows version of Openssl (http://asecuritysite.com/openssl.zip).

## 1 Private Key

Demo: https://youtu.be/3n2TMpHqE18 (skip past the Diffie-Hellman part, as that will be covered in another unit).

| No | Description | Result |
|---|---|---|
| **1** | Use:<br><br>`openssl list-cipher-commands`<br><br>`openssl version` | Outline five encryption methods that are supported:<br><br>Outline the version of OpenSSL: |
| **2** | Using openssl and the command in the form:<br><br>`openssl prime –hex 1111` | Check if the following are prime numbers:<br><br>42 [Yes][No]<br>1421 [Yes][No] |
| **2** | Now create a file named myfile.txt (either use Notepad or another editor).<br><br>Next encrypt with aes-256-cbc<br><br>`openssl enc -aes-256-cbc -in myfile.txt -out encrypted.bin`<br><br>and enter your password. | Use the following command to view the output file:<br><br>`cat encrypted.bin`<br><br>Is it easy to write out or transmit the output: [Yes][No] |
| **3** | Now repeat the previous command and add the –base64 option. | Use following command to view the output file: |

| | | |
|---|---|---|
| | `openssl enc -aes-256-cbc -in myfile.txt -out encrypted.bin -base64` | `cat encrypted.bin`<br><br>Is it easy to write out or transmit the output: [Yes][No] |
| **4** | Now Repeat the previous command and observe the encrypted output.<br><br>`openssl enc -aes-256-cbc -in myfile.txt -out encrypted.bin -base64` | Has the output changed? [Yes][No]<br><br>Why has it changed? |
| **5** | Now let's decrypt the encrypted file with the correct format:<br><br>`openssl enc -d -aes-256-cbc -in encrypted.bin -pass pass:napier -base64` | Has the output been decrypted correctly?<br><br>What happens when you use the wrong password? |
| **6** | If you are working in the lab, now give you private key to your neighbour, and get them to encrypt a secret message for you. | Did you manage to decrypt their message? [Yes][No] |
| **7** | Now encrypt a file with Blowfish and see if you can decrypt it. | Did you manage to decrypt the file? [Yes][No] |
| **8** | Now encrypt a file with 3DES and see if you can decrypt it. | Did you manage to decrypt the file? [Yes][No] |
| **9** | Now encrypt a file with RC2 and see if you can decrypt it. | Did you manage to decrypt the file? [Yes][No] |

.

# 2 Hashing

The hashcat version has a time-out, so enter the following command:

date -s "1 OCT 2015 18:00:00"

Demo: http://youtu.be/Xvbk2nSzEPk

| No | Description | Result |
|---|---|---|
| **1** | Using (either on your Windows desktop or on Kali):<br><br>`http://asecuritysite.com/encryption/md5`<br><br>Match the hash signatures with their words ("Falkirk", "Edinburgh", "Glasgow" and "Stirling").<br><br>`03CF54D8CE19777B12732B8C50B3B66F`<br>`D586293D554981ED611AB7B01316D2D5`<br>`48E935332AADEC763F2C82CDB4601A25`<br>`EE19033300A54DF2FA41DB9881B4B723` | `03CF5:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`D5862:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`48E93:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`EE190:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]? |
| **2** | Repeat Part 1, but now use openssl, such as:<br><br>echo -n 'Falkirk' \| openssl md5 | `03CF5:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`D5862:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`48E93:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]?<br><br>`EE190:` Is it [Falkirk][Edinburgh][Glasgow][Stirling]? |
| **3** | Using (either on your Windows desktop or on Kali):<br><br>`http://asecuritysite.com/encryption/md5`<br>Determine the number of hex characters in the following hash signatures. | MD5 hex chars:<br><br>SHA-1 hex chars:<br><br>SHA-256 hex chars: |

| | | |
|---|---|---|
| | | SHA-384 hex chars:<br><br>SHA-512 hex chars:<br><br>How does the number of hex characters relate to the length of the hash signature: |
| | | |
| **3** | From your Windows desktop or Kali, for the following /etc/shadow file, determine the matching password:<br><br>`bill:$apr1$waZS/8Tm$jDZmiZBct/c2hysERcZ3m1`<br>`mike:$apr1$mKfrJquI$KxOCL9krmqhCuOSHKqp5Q0`<br>`fred:$apr1$Jbe/hCIb$/k3A4kjpJyC06BUUaPRKs0`<br>`ian:$apr1$OGyPhsLi$jTTzWOHNS4Cl5ZEoyFLjB.`<br>`jane: $1$rqOIRBBN$R2pOQH9egTTVN1Nlst2U7.` | The passwords are password, napier, inkwell and Ankle123.<br>[Hint: openssl passwd -apr1 -salt ZaZS/8TF napier]<br><br>Bill's password:<br><br>Mike's password:<br><br>Fred's password:<br><br>Ian's password:<br><br>Jane's password: |
| **4** | From your Windows desktop or Kali, download the following:<br><br>`http://asecuritysite.com/files02.zip`<br><br>and the files should have the following MD5 signatures:<br><br>`MD5(1.txt)= 5d41402abc4b2a76b9719d911017c592`<br>`MD5(2.txt)= 69faab6268350295550de7d587bc323d`<br>`MD5(3.txt)= fea0f1f6fede90bd0a925b4194deac11`<br>`MD5(4.txt)= d89b56f81cd7b82856231e662429bcf2` | Which file(s) have been modified: |

| | | |
|---|---|---|
| **5** | From your Windows desktop or Kali, download the following ZIP file:<br><br>`http://asecuritysite.com/letters.zip`<br><br>View the Postscript files using:<br><br>`http://view.samurajdata.se/` | Outline what the letters contain:<br><br>Now determine the MD5 signature for them. What can you observe from the result? |
| **6** | Select either Windows or Kali for this part:<br><br>On Kali, download the following ZIP file and run the two programs, and run them in a command console:<br><br>`http://asecuritysite.com/files01u.zip`<br><br>**Or** on Windows, download the following ZIP file and run the two programs, and run them in a command console:<br><br>`http://asecuritysite.com/files01.zip` | What do the programs do?<br><br>Now determine the MD5 signature for them. What can you observe from the result? |

# 3 Hash Cracking (MD5)

| No | Description | Result |
|---|---|---|
| **1** | On Kali, next create a words file (**words**) with the words of "napier", "password" "Ankle123" and "inkwell"<br><br>Using hashcat crack the following MD5 signatures (hash1):<br>`232DD5D7274E0D662F36C575A3BD634C`<br>`5F4DCC3B5AA765D61D8327DEB882CF99`<br>`6D5875265D1979BDAD1C8A8F383C5FF5`<br>`04013F78ACCFEC9B673005FC6F20698D`<br>Command used: `hashcat -m 0 hash1 words` | `232DD...634C` Is it [napier][password][Ankle123][inkwell]?<br><br>`5F4DC...CF99` Is it [napier][password][Ankle123][inkwell]?<br><br>`6D587...5FF5` Is it [napier][password][Ankle123][inkwell]?<br><br>`04013...698D` Is it [napier][password][Ankle123][inkwell]? |

| | | |
|---|---|---|
| **2** | Using the method used in the first part of this tutorial, find crack the following for names of fruits (the fruits are all in lowercase):<br><br>FE01D67A002DFA0F3AC084298142ECCD<br>1F3870BE274F6C49B3E31A0C6728957F<br>72B302BF297A228A75730123EFEF7C41<br>8893DC16B1B2534BAB7B03727145A2BB<br>889560D93572D538078CE1578567B91A | FE01D:<br><br>1F387:<br><br>72B30:<br><br>8893D:<br><br>88956: |

# 4 Hashing Cracking (LM Hash/Windows)

All of the passwords in this section are in lowercase.

| No | Description | Result |
|---|---|---|
| **1** | On Kali, and using John the Ripper, and using a word list with the names of fruits, crack the following pwdump passwords:<br><br>fred:500:E79E56A8E5C6F8FEAAD3B435B51404EE:5EBE7DFA074DA8EE8AEF1FAA2BBDE876:::<br>bert:501:10EAF413723CBB15AAD3B435B51404EE:CA8E025E9893E8CE3D2CBF847FC56814::: | Fred:<br>Bert: |
| **2** | On Kali, and using John the Ripper, the following pwdump passwords (they are names of major Scottish cities/towns):<br><br>Admin:500:629E2BA1C0338CE0AAD3B435B51404EE:9408CB400B20ABA3DFEC054D2B6EE5A1:::<br>fred:501:33E58ABB4D723E5EE72C57EF50F76A05:4DFC4E7AA65D71FD4E06D061871C05F2:::<br>bert:502:BC2B6A869601E4D9AAD3B435B51404EE:2D8947D98F0B09A88DC9FCD6E546A711::: | Admin:<br>Fred:<br>Bert: |
| **3** | On Kali, and using John the Ripper, crack the following pwdump passwords (they are the names of animals):<br><br>fred:500:5A8BB08EFF0D416AAAD3B435B51404EE:85A2ED1CA59D0479B1E3406972AB1928:::<br>bert:501:C6E4266FEBEBD6A8AAD3B435B51404EE:0B9957E8BED733E0350C703AC1CDA822:::<br>admin:502::333CB006680FAF0A417EAF50CFAC29C3:D2EDBC29463C40E76297119421D2A707::: | Fred:<br>Bert:<br>Admin: |

Repeat all 4.1, 4.2 and 4.3 using **Ophcrack**, and the rainbow table contained on the instance (rainbow_tables_xp_free).