

به نام خدا



«امنیت داده و شبکه»

دکتر امینی

تمرین سوم

علیرضا دهقانیپور فراشاه

۹۸۱۰۱۵۵۵

سوال اول.....	3
سوال دوم.....	4
بخش اول.....	4
بخش دوم.....	11
سوال سوم.....	12
بخش اول.....	12
بخش دوم.....	18
سوال چهارم.....	19

سوال اول

(الف)

1. در گام اول A ابتدا ID خود را به همراه رمزشدهی نانس برای B می‌فرستد تا بتواند در ادامه به کمک نانس از تازگی کلید اطمینان حاصل یابد. در این گام مقدار نانس به وسیلهی کلید مخفی میان خودش و KDC رمز می‌کند.
2. در گام دوم B پیام دریافت شده در گام اول را به همراه ID خود و رمزشدهی نانس خود به KDC ارسال می‌کند.
3. در این گام KDC کلید جلسه به همراه ID شخص B به همراه نانس A را با کلید میان خودش و A رمز می‌کند و همچنین کلید جلسه به همراه ID شخص A به همراه نانس B را با کلید میان خودش و B رمز می‌کند و این دو پیام را کنار یکدیگر قرار می‌دهد و برای B می‌فرستد. در این گام B پس از دریافت پیام می‌تواند بخش اول پیام را با کلید Kb باز کند و کلید جلسه را بدست آورد و نانس را با نانس ارسالی خودش مقایسه کند و از تازگی کلید جلسه اطمینان یابد.
4. در این گام B بخش دوم پیام دریافتی در گام سه را به A ارسال می‌کند. A در این گام با رمزگشایی پیام به کمک Ka می‌تواند به کلید جلسه دسترسی پیدا کند و با مقایسه نانس ارسالی در گام اول و نانس دریافت شده در این پیام از تازگی کلید مطمئن شود.

(ب)

بله، هم A و هم B هر دو یک نانس تولید کرده و آن را ارسال می‌کنند و KDC آن نانس را رمز می‌کند و فرستد و در هنگام دریافت کلید جلسه هر دوی A و B می‌توانند نانس دریافتی را با نانی که خود ارسال کرده‌اند مقایسه کنند و از تازگی کلید مطمئن شوند.

(پ)

خیر، زیرا در این روش اگر Ka و Kb لو برود مهاجم با داشتن پیام‌های قبلی تمامی پیام‌ها را رمزگشایی می‌کند و می‌تواند به کلید جلسات در تمام مراحل قبل دسترسی پیدا کند زیرا در تولید کلید هیچ عامل تصادفی‌ای وجود ندارد.

(ت)

خیر وجود ندارد زیرا که وقتی A در گام ۴ ام به کلید جلسه دست می‌یابد هیچ پیامی برای B ارسال نمی‌کند که نشان دهد کلید را دارد و زنده است. اما A در گام ۴ ام با دریافت پیام از زنده بودن B و دریافت کلید از سمت آن مطمئن می‌شود زیرا این پیام فقط از سمت B می‌تواند ارسال شود و به دلیل وجود نانس و تازگی کلید امکان حملهی replay در این گام وجود ندارد.

(ث)

می‌توان تازگی را با استفاده از مهر زمانی ایجاد کرد ولی باید ساعت‌ها sync باشد و نتوان حملهی suppress-replay زد.

(ج)

نادرست، در مقابل این حمله مقاوم است. زیرا با تولید نانس توسط هر یک از A و B و مقایسهی نانس دریافتی از KDC می‌توان به تازگی کلید پی برد. حال هر گام را بررسی می‌کنیم که آیا می‌توان حملهی تکرار زد یا خیر. در گام اول اگر پیام تکراری ارسال کنیم و خود را جای A بگذاریم در گام چهارم به علت نداشتن Ka نمی‌توانیم کلید جلسه را بدست آوریم. در گام دوم نیز اگر تکرار بزنیم در گام سوم به علت نداشتن Kb نمی‌توان کلید جلسه را بدست آورد. در گام سوم و چهارم نیز به علت وجود نانس امکان حملهی تکرار وجود ندارد.

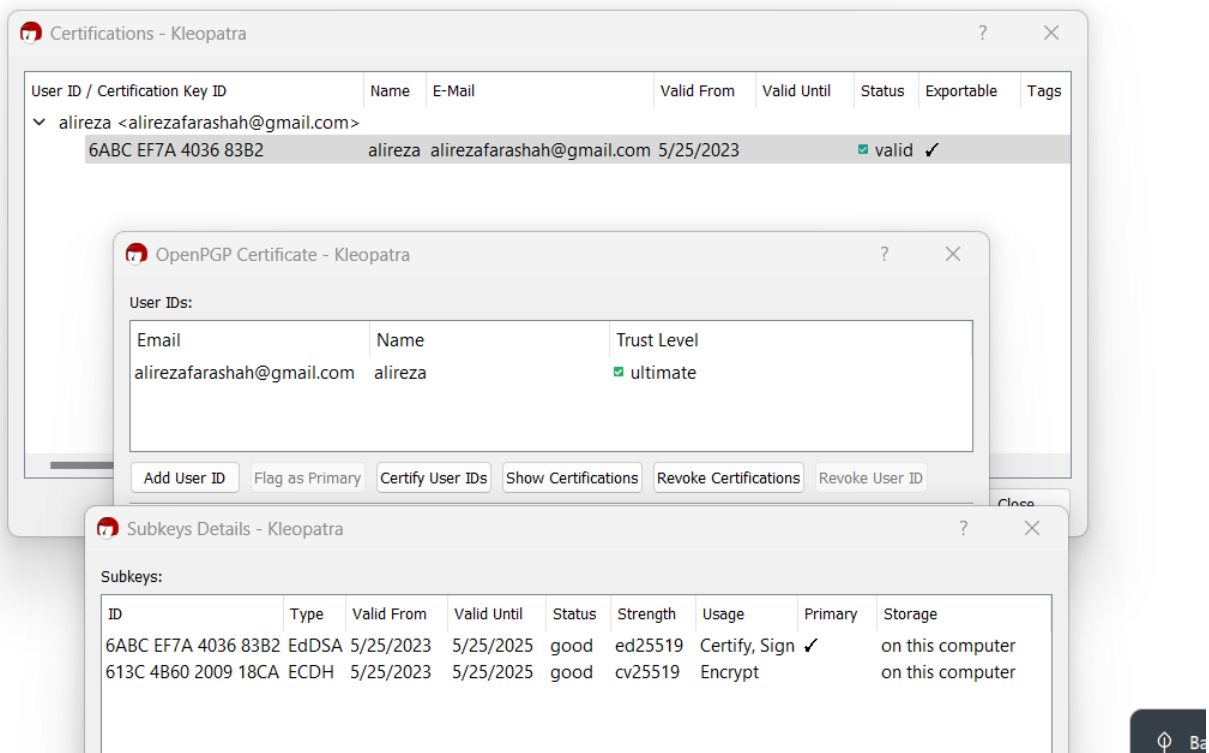
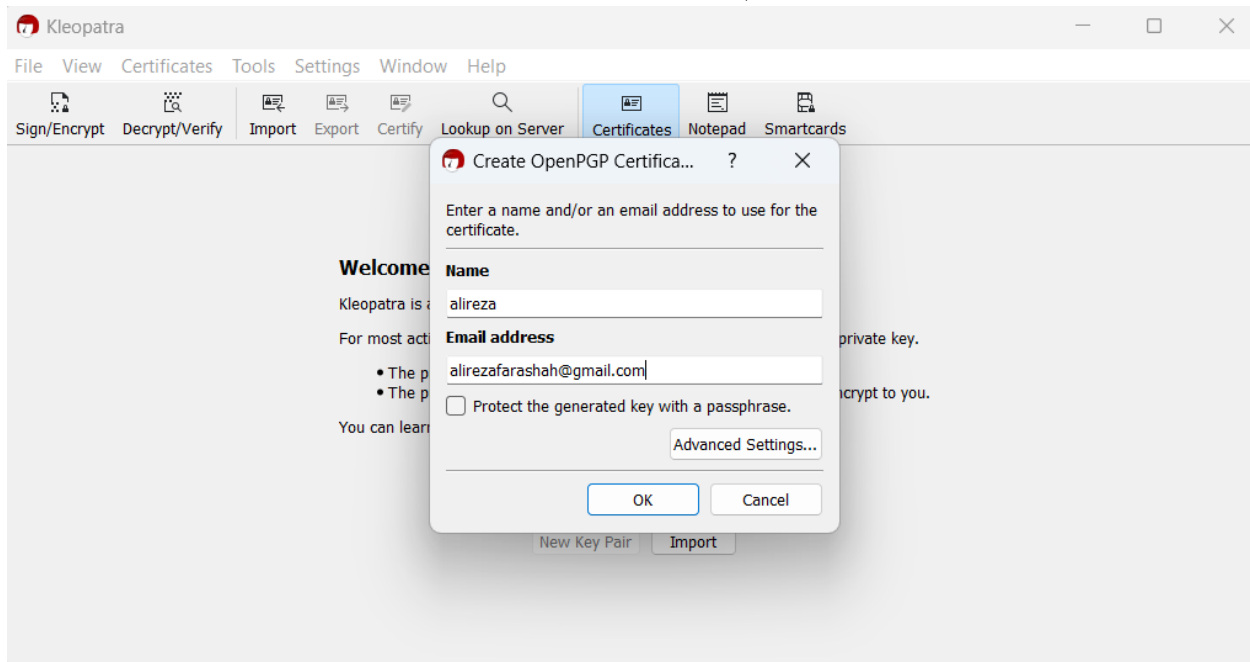
(چ)

مقاوم نیست زیرا اگر زمان‌ها sync نباشد و فرض کنید ساعت A کمی جلوتر باشد آنگاه مهاجم می‌تواند پیام A را ذخیره کند و دوباره در زمان جلوتر ارسال کند. برای جلوگیری از این مشکل می‌توان زمان‌ها را sync کرد و یا از نانس یا یک شمارنده استفاده کرد.

سوال دوم

بخش اول

آ در دو تصویر زیر ایجاد یک جفت کلید عمومی با اسم و ایمیل را مشاهده می کنید.



ب) همانطور که در تصاویر زیر مشخص است الگوریتم امضا EdDSA و الگوریتم رمز AES و الگوریتم هش SHA-512 است. همچنین KeyID برابر 2x6ABC EF7A 4036 83B0 است.

```
alirezaf@LAPTOP-E1B871N6: / x + v
alirezaf@LAPTOP-E1B871N6:/mnt/c/Users/alireza/Desktop/AlirezaFarashah_98101555$ pgpdump alireza_0x403683B2_public.asc
Old: Public Key Packet(tag 6)(51 bytes)
  Ver 4 - new
    Public key creation time - Thu May 25 13:45:02 +0430 2023
    Pub alg - EdDSA Edwards-curve Digital Signature Algorithm(pub 22)
    Unknown public key(pub 22)
Old: User ID Packet(tag 13)(35 bytes)
  User ID - alireza <alirezafarashah@gmail.com>
Old: Signature Packet(tag 2)(153 bytes)
  Ver 4 - new
    Sig type - Positive certification of a User ID and Public Key packet(0x13).
    Pub alg - EdDSA Edwards-curve Digital Signature Algorithm(pub 22)
    Hash alg - SHA512(hash 10)
    Hashed Sub: issuer fingerprint(sub 33)(21 bytes)
      v4 - Fingerprint - dd 92 a1 43 39 a8 4a 4f fb 6f 9f 5a 6a bc ef 7a 40 36 83 b2
    Hashed Sub: signature creation time(sub 2)(4 bytes)
      Time - Thu May 25 13:45:02 +0430 2023
    Hashed Sub: key flags(sub 27)(1 bytes)
      Flag - This key may be used to certify other keys
      Flag - This key may be used to sign data
    Hashed Sub: key expiration time(sub 9)(4 bytes)
      Time - Sun May 25 13:00:00 +0430 2025
    Hashed Sub: preferred symmetric algorithms(sub 11)(4 bytes)
      Sym alg - AES with 256-bit key(sym 9)
      Sym alg - AES with 192-bit key(sym 8)
      Sym alg - AES with 128-bit key(sym 7)
      Sym alg - Triple-DES(sym 2)
    Hashed Sub: unknown(sub 34)(1 bytes)
    Hashed Sub: preferred hash algorithms(sub 21)(5 bytes)
      Hash alg - SHA512(hash 10)
```

```
      Hash alg - SHA512(hash 10)
      Hash alg - SHA384(hash 9)
      Hash alg - SHA256(hash 8)
      Hash alg - SHA224(hash 11)
      Hash alg - SHA1(hash 2)
    Hashed Sub: preferred compression algorithms(sub 22)(3 bytes)
      Comp alg - ZLIB <RFC1950>(comp 2)
      Comp alg - BZip2(comp 3)
      Comp alg - ZIP <RFC1951>(comp 1)
    Hashed Sub: features(sub 30)(1 bytes)
      Flag - Modification detection (packets 18 and 19)
    Hashed Sub: key server preferences(sub 23)(1 bytes)
      Flag - No-modify
    Sub: issuer key ID(sub 16)(8 bytes)
      Key ID - 0x6ABCEf7A403683B2
    Hash left 2 bytes - bb a6
    Unknown signature(pub 22)
Old: Public Subkey Packet(tag 14)(56 bytes)
  Ver 4 - new
    Public key creation time - Thu May 25 13:45:02 +0430 2023
    Pub alg - Reserved for Elliptic Curve(pub 18)
    Unknown public key(pub 18)
Old: Signature Packet(tag 2)(126 bytes)
  Ver 4 - new
    Sig type - Subkey Binding Signature(0x18).
    Pub alg - EdDSA Edwards-curve Digital Signature Algorithm(pub 22)
    Hash alg - SHA512(hash 10)
    Hashed Sub: issuer fingerprint(sub 33)(21 bytes)
      v4 - Fingerprint - dd 92 a1 43 39 a8 4a 4f fb 6f 9f 5a 6a bc ef 7a 40 36 83 b2
    Hashed Sub: signature creation time(sub 2)(4 bytes)
      Time - Thu May 25 13:45:02 +0430 2023
    Hashed Sub: key flags(sub 27)(1 bytes)
      Flag - This key may be used to encrypt communications
      Flag - This key may be used to encrypt storage
    Hashed Sub: key expiration time(sub 9)(4 bytes)
      Time - Sun May 25 13:00:00 +0430 2025
    Sub: issuer key ID(sub 16)(8 bytes)
      Key ID - 0x6ABCEf7A403683B2
    Hash left 2 bytes - b0 a7
    Unknown signature(pub 22)
```

پ) در اینجا از یک سیستم دیگر برای فرستنده استفاده می‌کنیم که با اسم zalireza و همان جیمیل خودم برایش یک جفت کلید تولید می‌کنم و آن را در keys.gnupg.com آپلود می‌کنیم. در شکل زیر این روند را مشاهده می‌کنید.

```
Windows PowerShell
PS C:\Users\user\Desktop\AlirezaFarashah98101555> gpg --list-keys
C:\Users\user\AppData\Roaming\gnupg\pubring.kbx
-----
pub   ed25519 2023-05-25 [SC] [expires: 2025-05-25]
       86E337B0ECF006141C7E9F299E30D579ED5B3B1D
uid           [ultimate] alireza2 <alirezafarashah@gmail.com>
sub   cv25519 2023-05-25 [E] [expires: 2025-05-25]

PS C:\Users\user\Desktop\AlirezaFarashah98101555> gpg --keyserver certserver.pgp.com --send-key 86E337B0ECF006141C7E9F299E30D579ED5B3B1D
gpg: sending key 9E30D579ED5B3B1D to hkp://certserver.pgp.com
gpg: keyserver send failed: Unknown error
gpg: keyserver send failed: Unknown error
PS C:\Users\user\Desktop\AlirezaFarashah98101555> gpg --keyserver keys.gnupg.net --send-key 86E337B0ECF006141C7E9F299E30D579ED5B3B1D
gpg: sending key 9E30D579ED5B3B1D to hkp://keyserver.ubuntu.com
PS C:\Users\user\Desktop\AlirezaFarashah98101555>
```

حال در سیستم دیگر کلید را import می‌کنیم. در تصویر زیر مشاهده می‌کنید.

```
Windows PowerShell
PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> gpg --keyserver hkp://keyserver.ubuntu.com --recv-keys 86E337B0ECF006141C7E9F299E30D579ED5B3B1D
gpg: key 9E30D579ED5B3B1D: "alireza2 <alirezafarashah@gmail.com>" not changed
gpg: Total number processed: 1
gpg:      unchanged: 1
PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> gpg --list-keys
C:\Users\alireza\AppData\Roaming\gnupg\pubring.kbx
-----
pub   ed25519 2023-05-25 [SC] [expires: 2025-05-25]
       DD92A14339A84A4FFB6F9F5A6ABCE7A403683B2
uid           [ultimate] alireza <alirezafarashah@gmail.com>
sub   cv25519 2023-05-25 [E] [expires: 2025-05-25]

pub   ed25519 2023-05-25 [SC] [expires: 2025-05-25]
       86E337B0ECF006141C7E9F299E30D579ED5B3B1D
uid           [ unknown] alireza2 <alirezafarashah@gmail.com>
sub   cv25519 2023-05-25 [E] [expires: 2025-05-25]

PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555>
```

در ادامه فایل message.txt را رمزنگاری می‌کنیم و message.gpg را تولید می‌کنیم که در تصویر زیر مشاهده می‌کنید.

```

Windows PowerShell
PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> type .\message.txt
alireza dehghanpour farashah 98101555
PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> gpg --output message.gpg --encrypt --recipient alireza2 .\message.txt
gpg: 3A4C3F8014CBC2E4: There is no assurance this key belongs to the named user

sub cv25519/3A4C3F8014CBC2E4 2023-05-25 alireza2 <alireza2@gmail.com>
Primary key fingerprint: 86E3 3780 ECF0 0614 1C7E 9F29 9E30 D579 ED5B 3B1D
Subkey fingerprint: 3338 9136 ECD3 AF38 1DD0 3EC4 3A4C 3F80 14CB C2E4

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> ls

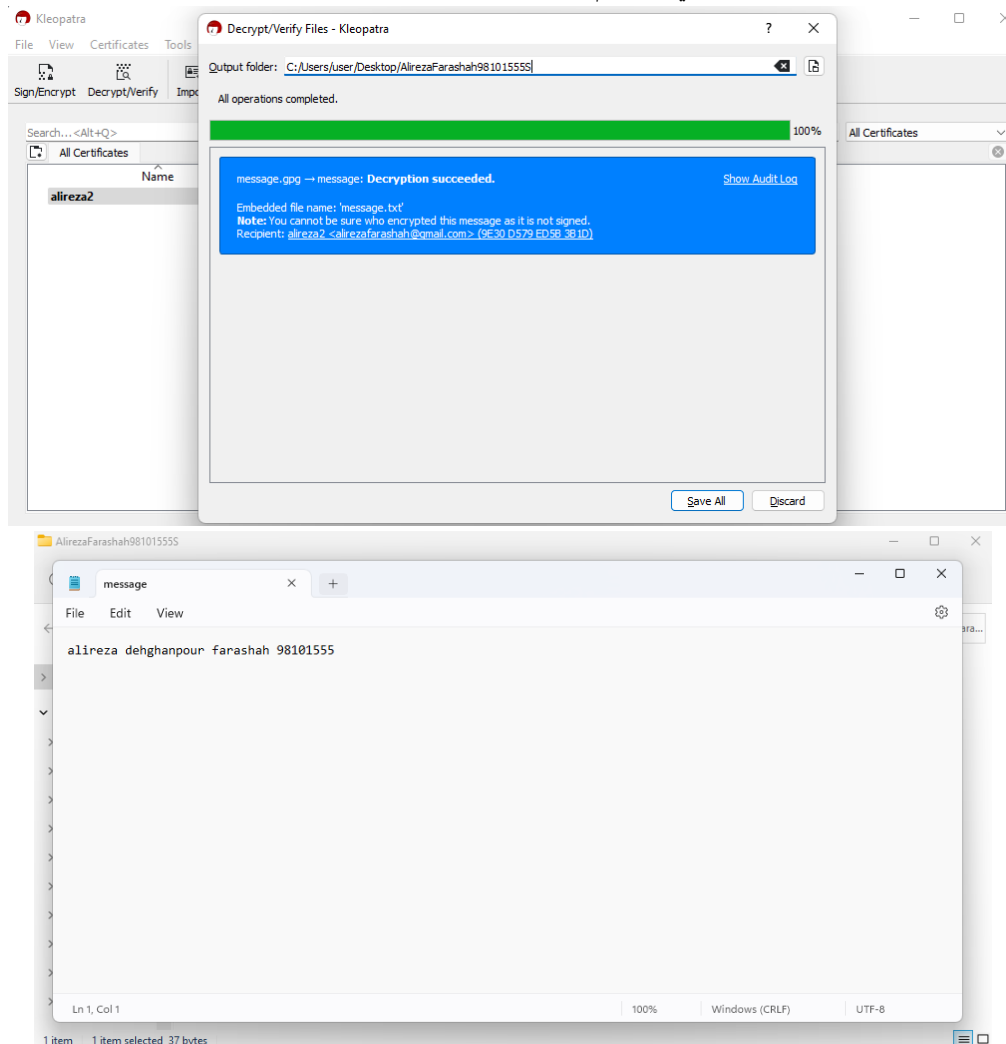
Directory: C:\Users\alireza\Desktop\AlirezaFarashah_98101555

Mode                LastWriteTime         Length Name
----                -
-a-----          5/25/2023   4:52 PM             677 alireza_0x403683B2_public.asc
-a-----          5/25/2023   6:49 PM             215 message.gpg
-a-----          5/25/2023   6:37 PM              37 message.txt

PS C:\Users\alireza\Desktop\AlirezaFarashah_98101555> |

```

در انتها توسط گیرنده message.gpg را رمزگشایی میکنیم.



پ) ابتدا همانطور که در شکل زیر مشاهده می کنید جفت کلید را تولید می کنیم.

OpenPGP

≡+ Import OpenPGP Key

🔑 Generate OpenPGP Keys

✓ Automatically save draft

🔒 alireza.dehghanpour <alireza.dehghanpour@sharif.edu>



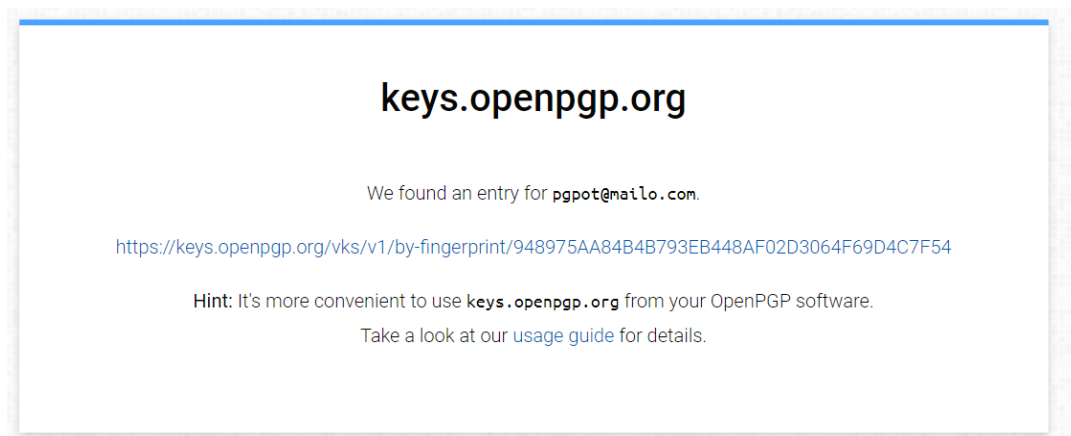
🔑 alireza.dehghanpour <alireza.dehghanpour@sharif.edu> (d5c7ed57363d259b)



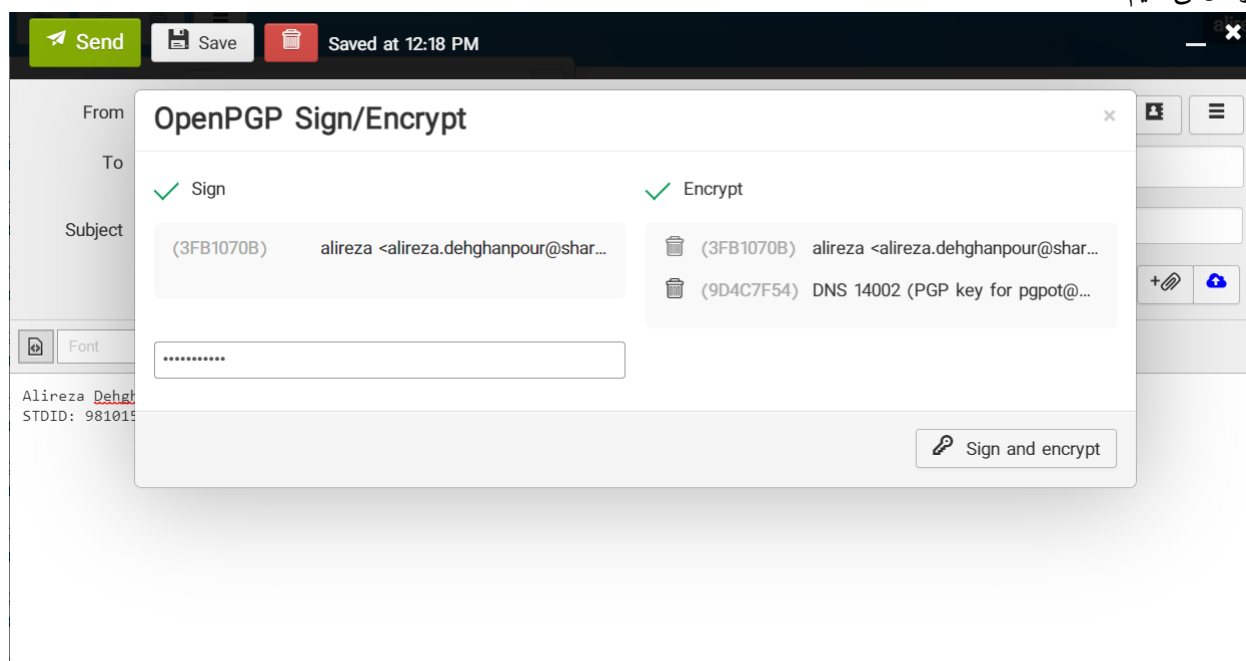
سپس ایمیل خود را ثبت می‌کنیم و در تصویر زیر مشاهده می‌کنید.

The screenshot shows the keys.openpgp.org website. The top navigation bar includes links to trigger, GitHub - pdejorge/..., GitHub - locuslab/f..., alirezafarashah/N-F..., de, and AugOOD/train_ood... The main content area has a white background with a blue border. It displays the text "keys.openpgp.org" and "You uploaded the key 19424D05E7FEA3547291532AD5C7ED57363D259B." Below this, it states "This key is now published with only non-identity information. (What does this mean?)" and "To make the key available for search by email address, you can verify it belongs to you:" followed by the email address "alireza.dehghanpour@sharif.edu" and a "Send Verification Email" button. A note at the bottom says "Note: Some providers delay emails for up to 15 minutes to prevent spam. Please be patient." The bottom section of the screenshot shows the same website with the text "keys.openpgp.org" and "Your key 19424D05E7FEA3547291532AD5C7ED57363D259B is now published for the identity alireza.dehghanpour@sharif.edu."


حال کلید عمومی pgpot را بدست می‌آوریم.




حال ایمیل را می‌سازیم و با کلید خصوصی خود امضا و رمز می‌کنیم سپس با کلید عمومی pgpot رمز می‌کنیم. سپس ایمیل رمز شده را ارسال می‌کنیم.




در ادامه پاسخ را به صورت رمز شده مشاهده می کنید.

 **Re: PGP-98101555**

 **DNS 14012** ✓ (5 Khordaad 1402 12:19 PM)


To: alireza.dehghanpour@sharif.edu




-----BEGIN PGP MESSAGE-----


wcBMAwB21Fb42S96AQf9HEHX6y5xsnTinziKP1y+wlgcAz8yOtFweJqYrk6F5cjX
Adq3ctobktahYynmuelZjiUPELvP3xypVJszuqZUZYHqgOacb2BPFmAc/1pOAmCz
+g74GsfQ1PDqP+xylcU1NxJl1P3ofpWWnqed1eahl8QQTwCK2UaZ4vuEN75At
5fgFBLyG3rq91SJAQ5xBiSrouDj++N/xUeSCZMkqXFFKVZ2/Ln2CZLVDXlIKodiM
BMQT43QK/48reBTDfQOUzUYroT0sEiAO/xRa2nLP9MMPvg140F9d8ry905bsYtE
0q6tK/pblNmkGhzKE+TdpFwSZ8MgmI0RVHXtIRBPxV9LVCVQEE5eer880GQxCuXKI4
AOijueeDgqofglwpR+6MMZUPomHSe2WW3Vlo4HXZZG2o20+blMFTwgSuQopLj46t
7b/Xef61SmvFJctPTNQJt6pfjaDB4UyUBRVROo7vdunrZUOBilQWDYdoJfWJmXA9
5zQttbo2k4homQfU/7uJxza+F6M3UoQ1AfWjurYERfKXCze9k0KEjSUX/0VgmqRV
yVPSCBprym0BKz3nWadB1fn9EL5a48CVx4guSpFVqLl63lYcxvEX1H9uZ/dfmZ2E
Jdh6UJLDXEWB1HIX4BHh5hHJTvdTru4nQ5c0iS0yIHlcf5yya6GidW/4+llj52/q
NCR+xQfFrY+uZ5efD2k16aXpFEjrziBqMJhkmZPcZhGQjZ5ewCAXtYxicOWISpmj
GTPGzWZSS7UHCqv0tF89djNurrvuaLcZwrLL9CBU0qH+vp+1pld6bt2YrHLWpXR
svnzUQRyanOTuR1b7mZMf+Nv+wSYwM20aiN1Ku41T1NDR++FccFN9TBEokLGrEom
BE6iMBBTUyqdg4G79D8VCB8RWJAG2UL408qOZIOJhxfp89i1nsQk2pdgukBwMI9
Sg8zZVtgBtR2TO/T43tyqycF0YpxDPPTHE88jw/w1Frp2bbh3sVExUxkFB3ehTI
KLmhcwcS7h5pK0ZxpQ2FcBFvQMliv0/lyXsOT8L+LNMMfAvi6KLhgaZt0WQIt3yG
vrDRgVYzjH/UQFuF170B0hNoJ2WG3e0dPXh7QrYi6+PmvAZvsfwgHdTKWYb9oGS
7gGLYK1lawM5DCIQ2qU7++s8xeK04kZJOJ6iCVQpCnJrMy2hEZUb79DT05nX/u+3
GGkElcb23oUp6Phvg+C0yR5WD9YwLV8h7/eqdlcYfDINULh4NS2B+UI8v2hzjOSd
5gh0Prj9tzuITFV5nhWMV1YuKfo2Ap6l0nFjgSLiJHuFH1+LS+mhrWWpPqeAB20+
+zk0gQgb/QZ8EgMGfJElz+lkr/XP6fZqkDgco7Pug2gdhjApNCpHmdkesCRhb4dx

حال با کلید خود رمز را باز می کنیم.

 **Re: PGP-98101555**

 **DNS 14012** ✓ (5 Khordaad 1402 12:19 PM)

To: alireza.dehghanpour@sharif.edu



from:alireza.dehghanpour@sharif.edu
body:Alireza Dehghanpour Farashah
STDID: 98101555
time:1685090788
token:LAIKD-9W6OW-KB6W5-0N2WR-L1GI4-MEDIL-DBCYV

(الف)

PGP برای مدیریت دسته کلیدهای عمومی از این مدل استفاده می‌کند که جایگزین زیرساخت توزیع کلید (CA) است. در این مدل با استفاده از تعدادی فیلد که فیلدهای trust نامیده می‌شوند میزان اعتماد به هر کلید را مشخص می‌کند.

(ب)

- Key legitimacy: بیانگر میزان اعتماد فرد به انتساب کلید عمومی به شناسه فرد است.
- Signature trust: هر کلید عمومی دارای چند امضا است و میزان اعتماد به هر یک از این امضاها را signature trust می‌گویند. یعنی درجه‌ی اعتماد به هر یک از این امضاها.
- Owner trust: میزان اعتماد به صاحب کلید برای تایید اعتبار کلید عمومی دیگران.

(پ)

- به کلید خودمان که اعتماد داریم پس YOU معتبر است. همچنین تمامی کلیدهایی که توسط ما امضا شوند معتبر هستند. یعنی A, B, C, D همگی معتبر اند. F نیز چون توسط یک فرد معتمد امضا شده است کلیدش معتبر است. I نیز توسط E و B که هر دو نیمه معتمد هستند امضا شده است پس معتبر است.
- بله زیرا آن وقت H توسط B و E امضا شده است که هر دو نیمه معتمد هستند بنابراین کلید H معتبر خواهد شد.
- بله چون به طور کامل به C اعتماد داریم تمامی کلیدهای امضا شده توسط او معتبر هستند یعنی G نیز معتبر خواهد شد.
- بله زیرا آن وقت فقط توسط E امضا شده است و E یک فرد نیمه معتبر است و چون دیگر I فقط توسط یک فرد نیمه معتبر امضا شده است کلیدش معتبر نیست.
- هرچقدر این یال‌ها بیشتر شود تعداد کلیدهای بیشتری برای ما معتبر خواهد شد زیرا احتمال امضا شدن توسط افراد معتبر و نیمه معتبر بیشتر می‌شود.

سوال سوم

بخش اول

در این سوال از WSL در ویندوز استفاده می‌کنیم. ابتدا بایست 2apache را نصب کرد. سپس وارد دایرکتوری گفته شده رفت و دایرکتوری خواسته شده را ساخت.

```
alirezaf@LAPTOP-E1B871N6: / × + v
alirezaf@LAPTOP-E1B871N6:/$ cd var/www
alirezaf@LAPTOP-E1B871N6:/var/www$ mkdir sharif_98101555
mkdir: cannot create directory 'sharif_98101555': Permission denied
alirezaf@LAPTOP-E1B871N6:/var/www$ sudo mkdir sharif_98101555
alirezaf@LAPTOP-E1B871N6:/var/www$ ls
html sharif_98101555
alirezaf@LAPTOP-E1B871N6:/var/www$ |
```

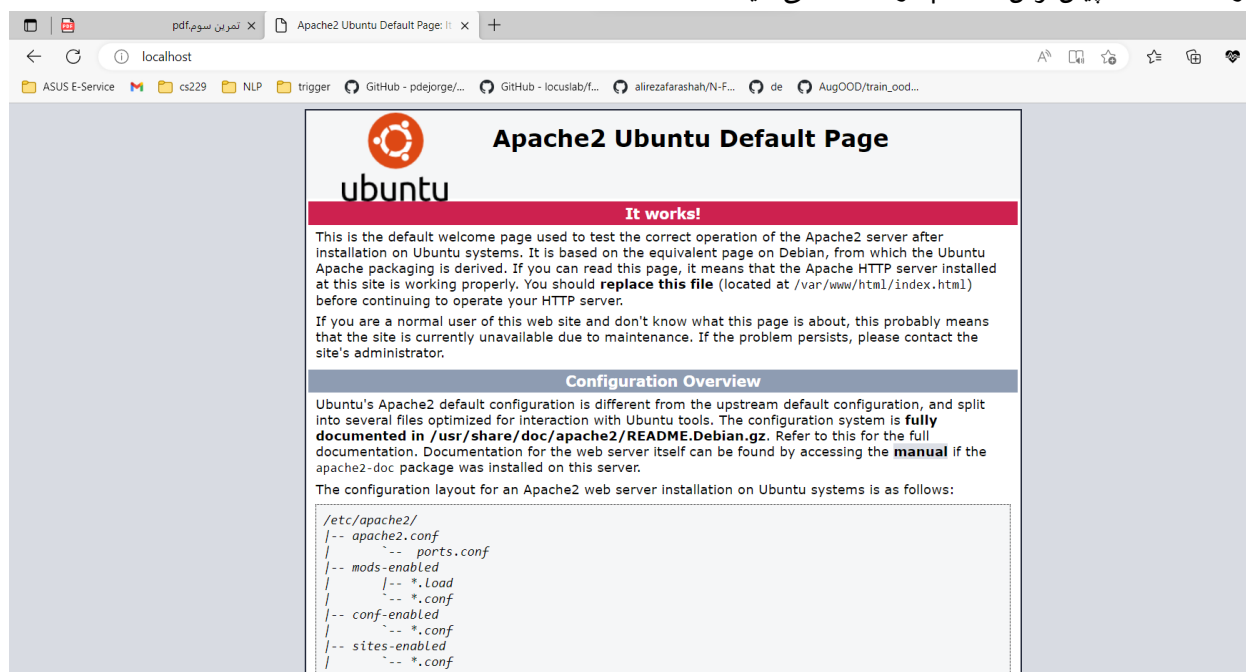
سپس فایل html خواسته شده را ایجاد می‌کنیم.

```
alirezaf@LAPTOP-E1B871N6: / × + v
GNU nano 4.8
<h1>
        DNS-Course-98101555
</h1>
<p>
        Name: Alireza
        <br>
        LastName: Dehghanpour
</p>|
```

سپس port های http و https را در فایروال فعال می کنیم و سپس mod_ssl را فعال می کنیم. و در نهایت سرویس apache را ریستارت می کنیم.

```
alirezaf@LAPTOP-E1B871N6: / x + v
alirezaf@LAPTOP-E1B871N6:/var/www/sharif_98101555$ sudo ufw allow "Apache Full"
Rules updated
Rules updated (v6)
alirezaf@LAPTOP-E1B871N6:/var/www/sharif_98101555$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
alirezaf@LAPTOP-E1B871N6:/var/www/sharif_98101555$ sudo service apache2 restart
* Restarting Apache httpd web server apache2 [ OK ]
alirezaf@LAPTOP-E1B871N6:/var/www/sharif_98101555$ |
```

در ادامه صفحه پیش فرض apache را مشاهده می کنید.



سپس گواهی خود امضا را ایجاد می‌کنیم.

```
root@LAPTOP-E1B871N6: /var X + v
alirezaf@LAPTOP-E1B871N6:/var/www/sharif_98101555$ sudo su
root@LAPTOP-E1B871N6:/var/www/sharif_98101555# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl
/private/apache-xvdemo-selfsigned.key -out /etc/ssl/certs/apache-xvdemo-selfsigned.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/apache-xvdemo-selfsigned.key'
-----
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]:IR
State or Province Name (full name) [Some-State]:Tehran
Locality Name (eg, city) []:Tehran
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DNS
Organizational Unit Name (eg, section) []:DNS-GP1
Common Name (e.g. server FQDN or YOUR name) []:Alireza
Email Address []:alirezafarashah@gmail.com
root@LAPTOP-E1B871N6:/var/www/sharif_98101555# |
```

محتویات این دو فایل گواهی و امضا در شکل زیر قابل مشاهده هستند.

```
root@LAPTOP-E1B871N6: /etc X + v
root@LAPTOP-E1B871N6:/etc/ssl/private# ls -lt apache-xvdemo-selfsigned.key
-rw----- 1 root root 1704 May 26 10:48 apache-xvdemo-selfsigned.key
root@LAPTOP-E1B871N6:/etc/ssl/private# cd /etc/ssl/certs/
t apacheroot@LAPTOP-E1B871N6:/etc/ssl/certs# ls -lt apache-xvdemo-selfsigned.crt
-rw-r--r-- 1 root root 1440 May 26 10:50 apache-xvdemo-selfsigned.crt
root@LAPTOP-E1B871N6:/etc/ssl/certs# |
```

حال باید فایل config را ایجاد کنیم.

```
root@LAPTOP-E1B871N6: /etc X + v
root@LAPTOP-E1B871N6:/etc/ssl/certs# cd /etc/apache2/sites-available
root@LAPTOP-E1B871N6:/etc/apache2/sites-available# vi xvdemo.conf
root@LAPTOP-E1B871N6:/etc/apache2/sites-available# ls
000-default.conf default-ssl.conf xvdemo.conf
root@LAPTOP-E1B871N6:/etc/apache2/sites-available# |
```

```

<VirtualHost *:80>
    ServerAdmin webmaster@www.farashah.com
    DocumentRoot /var/www/sharif_98101555
    ServerName farashah
    <Directory /var/www/sharif_98101555>
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
<VirtualHost *:443>
    ServerName farashah
    DocumentRoot /var/www/sharif_98101555
    <Directory /var/www/sharif_98101555>
        AllowOverride All
        Require all granted
        Allow from All
    </Directory>
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-xvdemo-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-xvdemo-selfsigned.key
</VirtualHost>
~
~

```

سپس سرویس را ریلود می‌کنیم.

```

root@LAPTOP-E1B871N6: /etc  ×  +  ▾
root@LAPTOP-E1B871N6:/etc/apache2/sites-available# cd ..
root@LAPTOP-E1B871N6:/etc/apache2# a2ensite xvdemo.conf
Enabling site xvdemo.
To activate the new configuration, you need to run:
    service apache2 reload
root@LAPTOP-E1B871N6:/etc/apache2# cd sites-enabled
root@LAPTOP-E1B871N6:/etc/apache2/sites-enabled# ll
total 8
drwxr-xr-x 2 root root 4096 May 26 11:10 ./
drwxr-xr-x 8 root root 4096 May 26 10:04 ../
lrwxrwxrwx 1 root root 35 May 26 10:04 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 30 May 26 11:10 xvdemo.conf -> ../sites-available/xvdemo.conf
root@LAPTOP-E1B871N6:/etc/apache2/sites-enabled# systemctl reload apache2
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
root@LAPTOP-E1B871N6:/etc/apache2/sites-enabled# service apache2 reload
 * Reloading Apache httpd web server apache2
 *
root@LAPTOP-E1B871N6:/etc/apache2/sites-enabled# |

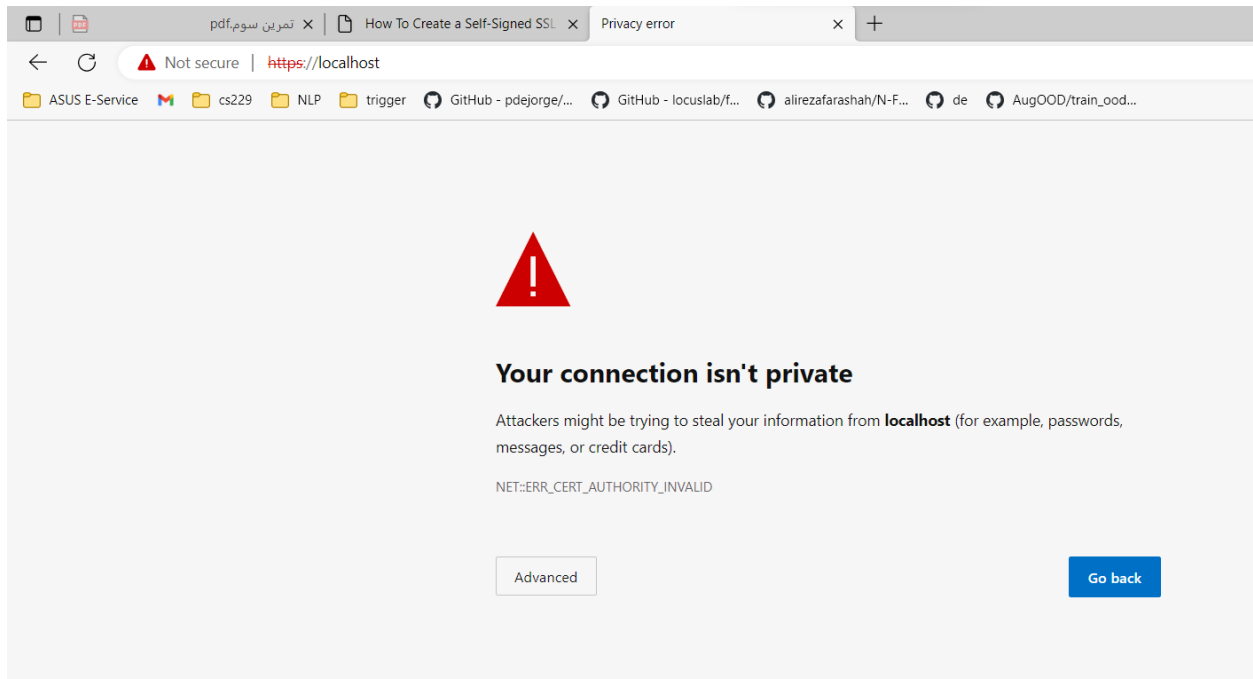
```

حال باید hosts entry خود ایجاد کنیم.

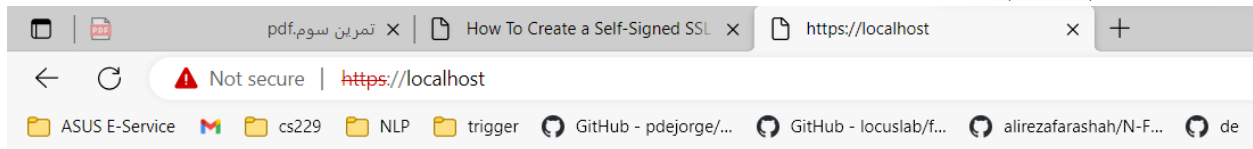
```
# This file was automatically generated by WSL. To stop automatic
tc/wsl.conf:
# [network]
# generateHosts = false
127.0.0.1      farashah
127.0.0.1      localhost
127.0.1.1      LAPTOP-E1B871N6.      LAPTOP-E1B871N6
0.0.0.0 bs.studycoder.com
0.0.0.0 bi.studycoder.com
0.0.0.0 bs.studycoder.com
0.0.0.0 bi.studycoder.com
0.0.0.0 bs.studycoder.com
0.0.0.0 bi.studycoder.com

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
~
```

ابتدا چون گواهی خود امضا است مرورگر وارد نمی‌شود.



ولی اگر وارد شویم خواهیم داشت:



DNS-Course-98101555

Name:Alireza
LastName:Dehghanpour

در تصویر زیر می‌توانید گواهی را مشاهده کنید.

Certificate Viewer: Alireza

General Details

Issued To

Common Name (CN)	Alireza
Organization (O)	DNS
Organizational Unit (OU)	DNS-GP1

Issued By

Common Name (CN)	Alireza
Organization (O)	DNS
Organizational Unit (OU)	DNS-GP1

Validity Period

Issued On	Friday, May 26, 2023 at 9:50:04 AM
Expires On	Saturday, May 25, 2024 at 9:50:04 AM

Fingerprints

SHA-256 Fingerprint	67 75 12 96 AC C4 37 FA 8A 2E FE 38 BE 76 1D CA 7B BC 9C 66 FF 5A 3E DE 7F 20 C8 22 2A C0 EC A3
SHA-1 Fingerprint	1C DB 4A 7E 7E 42 A3 A0 E8 BC A1 F0 57 05 47 F6 B9 16 54 27

بخش دوم

در این بخش باید در فایل config یک سری دستورات را قرار دهیم.

- برای عدم پشتیبانی از ورژن‌های آسیب‌پذیر:

```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

- برای اولویت دادن به ترجیحات مجموعه رمزنگاری سرور از دستور زیر استفاده می‌کنیم:

```
SSLHonorCipherOrder on
```

- برای غیرفعال کردن فشرده‌سازی:

```
SSLCompression off
```

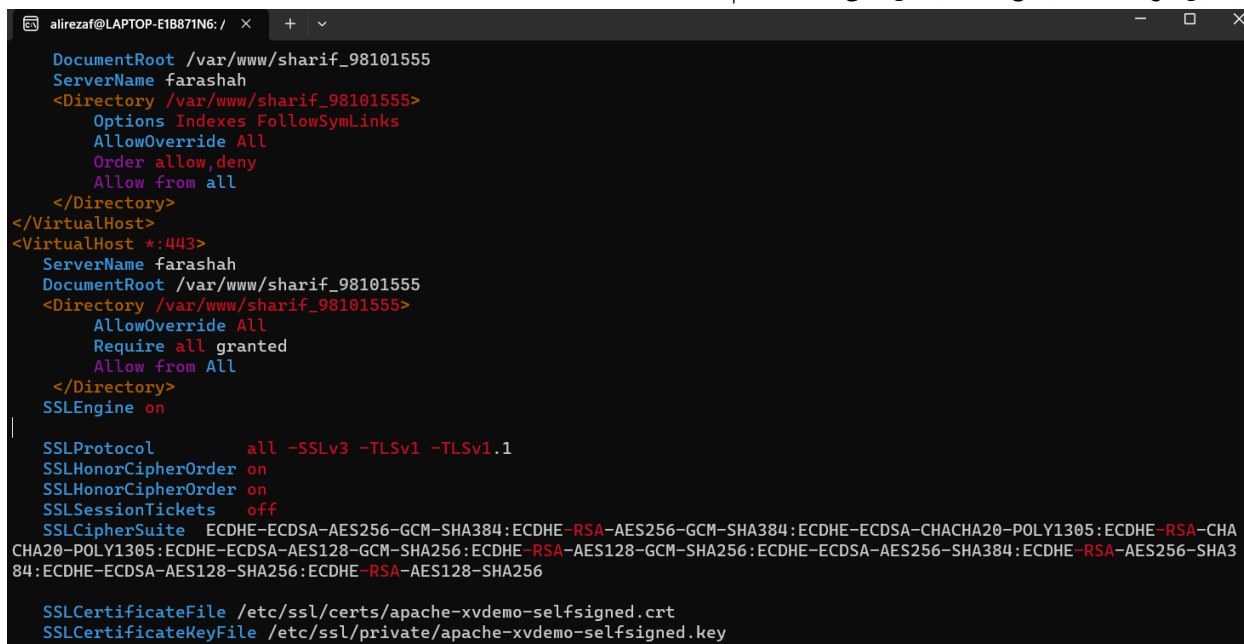
- دستوری که نقض شدن محرمانگی پیش‌رو جلوگیری می‌کند:

```
SSLSessionTickets off
```

- دستوری که سبب شود سرور از رمزنگاری‌های قوی استفاده کند.

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
```

باید این موارد را در فایل config بخش قبلی اضافه کنیم.



```
alirezaf@LAPTOP-E1B871N6: /
DocumentRoot /var/www/sharif_98101555
ServerName farashah
<Directory /var/www/sharif_98101555>
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
</VirtualHost>
<VirtualHost *:443>
    ServerName farashah
    DocumentRoot /var/www/sharif_98101555
    <Directory /var/www/sharif_98101555>
        AllowOverride All
        Require all granted
        Allow from All
    </Directory>
    SSLEngine on

    SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
    SSLHonorCipherOrder on
    SSLHonorCipherOrder on
    SSLSessionTickets off
    SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHA
    CHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA3
    84:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256

    SSLCertificateFile /etc/ssl/certs/apache-xvdemo-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-xvdemo-selfsigned.key
```

سوال چهارم

(الف)

اگر در مود AH باشیم چون IP فرستنده و گیرنده در محاسبه‌ی MAC دخیل است دچار مشکل می‌شویم. اما برای VPN از مود تونل در ESP استفاده می‌شود که در آن آدرس مبدا و مقصد دروازه‌های خروجی به بسته اضافه می‌شوند. همچنین اگر از مود انتقال در ESP استفاده بخواهد شود چون سرآیند IP تغییر نمی‌کند نمی‌توان host to host استفاده کرد.

(ب)

$$Total\ time = 25000\ \mu s + \frac{1024\ byte}{16\ byte} \cdot 0.25\ \mu s = 25016\ \mu s$$

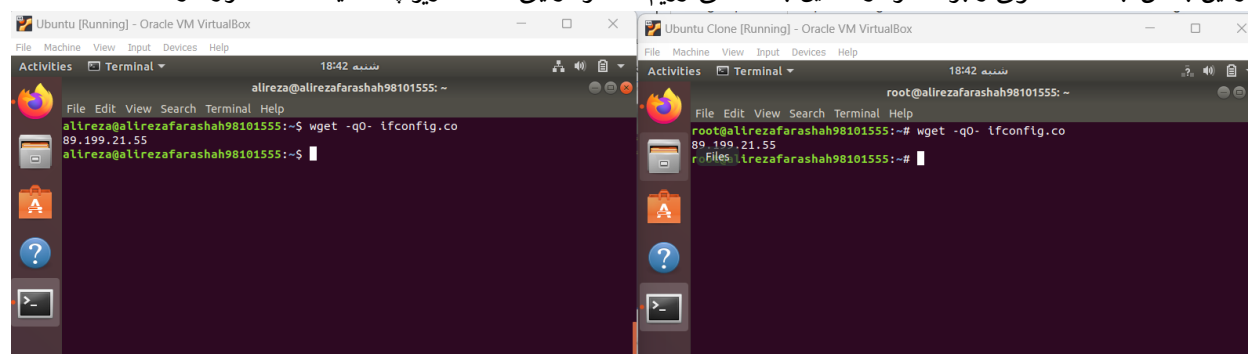
$$BandWidth = \frac{1024\ byte}{25016\ \mu s} = 40933\ byte/seconds$$

(پ)

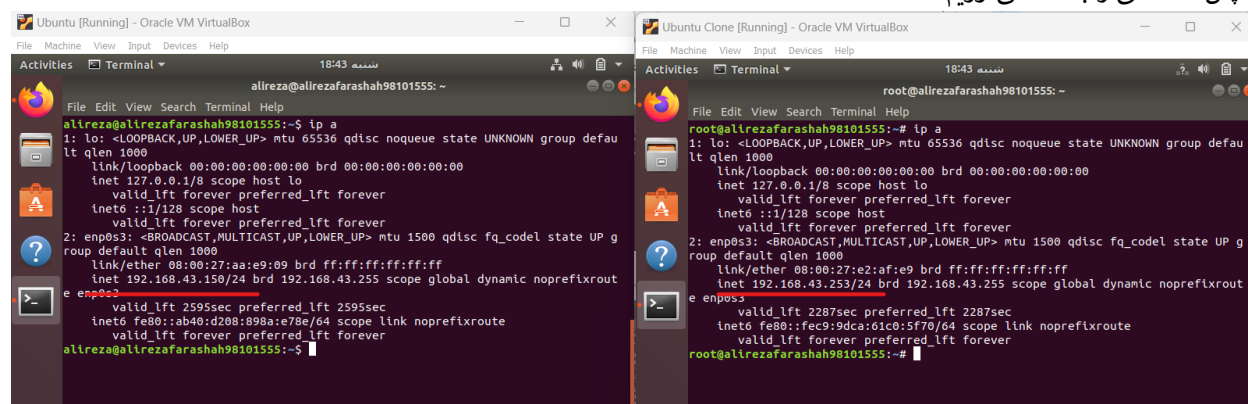
برای این سوال مراحل را از این لینک جلو می‌بریم.

<https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-debian-ubuntu/>

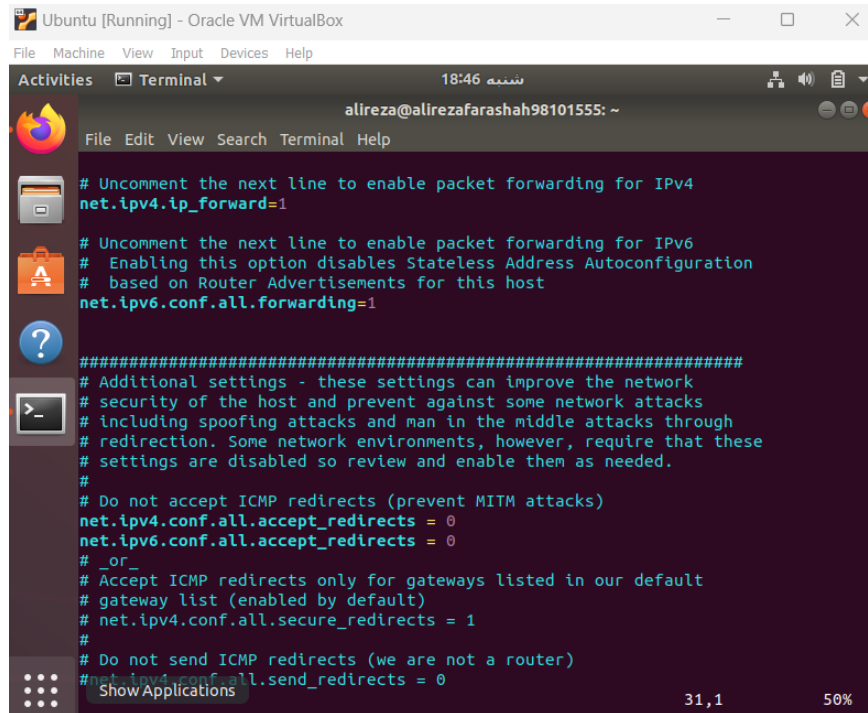
در این بخش ابتدا IP عمومی را برای هر دو ماشین بدست می‌آوریم که هر دو یکی هستند زیرا پشت یک NAT قرار دارند.



سپس IP محلی را بدست می‌آوریم.



در گام بعدی باید packet forwarding را فعال کنیم.



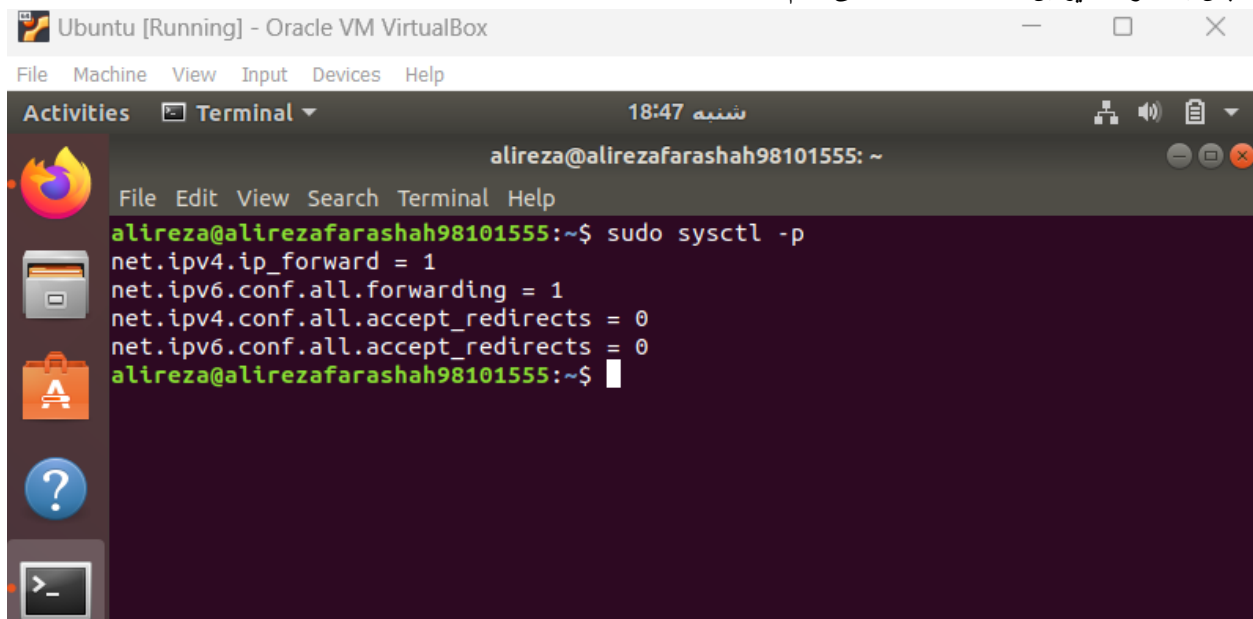
```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 18:46 شنبه
alireza@alirezafarashah98101555: ~
File Edit View Search Terminal Help

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
net.ipv4.conf.all.send_redirects = 0
Show Applications 31,1 50%
```

سپس به صورت زیر این تنظیمات را load می کنیم.



```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 18:47 شنبه
alireza@alirezafarashah98101555: ~
File Edit View Search Terminal Help

alireza@alirezafarashah98101555:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
alireza@alirezafarashah98101555:~$
```

سپس ابزار Strongswan را با دستور `sudo apt install strongswan` برای هر دو ماشین نصب می کنیم.
سپس بررسی می کنیم این سرویس فعال باشد.

```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 23:44 جمعه
alireza@alirezafarashah98101555: ~
File Edit View Search Terminal Help
alireza@alirezafarashah98101555:~$ sudo systemctl is-enabled strongswan.service
enabled
alireza@alirezafarashah98101555:~$ sudo systemctl status strongswan.service
● strongswan.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
   Loaded: loaded (/lib/systemd/system/strongswan.service; enabled; vendor pres
   Active: active (running) since Fri 2023-05-26 23:35:36 +0430; 8min ago
   Main PID: 4099 (starter)
     Tasks: 18 (limit: 4664)
    CGroup: /system.slice/strongswan.service
            └─4099 /usr/lib/ipsec/starter --daemon charon --nofork
              4129 /usr/lib/ipsec/charon

مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[CFG] loading aa certif
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[CFG] loading ocsip sign
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[CFG] loading attribute
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[CFG] loading crls from
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[CFG] loading secrets f
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[LIB] loaded plugins: c
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[LIB] dropped capabilit
مجموعه 26 23:35:37 alirezafarashah98101555 charon[4129]: 00[JOB] spawning 16 worke
مجموعه 26 23:35:37 alirezafarashah98101555 ipsec[4099]: charon (4129) started afte
مجموعه 26 23:35:37 alirezafarashah98101555 ipsec_starter[4099]: charon (4129) star
lines 1-19/19 (END)
alireza@alirezafarashah98101555:~$ s

```

حالا باید تنظیمات امنیتی تونل را در فایل ipsec.conf تعیین کنیم.

```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 19:06 شنبه
alireza@alirezafarashah98101555: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/ipsec.conf
config setup
    charondebug="all"
    uniqueids=yes
conn devgateway-to-prodgateway
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=192.168.43.150
    leftsubnet=192.168.43.0/24
    right=192.168.43.253
    rightsubnet=192.168.43.0/24
    ike=aes256-sha1-modp1024!
    esp=aes256-sha1!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart

```

```

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 19:06 شنبه
root@alirezafarashah98101555: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/ipsec.conf
config setup
    charondebug="all"
    uniqueids=yes
conn devgateway-to-prodgateway
    type=tunnel
    auto=start
    keyexchange=ikev2
    authby=secret
    left=192.168.43.253
    leftsubnet=192.168.43.0/24
    right=192.168.43.150
    rightsubnet=192.168.43.0/24
    ike=aes256-sha1-modp1024!
    esp=aes256-sha1!
    aggressive=no
    keyingtries=%forever
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=30s
    dpdtimeout=120s
    dpdaction=restart

```

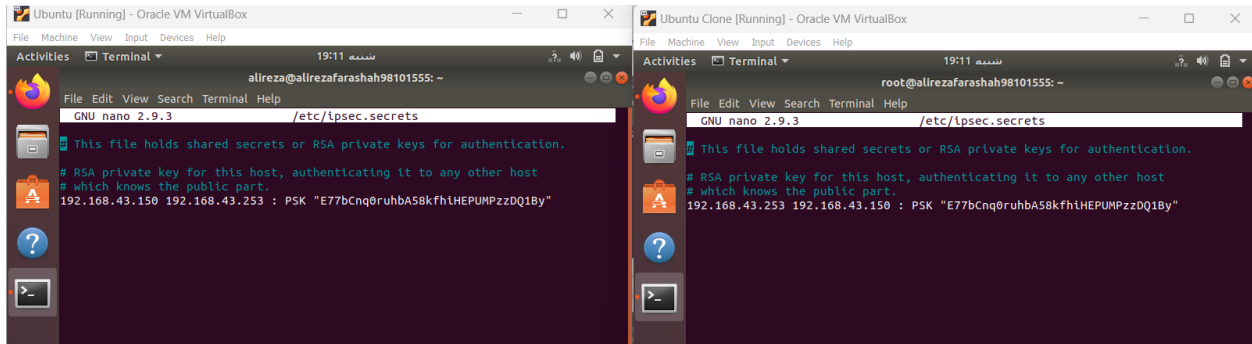
حال باید یک Pre-shared Key برای ارتباط تنظیم کنیم.

```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 00:08 شنبه
alireza@alirezafarashah98101555: ~
File Edit View Search Terminal Help
alireza@alirezafarashah98101555:~$ head -c 24 /dev/urandom | base64
E77bCnq0ruhBA58kfHlHEPUMPzzDQ18y
alireza@alirezafarashah98101555:~$

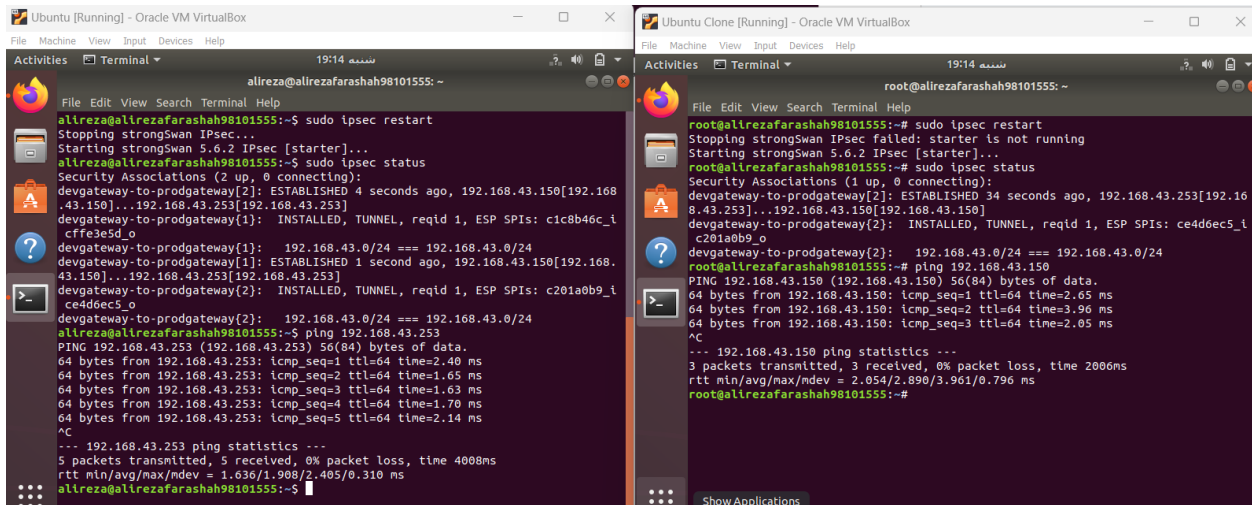
```

حال باید این مقدار را در `ipsec.secrets` قرار دهیم.



```
alireza@alirezafarashah98101555: ~  
GNU nano 2.9.3 /etc/ipsec.secrets  
# This file holds shared secrets or RSA private keys for authentication.  
# RSA private key for this host, authenticating it to any other host  
# which knows the public part.  
192.168.43.150 192.168.43.253 : PSK "E77bcnq0ruhba58kfhLHEPUMPzzDQ1By"  
root@alirezafarashah98101555: ~  
GNU nano 2.9.3 /etc/ipsec.secrets  
# This file holds shared secrets or RSA private keys for authentication.  
# RSA private key for this host, authenticating it to any other host  
# which knows the public part.  
192.168.43.253 192.168.43.150 : PSK "E77bcnq0ruhba58kfhLHEPUMPzzDQ1By"
```

حال `ipsec` را ریستارت می کنیم و وضعیت ارتباط را مشاهده می کنیم و دو طرف یکدیگر را ping می کنند.



```
alireza@alirezafarashah98101555: ~  
alireza@alirezafarashah98101555:~$ sudo ipsec restart  
Stopping strongSwan IPsec...  
Starting strongSwan 5.6.2 IPsec [starter]...  
alireza@alirezafarashah98101555:~$ sudo ipsec status  
Security Associations (2 up, 0 connecting):  
devgateway-to-prodgateway[2]: ESTABLISHED 4 seconds ago, 192.168.43.150[192.168.43.150]...192.168.43.253[192.168.43.253]  
devgateway-to-prodgateway[1]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c1c8b46c_l cfe3e5d_o  
devgateway-to-prodgateway[1]: 192.168.43.0/24 == 192.168.43.0/24  
devgateway-to-prodgateway[1]: ESTABLISHED 1 second ago, 192.168.43.150[192.168.43.150]...192.168.43.253[192.168.43.253]  
devgateway-to-prodgateway[2]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c201a0b9_l ce4d6ec5_o  
devgateway-to-prodgateway[2]: 192.168.43.0/24 == 192.168.43.0/24  
alireza@alirezafarashah98101555:~$ ping 192.168.43.253  
PING 192.168.43.253 (192.168.43.253) 56(84) bytes of data.  
64 bytes from 192.168.43.253: icmp_seq=1 ttl=64 time=2.40 ms  
64 bytes from 192.168.43.253: icmp_seq=2 ttl=64 time=1.65 ms  
64 bytes from 192.168.43.253: icmp_seq=3 ttl=64 time=1.63 ms  
64 bytes from 192.168.43.253: icmp_seq=4 ttl=64 time=1.70 ms  
64 bytes from 192.168.43.253: icmp_seq=5 ttl=64 time=2.14 ms  
^C  
--- 192.168.43.253 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4008ms  
rtt min/avg/max/mdev = 1.636/1.908/2.405/0.310 ms  
alireza@alirezafarashah98101555:~$  
root@alirezafarashah98101555: ~  
root@alirezafarashah98101555:~# sudo ipsec restart  
Stopping strongSwan IPsec failed: starter is not running  
Starting strongSwan 5.6.2 IPsec [starter]...  
root@alirezafarashah98101555:~# sudo ipsec status  
Security Associations (1 up, 0 connecting):  
devgateway-to-prodgateway[2]: ESTABLISHED 34 seconds ago, 192.168.43.253[192.168.43.253]...192.168.43.150[192.168.43.150]  
devgateway-to-prodgateway[2]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: ce4d6ec5_l c201a0b9_o  
devgateway-to-prodgateway[2]: 192.168.43.0/24 == 192.168.43.0/24  
root@alirezafarashah98101555:~# ping 192.168.43.150  
PING 192.168.43.150 (192.168.43.150) 56(84) bytes of data.  
64 bytes from 192.168.43.150: icmp_seq=1 ttl=64 time=2.65 ms  
64 bytes from 192.168.43.150: icmp_seq=2 ttl=64 time=3.96 ms  
64 bytes from 192.168.43.150: icmp_seq=3 ttl=64 time=2.05 ms  
^C  
--- 192.168.43.150 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2006ms  
rtt min/avg/max/mdev = 2.054/2.890/3.961/0.796 ms  
root@alirezafarashah98101555:~#
```