2021

ENCRYPTION AND PKI

GAGANPREET SINGH

Encryption and PKI

Encryption and PKI 1

1. Create a web server (IIS) that will accept secure connections on port 8888 2

1.1 Show the connection and usage of the port 8888 2

1.2 Usage 5

1.3 Certification 6

2.USING OPENSSL OR ANY WEBTOOL, CREATE A PAIR OF KEYS(PRIVATE AND PUBLIC) . Find a way to prove that the private key you have is a match to the public key. 10

2.1– KEYPAIR GENERATION 10

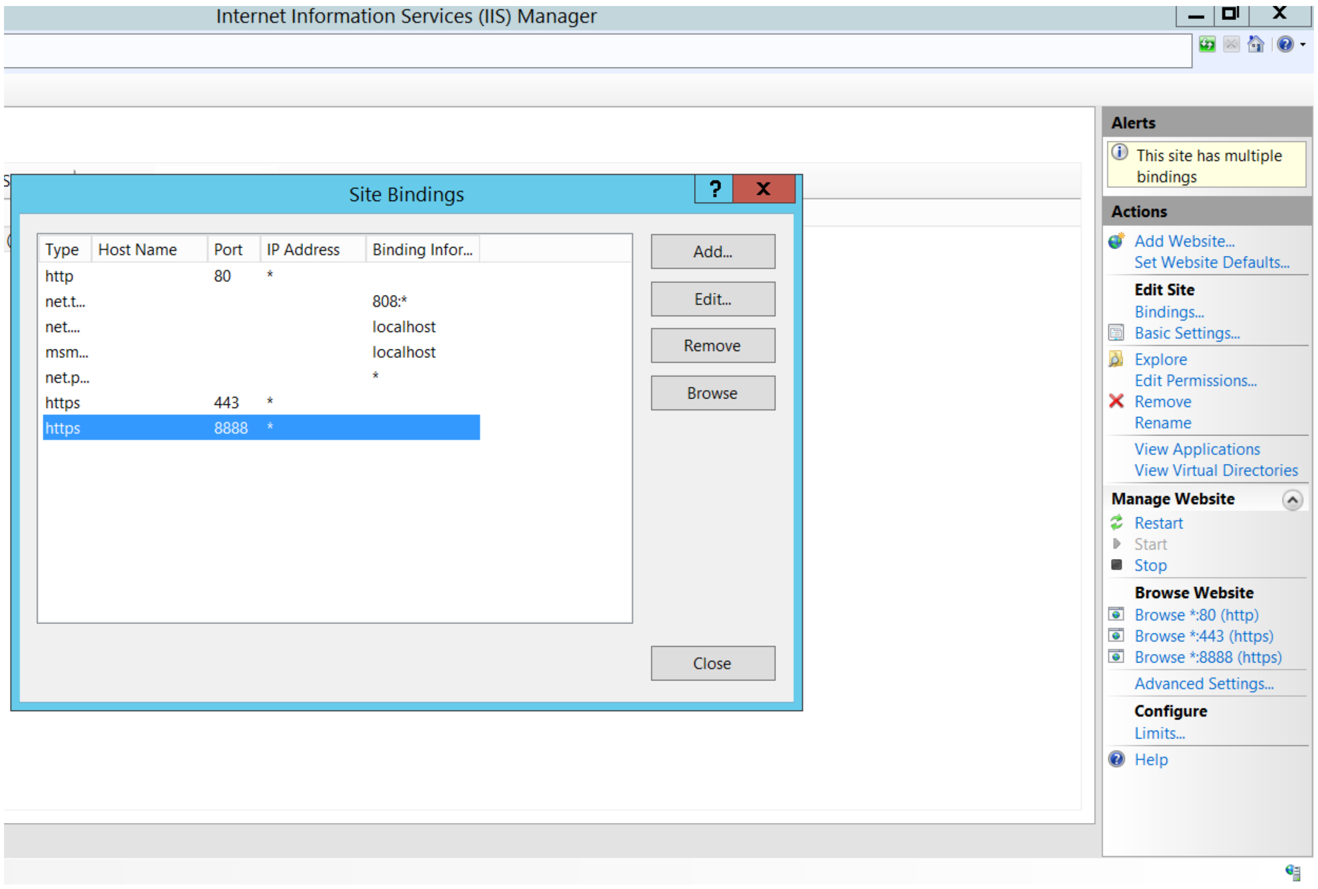
2.2– VERIFY PRIVATE AND PUBLIC KEY MATCH 13

1. Create a web server (IIS) that will accept secure connections on port 8888

1.1 Show the connection and usage of the port 8888

1.ADDING THE PORT INTO THE SERVER

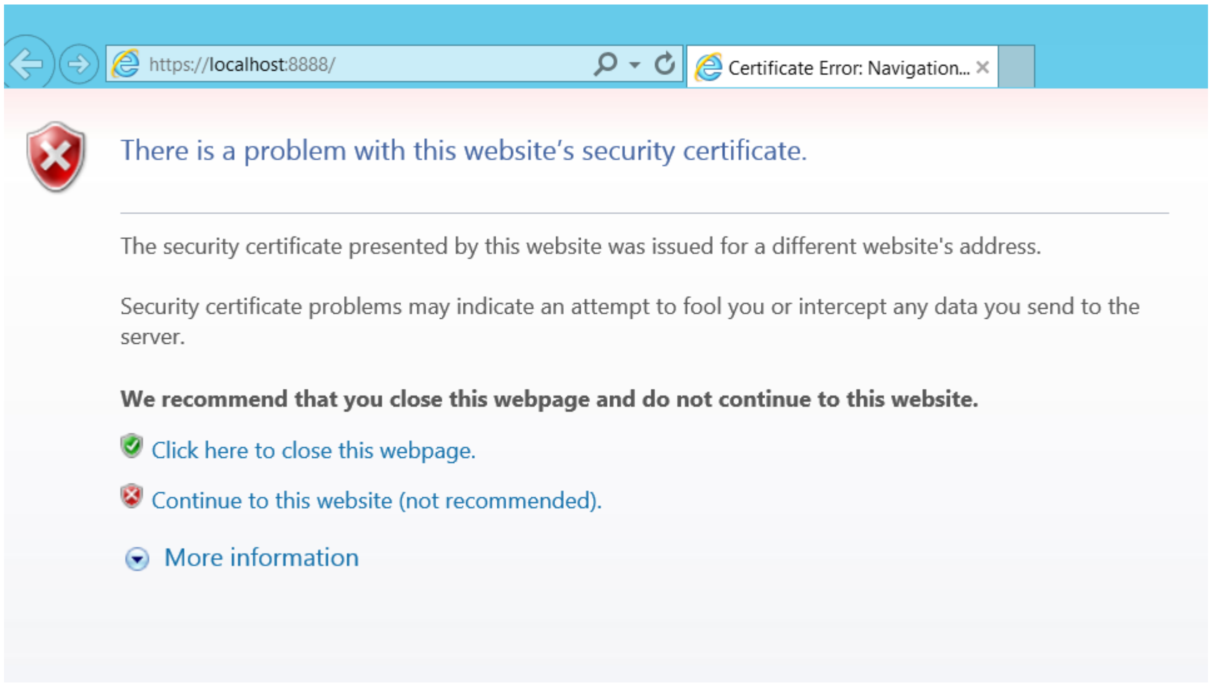
- With the provided references we have created an IIS https secure server for the default website on the port 8888.



Type	Host Name	Port	IP Address	Binding Infor...
http		80	*	
net.t...				808:*
net....				localhost
msm...				localhost
net.p...				*
https		443	*	
https		8888	*	

2.SHOWING ERROR ON LOCALHOST

- Port 8888 cannot browse with the localhost so, for hosting we must use our system-name instead of localhost and then we can establish the server that will accept secure connection.



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

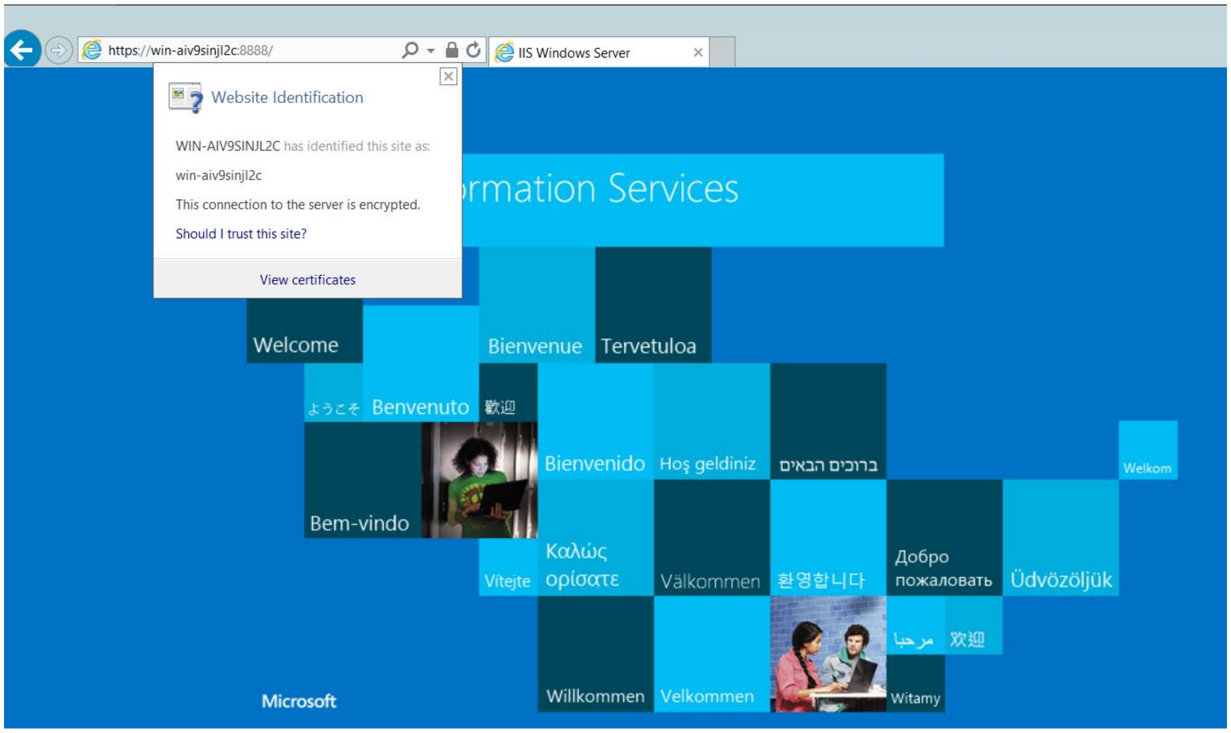
Click here to close this webpage.

Continue to this website (not recommended).

More information

3.IIS SERVER ON PORT8888

- Here we can see that we used https://win-aiv9sinjl2c:8888/ to host the server where win-aiv9sinjl2c is the system-name.
- The padlock clearly shows that "This connection on the server is encrypted" that means this webserver is secured with the encryption and ready to accept secure connections.


https://win-aiv9sinjl2c:8888/

IIS Windows Server

Website Identification

WIN-AIV9SINJL2C has identified this site as:

win-aiv9sinjl2c

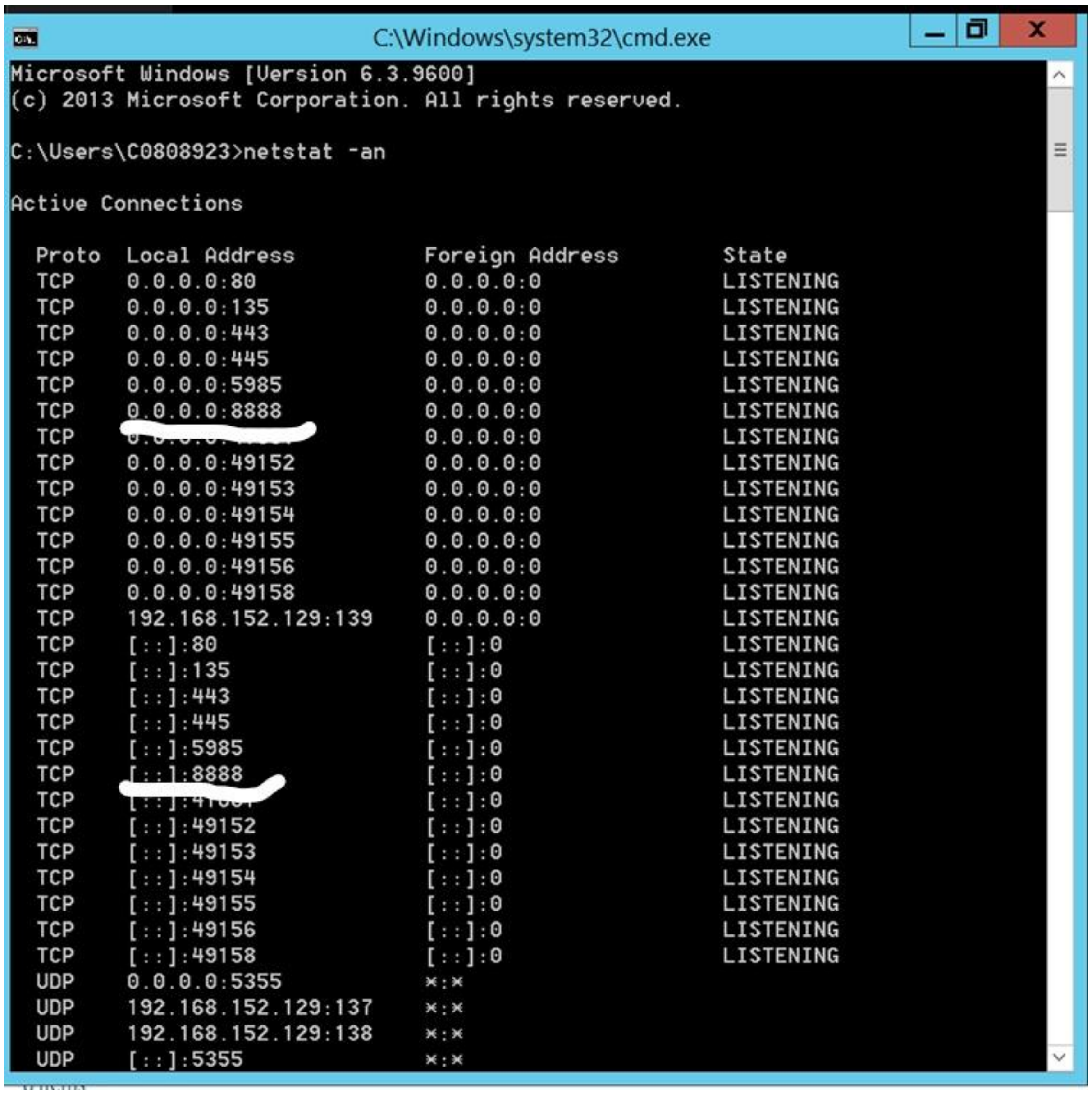
This connection to the server is encrypted.

Should I trust this site?

View certificates

1.2 Usage

- With the help of netstat which is command-line network utility that displays the network connections for TCP shows that port 8888 is currently listening and using the data.
- So, that means ports are working properly fine.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\C0808923>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8888           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING
  TCP    192.168.152.129:139    0.0.0.0:0              LISTENING
  TCP    [::]:80                [::]:0                 LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:443               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5985              [::]:0                 LISTENING
  TCP    [::]:8888              [::]:0                 LISTENING
  TCP    [::]:47001             [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [::]:49158             [::]:0                 LISTENING
  UDP    0.0.0.0:5355           *:*
  UDP    192.168.152.129:137    *:*
  UDP    192.168.152.129:138    *:*
  UDP    [::]:5355              *:*
```

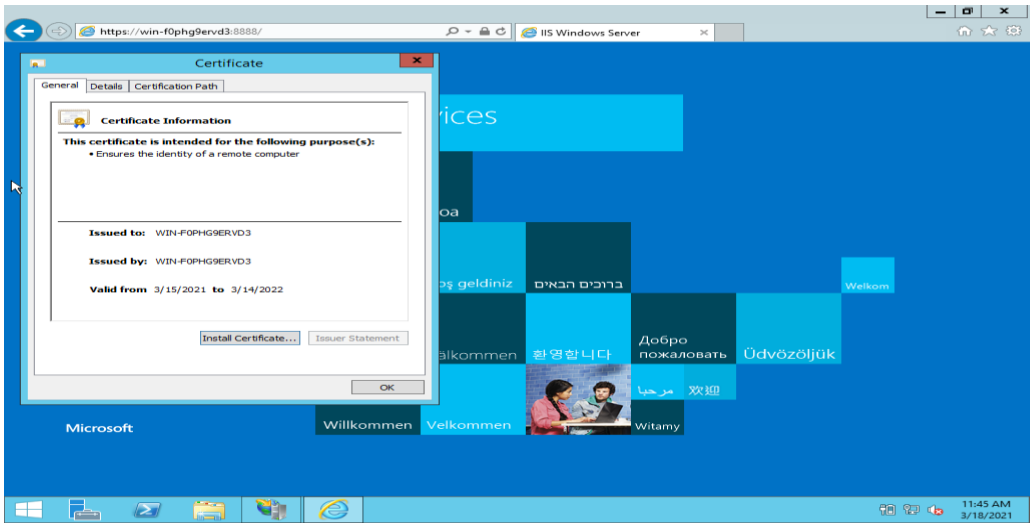
- TCP 8888 mainly used for the data communication over the network and uses ddi-tcp-1 services.
- The main benefit of TCP is it guarantee's communication over port 8888 in the same order which they were sent, this is the main difference between TCP and UDP.
- Although, port 8888 is unofficial and unauthorized port.

1.3 Certification

- In non-development environment like this case, the certifying authority is the user or the server manager or a company.

1. GENERAL CERTIFICATE INFORMATION

Below is the screenshot of the general tab of certificate properties which gives information regarding who the certificate is issued to, from whom it has been issued and the time validity for which the certificate is validate.



Certificate Information

This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer

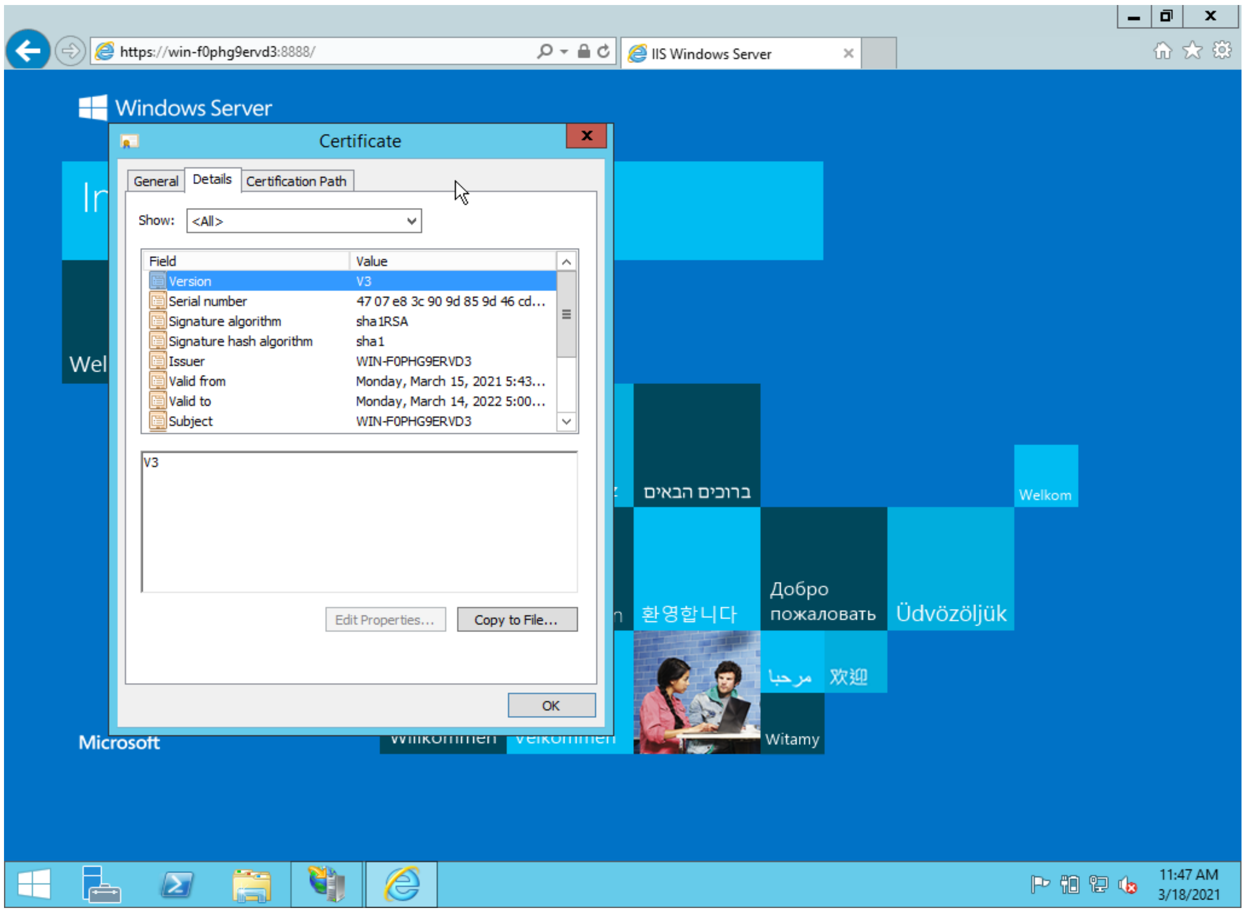
Issued to: WIN-F0PHG9ERVD3

Issued by: WIN-F0PHG9ERVD3

Valid from 3/15/2021 to 3/14/2022

2.BASIC DETAILS OF THE CERTIFICATE

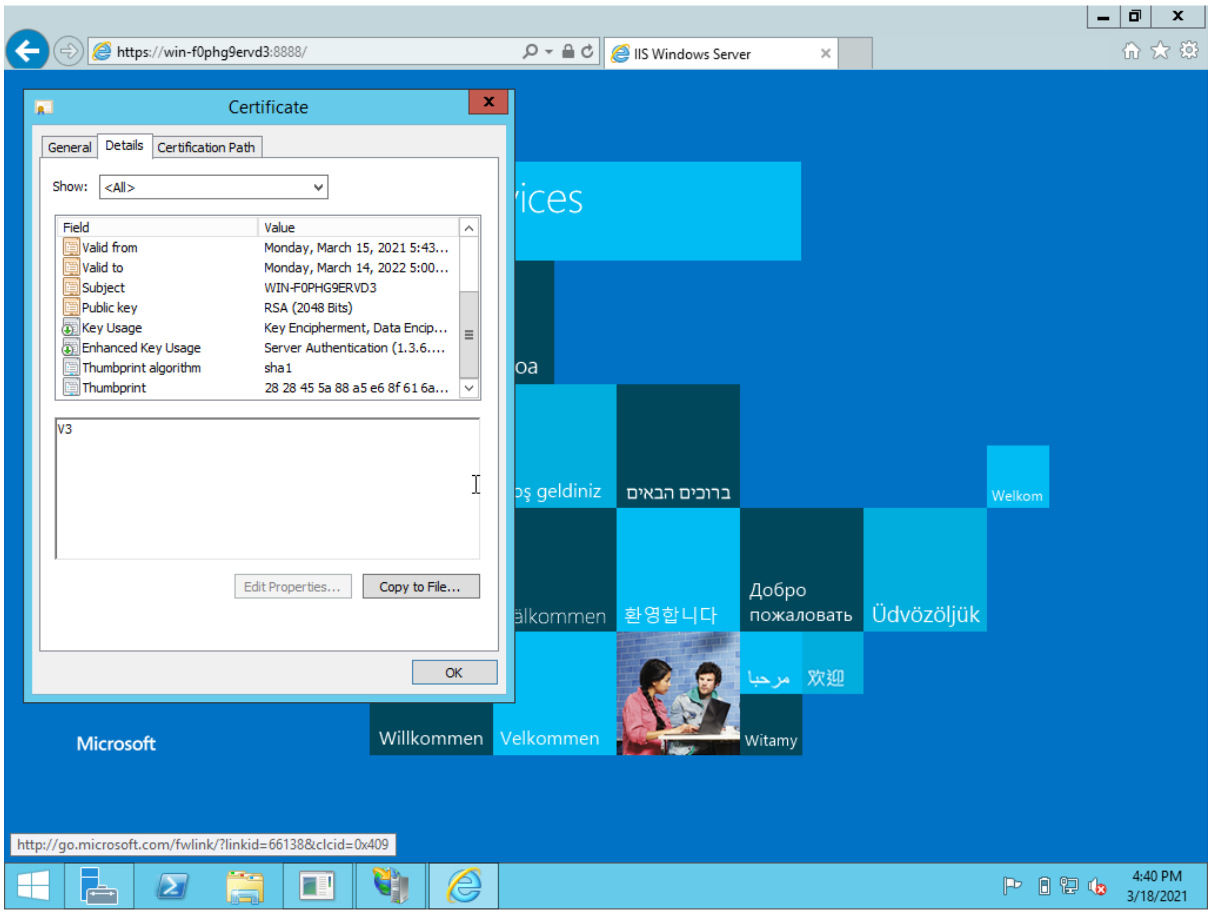
This tab shows the various attributes of the certificate including the version, serial number, signature algorithm, signature hash algorithm and many others.



Field	Value
Version	V3
Serial number	47 07 e8 3c 90 9d 85 9d 46 cd...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	WIN-F0PHG9ERVD3
Valid from	Monday, March 15, 2021 5:43...
Valid to	Monday, March 14, 2022 5:00...
Subject	WIN-F0PHG9ERVD3

V3

3.OVERALL ANALYSIS OF CERTIFICATE



Field	Value
Valid from	Monday, March 15, 2021 5:43...
Valid to	Monday, March 14, 2022 5:00...
Subject	WIN-F0PHG9ERVD3
Public key	RSA (2048 Bits)
Key Usage	Key Encipherment, Data Encip...
Enhanced Key Usage	Server Authentication (1.3.6....
Thumbprint algorithm	sha1
Thumbprint	28 28 45 5a 88 a5 e6 8f 61 6a...

V3

- This certificate can be used by the devices connected to the internal network(intranet) without any issues.
- An external device can access this, but this will show that the connection is not to be trusted and because it is a user signed certificate, it is very hard to assure external users about the security of the webpage or web connection.
- Most used browsers and OS do not trust self-signed certificates. The browsers will prompt the users to manually accept the risks involved with accessing these websites and show a warning message.

- This is due to the certificate being issued by an individual or independent organization rather than a Certifying Authority (CA), as in a PKI, both parties must trust CA and the set of rules they follow.
- But a self-signed certificate is not bound by this set of rules, making it easier for malicious elements to tamper with the system. So, for this reason, even if the certificate is valid, it will still be considered untrustworthy.

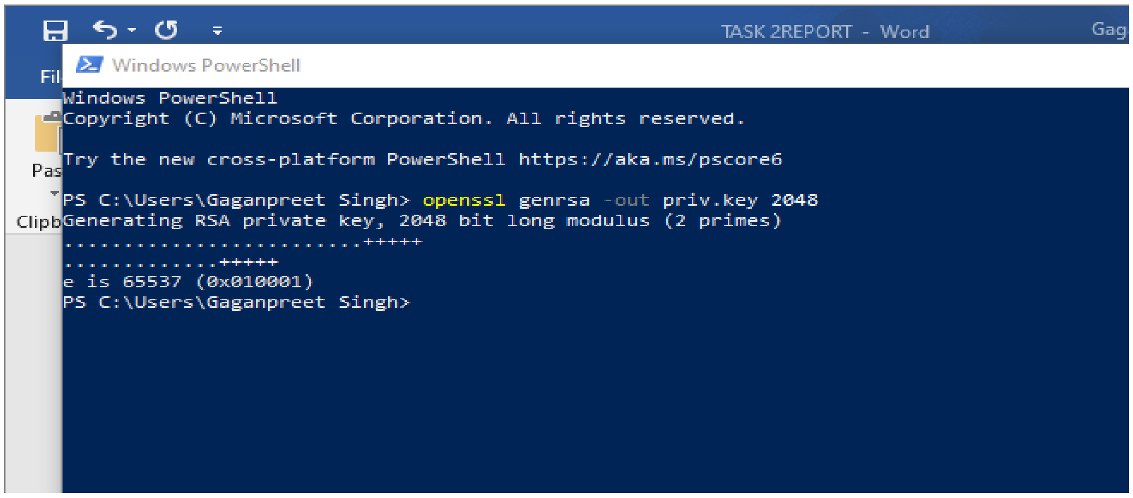
2.USING OPENSSL OR ANY WEBTOOL, CREATE A PAIR OF KEYS (PRIVATE AND PUBLIC) . Find a way to prove that the private key you have is a match to the public key.

2.1– KEYPAIR GENERATION

To create a key-pair we will be using RSA algorithm. RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone.

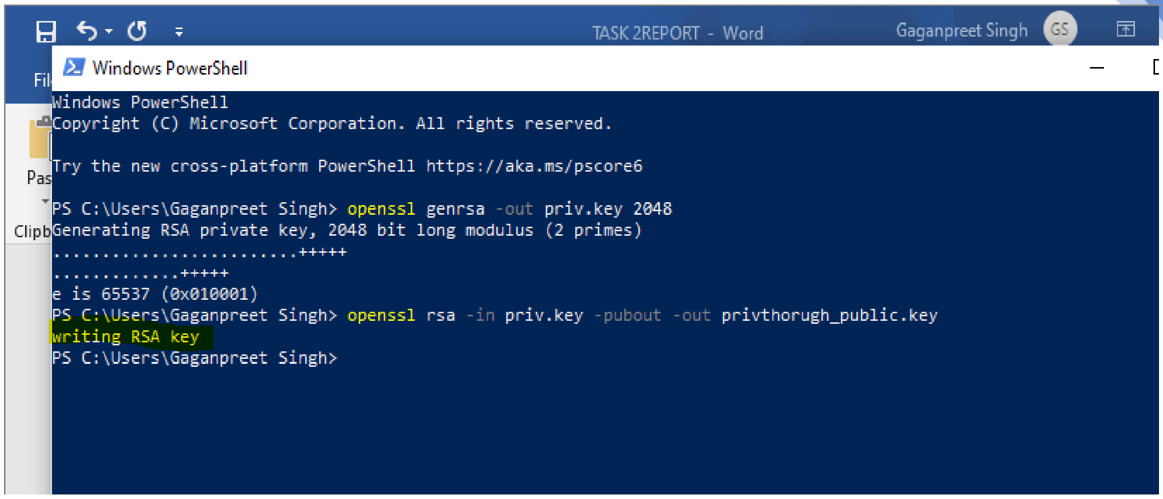
To create the key pair, we need to follow below steps:

1. First, we will be creating 2048 key size key using the command **openssl genrsa -out priv.key 2048** using openssl.



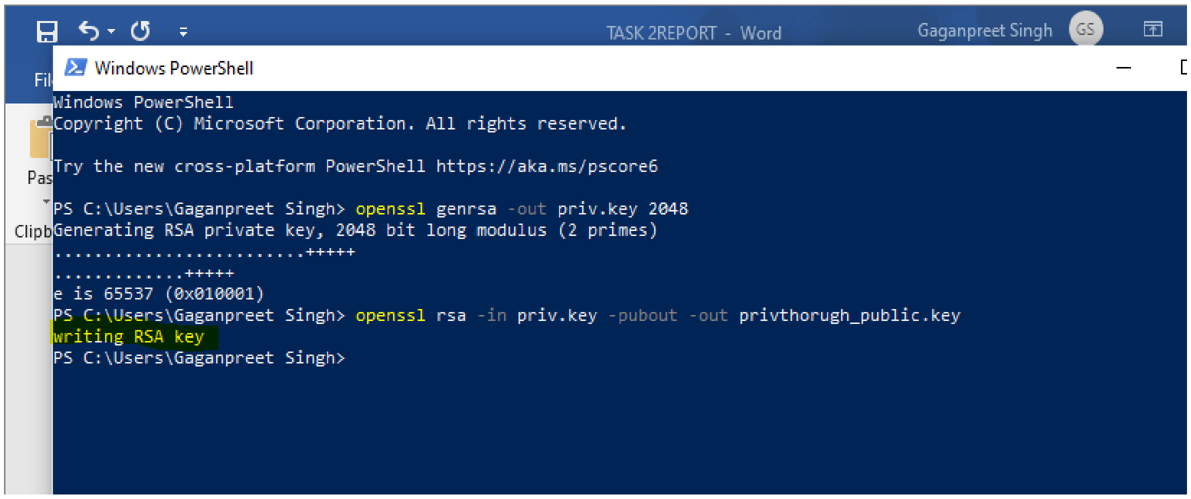
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Gaganpreet Singh> openssl genrsa -out priv.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.........................+++++
.............+++++
e is 65537 (0x010001)
PS C:\Users\Gaganpreet Singh>
```

2. Open shell and type the command.
3. Now generate the public key using the same private key by using the command **openssl rsa -in priv.key -pubout -out privthorugh_public.key.**



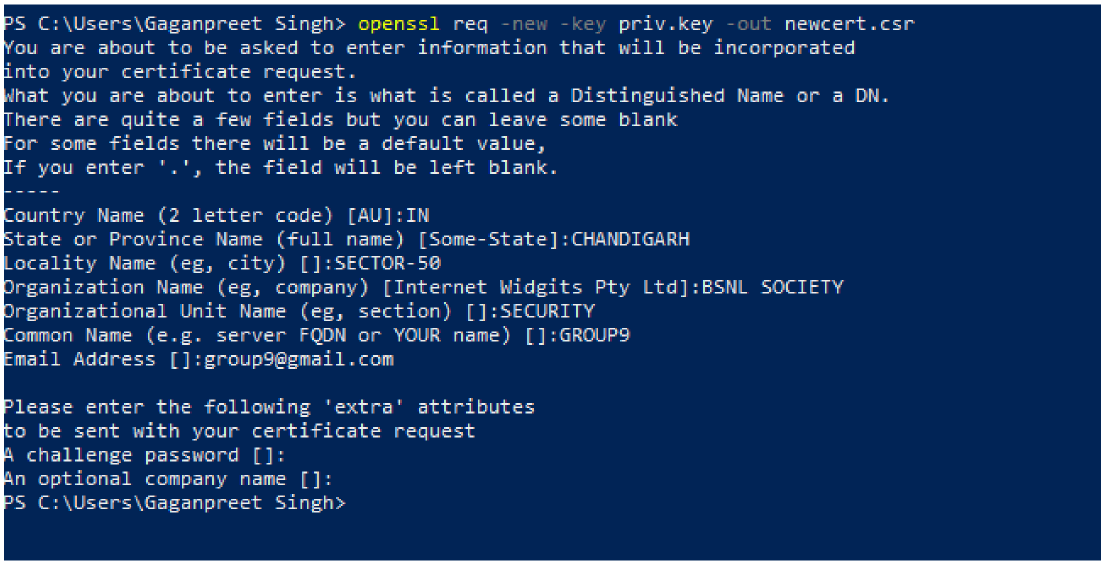
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Gaganpreet Singh> openssl genrsa -out priv.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........................+++++
.............+++++
e is 65537 (0x010001)
PS C:\Users\Gaganpreet Singh> openssl rsa -in priv.key -pubout -out privthorugh_public.key
writing RSA key
PS C:\Users\Gaganpreet Singh>
```

4. We can check the created key by using dir command.



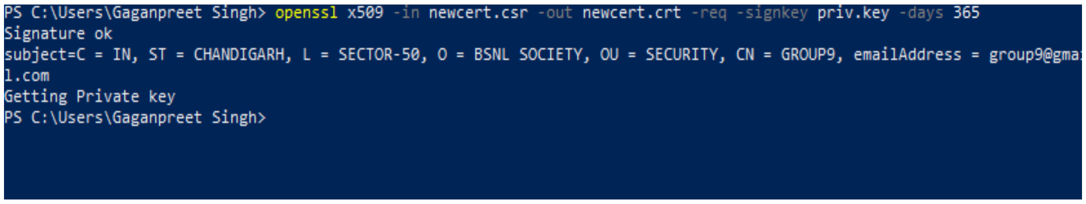
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Gaganpreet Singh> openssl genrsa -out priv.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........................+++++
.............+++++
e is 65537 (0x010001)
PS C:\Users\Gaganpreet Singh> openssl rsa -in priv.key -pubout -out privthorugh_public.key
writing RSA key
PS C:\Users\Gaganpreet Singh>
```

5. Now, after this we'll be creating Certificate Signing Request using the key pair by the command **openssl req -new -key priv.key -out newcert.csr.** This command requires several questions to be answered but we are not here in development environment, so, we will be filling non-specific info.



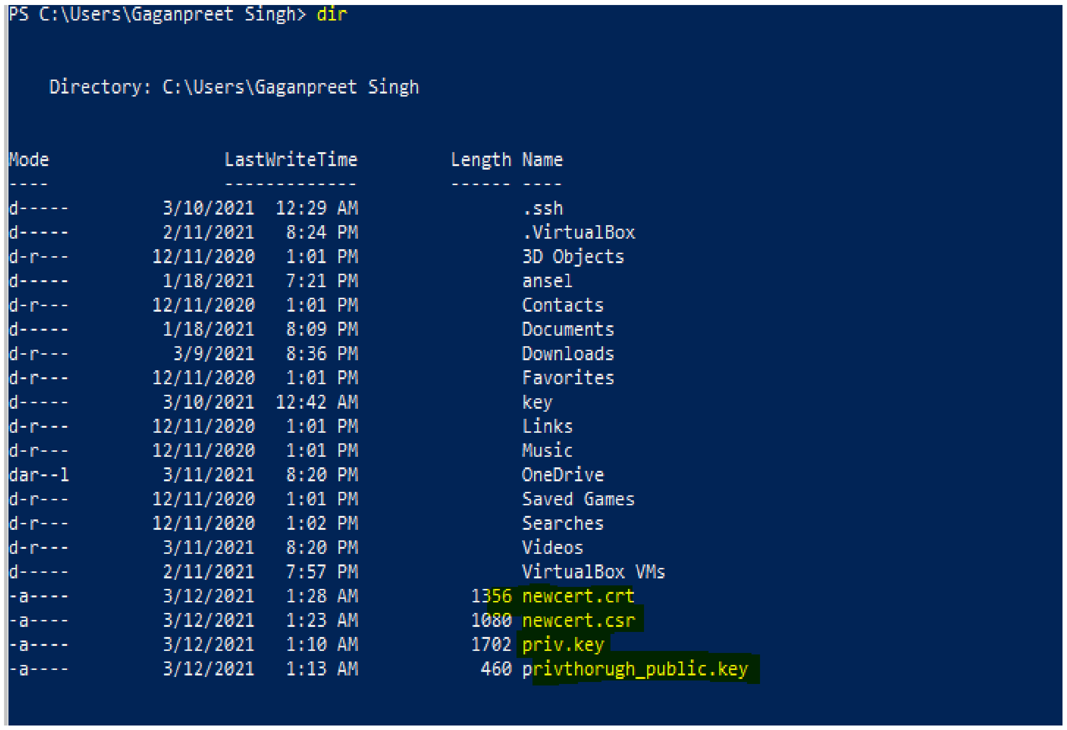
```
PS C:\Users\Gaganpreet Singh> openssl req -new -key priv.key -out newcert.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:CHANDIGARH
Locality Name (eg, city) []:SECTOR-50
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BSNL SOCIETY
Organizational Unit Name (eg, section) []:SECURITY
Common Name (e.g. server FQDN or YOUR name) []:GROUP9
Email Address []:group9@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
PS C:\Users\Gaganpreet Singh>
```

6. Now, if we are in development environment then this csr is sent to a Certification Authority but we are doing for home practice so, we will be creating a self-signed certificate using the command **openssl x509 -in newcert.csr -out newcert.crt -req -signkey priv.key -days 365** and set the validity for 365 days.



```
PS C:\Users\Gaganpreet Singh> openssl x509 -in newcert.csr -out newcert.crt -req -signkey priv.key -days 365
Signature ok
subject=C = IN, ST = CHANDIGARH, L = SECTOR-50, O = BSNL SOCIETY, OU = SECURITY, CN = GROUP9, emailAddress = group9@gma
l.com
Getting Private key
PS C:\Users\Gaganpreet Singh>
```

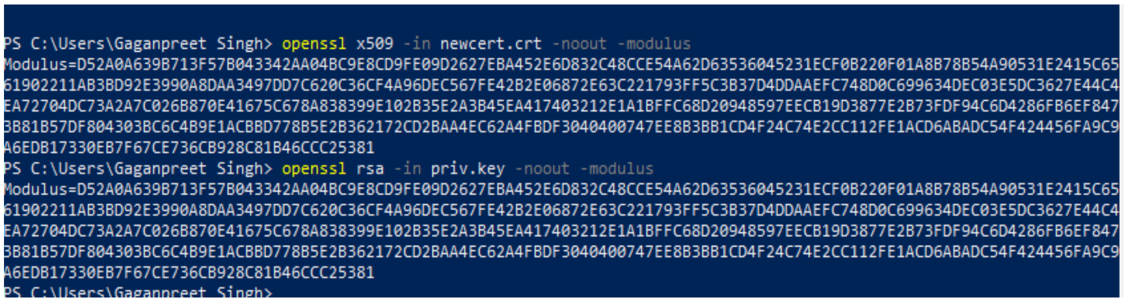
7. Check the files created using dir command.



```
PS C:\Users\Gaganpreet Singh> dir


    Directory: C:\Users\Gaganpreet Singh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/10/2021  12:29 AM                .ssh
d-----         2/11/2021   8:24 PM                .VirtualBox
d-r---        12/11/2020   1:01 PM                3D Objects
d-----         1/18/2021   7:21 PM                ansel
d-r---        12/11/2020   1:01 PM                Contacts
d-----         1/18/2021   8:09 PM                Documents
d-r---          3/9/2021   8:36 PM                Downloads
d-r---        12/11/2020   1:01 PM                Favorites
d-----         3/10/2021  12:42 AM                key
d-r---        12/11/2020   1:01 PM                Links
d-r---        12/11/2020   1:01 PM                Music
dar--l         3/11/2021   8:20 PM                OneDrive
d-r---        12/11/2020   1:01 PM                Saved Games
d-r---        12/11/2020   1:02 PM                Searches
d-r---         3/11/2021   8:20 PM                Videos
d-----         2/11/2021   7:57 PM                VirtualBox VMs
-a----         3/12/2021   1:28 AM           1356 newcert.crt
-a----         3/12/2021   1:23 AM           1080 newcert.csr
-a----         3/12/2021   1:10 AM           1702 priv.key
-a----         3/12/2021   1:13 AM            460 privthorugh_public.key
```

2.2– VERIFY PRIVATE AND PUBLIC KEY MATCH

8. Now about RSA algorithm, which has the formula$((m^e)^d)\%n=m)$ which states e and n are in public key and d and n are in private key
To check the key files are related we have to check n's and if they match files are two halves of the same key
For this i used following commands- **openssl x509 -in newcert.crt -noout -modulus** and **openssl rsa -in priv.key -noout -modulus** to check the modulus value.



```
PS C:\Users\Gaganpreet Singh> openssl x509 -in newcert.crt -noout -modulus
Modulus=D52A0A639B713F57B043342AA04BC9E8CD9FE09D2627EBA452E6D832C48CCE54A62D63536045231ECF0B220F01A8B78B54A90531E2415C65
61902211AB3BD92E3990A8DAA3497DD7C620C36CF4A96DEC567FE42B2E06872E63C221793FF5C3B37D4DDAAEFC748D0C699634DEC03E5DC3627E44C4
EA72704DC73A2A7C026B870E41675C678A838399E102B35E2A3B45EA417403212E1A1BFFC68D20948597EECB19D3877E2B73FDF94C6D4286FB6EF847
3B81B57DF804303BC6C4B9E1ACBBD778B5E2B362172CD2BAA4EC62A4FBDF3040400747EE8B3BB1CD4F24C74E2CC112FE1ACD6ABADC54F424456FA9C9
A6EDB17330EB7F67CE736CB928C81B46CCC25381
PS C:\Users\Gaganpreet Singh> openssl rsa -in priv.key -noout -modulus
Modulus=D52A0A639B713F57B043342AA04BC9E8CD9FE09D2627EBA452E6D832C48CCE54A62D63536045231ECF0B220F01A8B78B54A90531E2415C65
61902211AB3BD92E3990A8DAA3497DD7C620C36CF4A96DEC567FE42B2E06872E63C221793FF5C3B37D4DDAAEFC748D0C699634DEC03E5DC3627E44C4
EA72704DC73A2A7C026B870E41675C678A838399E102B35E2A3B45EA417403212E1A1BFFC68D20948597EECB19D3877E2B73FDF94C6D4286FB6EF847
3B81B57DF804303BC6C4B9E1ACBBD778B5E2B362172CD2BAA4EC62A4FBDF3040400747EE8B3BB1CD4F24C74E2CC112FE1ACD6ABADC54F424456FA9C9
A6EDB17330EB7F67CE736CB928C81B46CCC25381
PS C:\Users\Gaganpreet Singh>
```

9. Now we can the modulus value match which means the files are two halves of the same key.