**Exercise 1**

**download**

**extract**

**powershell, cd to the folder location of hashcat**

**Task 1**

.\hashcat -a 3 -m 100 8807496363c5346684cba0d9101be93744a27652 ?d?d?d?d?d?d?d?d

.\hashcat -a 3 -m 100 e4099db8f15134974e750c132ede21bb7dcf7052 ?l?l?l?l?l?l?l?l

.\hashcat -a 3 -m 100 20d75f2aa30ae7101504d95bdda40ce235bb258c ?u?l?l?l?l?l?l?d

**Task 2**

.\hashcat -a 0 -m 100 -r rules\best64.rule b5a0a46442a34a244f6ad69dcaa7353c99623eee (location+)rockyou.txt

**Task 3**

**hashes 复制到txt里保存**

.\hashcat -a 0 -m 100 location+FileName.txt (location+)rockyou.txt

**Task 4**

.\hashcat -a 0 -m 100 -r rules\best64.rule (location+)FileName.txt (location+)rockyou.txt --potfile-disable

**Task 5**

**hashes 复制到新的txt里保存**

.\hashcat -a 0 -m 110 (location+)newFileName.txt (location+)rockyou.txt

**Task 6**

.\hashcat -a 0 -m 110 -r rules\best64.rule (location+)newFileName.txt (location+)rockyou.txt --potfile-disable

**Task 7**

**hashes 复制到新的txt里保存**

.\hashcat −a 3 −m 3200 xxxxxxxx (location+)rockyou.txt

**Exercise 2 Task 2**

**.\openssl ecparam -out ca\_private\_key.pem -name prime256v1 -genkey**

**.\openssl req -new -key ca\_private\_key.pem -out ca\_csr.pem -config (location+)openssl.cnf**

—-----

enter information

-----

**.\openssl req -x509 -key ca\_private\_key.pem -in ca\_csr.pem -out ca\_certificate.pem -days 365 -config (location+)openssl.cnf**

Warning (is ok)

**.\openssl ecparam -out domain\_private\_key.pem -name prime256v1 -genkey**

**.\openssl req -new -key domain\_private\_key.pem -out domain\_csr.pem -config** (location+)**openssl.cnf**

enter information -----

Common Name:21094655d.polyu.edu.hk

**.\openssl x509 -req -in domain\_csr.pem -CA ca\_certificate.pem -CAkey ca\_private\_key.pem -CAcreateserial -out domain\_certificate.pem -days 365**

return:

Certificate request self-signature ok

subject=C=HK, ST=Kowloon, L=city, O=PolyU, OU=COMP3334, CN=21094655d.polyu.edu.hk, emailAddress=21094655d@connect.polyu.hk