Introduction to Cryptography

Task-1
You have received the following encrypted message: “Xjnvw lc sluxjmw jsqm wjpmcqbg jg wqcxqmnvw; xjzjmmjd lc wjpm sluxjmw jsqm bqccqm zqy.” Zlwvzjxj Zpcvcol
You can guess that it is a quote. Who said it?
Miyamoto Musashi

Task-2
Decrypt the file quote01 encrypted (using AES256) with the key s!kR3T55 using gpg. What is the third word in the file?
waste

```
nitin@nobara-pc ~/D/intro-to-cryptography> cd task02/
nitin@nobara-pc ~/D/i/task02> gpg --output original_message.txt --decrypt quote01.txt.gpg
gpg: directory '/home/nitin/.gnupg' created
gpg: keybox '/home/nitin/.gnupg/pubring.kbx' created
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
nitin@nobara-pc ~/D/i/task02> ls
original_message.txt  quote01.txt.gpg  quote02  quote03.txt.gpg
nitin@nobara-pc ~/D/i/task02> cat original_message.txt
Do not waste time idling or thinking after you have set your goals.
Miyamoto Musashi
nitin@nobara-pc ~/D/i/task02>
```

Decrypt the file quote02 encrypted (using AES256-CBC) with the key s!kR3T55 using openssl. What is the third word in the file?
Science

```
nitin@nobara-pc ~/D/i/task02> openssl aes-256-cbc -d -in quote02 -out original_message_2.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
nitin@nobara-pc ~/D/i/task02> openssl aes-256-cbc -pbkdf2 -iter 1000 -d -in quote02 -out original_message_2.txt
enter AES-256-CBC decryption password:
bad decrypt
009E4FCD947F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:providers/implementations/c
```

Decrypt the file quote03 encrypted (using CAMELLIA256) with the key s!kR3T55 using gpg. What is the third word in the file?
understand

```
nitin@nobara-pc ~/D/i/task02 [1]> gpg --output original_message.txt --decrypt quote03.txt.gpg
gpg: CAMELLIA256.CFB encrypted data
gpg: encrypted with 1 passphrase
File 'original_message.txt' exists. Overwrite? (y/N) Y
nitin@nobara-pc ~/D/i/task02> cat original_message.txt
You must understand that there is more than one path to the top of the mountain.
Miyamoto Musashi
nitin@nobara-pc ~/D/i/task02>
```

Task-3
Bob has received the file ciphertext_message sent to him from Alice. You can find the key you need in the same folder. What is the first word of the original plaintext?
Perception

```
nitin@nobara-pc ~/D/i/task03> openssl pkeyutl -decrypt -in ciphertext_message  -inkey private-key-bob.pem -out decrypted.txt
```

```
nitin@nobara-pc ~/D/i/task03> cat decrypted.txt
"Perception is strong and sight weak. In strategy it is important to see distant things as if they were close and to take a distanced view of close things."
Miyamoto Musashi
```

Take a look at Bob's private RSA key. What is the last byte of p?
e7

Take a look at Bob's private RSA key. What is the last byte of q?
27

```
nitin@nobara-pc ~/D/i/task03> openssl rsa -in private-key-bob.pem -text -noout
```

```
prime1:
    00:ff:ea:65:3e:e5:96:96:0b:66:55:f1:f9:d0:37:
    66:e9:35:a5:c3:43:ca:66:75:40:49:46:8d:85:a7:
    ff:f4:73:97:69:11:a1:1e:37:f9:e3:38:cb:c0:5e:
    56:e9:1a:0d:f2:9f:80:56:87:2a:99:bb:88:8e:93:
    35:5a:9a:c6:f7:99:44:90:88:09:33:a6:0d:ea:b4:
    56:98:66:20:9c:34:e7:b9:33:64:4f:08:01:08:62:
    44:68:8f:df:79:0d:84:2b:77:e7:03:8b:3c:7a:e3:
    e0:e0:ee:23:64:22:51:ed:dd:b8:1c:b3:75:c4:3f:
    4a:cf:fc:7c:57:0b:95:75:e7
prime2:
    00:e8:72:11:5c:b5:5c:14:19:85:ce:e7:d2:e9:54:
    7b:58:ae:32:e9:e6:39:a7:65:b4:90:2f:53:b5:9d:
    22:62:84:fe:52:86:f5:01:a2:9c:b0:4f:80:ee:d4:
    07:27:3b:69:02:70:33:da:7d:97:56:b9:3e:f3:a1:
    84:9e:73:6a:47:e5:99:8c:44:86:75:c1:bf:71:89:
    06:b0:ee:dd:16:45:e7:05:fa:02:bd:e6:3e:b7:f2:
    fe:e7:22:0b:ed:ca:23:a0:68:0b:fe:fb:c3:57:19:
    21:58:6e:73:1d:9d:3c:2a:8a:c1:7e:ea:73:67:5a:
    cb:3d:a8:9b:be:50:08:9e:27
```

Task-4
A set of Diffie-Hellman parameters can be found in the file dhparam.pem. What is the size of the prime number in bits?
4096

What is the prime number's last byte (least significant byte)?
4f

```
nitin@nobara-pc ~/D/i/task04> openssl dhparam -in dhparams.pem -text -noout
    DH Parameters: (4096 bit)
```

Task-5
What is the SHA256 checksum of the file order.json?
2c34b68669427d15f76a1c06ab941e3e6038dacdfb9209455c87519a3ef2c660

Open the file order.json and change the amount from 1000 to 9000. What is the new SHA256 checksum?
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466

Using SHA256 and the key 3RfDFz82, what is the HMAC of order.txt?
c7e4de386a09ef970300243a70a444ee2a4ca62413aeaeb7097d43d2c5fac89f

```
nitin@nobara-pc ~/D/i/task05> sha256sum order.json
2c34b68669427d15f76a1c06ab941e3e6038dacdfb9209455c87519a3ef2c660  order.json
nitin@nobara-pc ~/D/i/task05> nano order.json
nitin@nobara-pc ~/D/i/task05> sha256sum order.json
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466  order.json
nitin@nobara-pc ~/D/i/task05> sha256hmac order.txt --key 3RfDFz82
c7e4de386a09ef970300243a70a444ee2a4ca62413aeaeb7097d43d2c5fac89f  order.txt
nitin@nobara-pc ~/D/i/task05>
```

Task-6
What is the size of the public key in bits?
4096

Till which year is this certificate valid?
2039

```
nitin@nobara-pc ~/D/i/task06> openssl x509 -in cert.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2b:29:0c:2f:b0:52:3a:79:89:1f:82:11:07:bd:9d:84:2a:23:d5:1c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = UK, ST = London, L = London, O = Default Company Ltd
        Validity
            Not Before: Aug 11 11:34:19 2022 GMT
            Not After : Feb 25 11:34:19 2039 GMT
        Subject: C = UK, ST = London, L = London, O = Default Company Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

Task-7
You were auditing a system when you discovered that the MD5 hash of the admin password is 3fc0a7acf087f549ac2b266baf94b8b1. What is the original password?
qwerty123