EMİRCAN KILIÇASLAN
ÖZLEM KILIÇKIRAN
CTIS 496 HW1

i) TABLE

Name	Email Address	Key id	fingerprint
Özlem	ozlem.kilickiran@ug.bilkent.edu.tr	31802677	E1A210AE0875FF9C3 75C3E1BEB19172331 802677
Emircan	emircan@ug.bilkent.edu.tr	427FCB6C	EFD3 5493 4BC4 3F63 2961 1034 D203 9FC3 427F CB6C

ii)

Özlem's Screen

```
[keyboxd]
---------
pub   rsa4096 2025-03-14 [SC]
      E1A210AE0875FF9C375C3E1BEB19172331802677
uid           [ultimate] ozlem (-) <ozlem.kilickiran@ug.bilkent.edu.tr>
sub   rsa4096 2025-03-14 [E]
      AB5AED00A9D2C81B9BD5987CAB8E4D13A04331C5

pub   rsa4096 2025-03-11 [SC] [expires: 2028-03-10]
      EFD354934BC43F6329611034D2039FC3427FCB6C
uid           [ unknown] Emircan K\xc4\xb1l\xc4\xb1◆aslan <emircan@ug.bilkent.edu.tr>
sub   rsa4096 2025-03-11 [E] [expires: 2028-03-10]
      6B3B99C27501B6866458CF98CB960D3418E67BE8
```

Emircan's Screen

```
pub   rsa4096 2025-03-14 [SC]
      E1A210AE0875FF9C375C3E1BEB19172331802677
uid [    bilinmeyen    ] ozlem (-) <ozlem.kilickiran@ug.bilkent.edu.tr>
sub   rsa4096 2025-03-14 [E]

pub   rsa4096 2025-03-11 [SC] [son kullanma tarihi: 2028-03-10]
      EFD354934BC43F6329611034D2039FC3427FCB6C
uid [     tamamen      ] Emircan Kılıçaslan <emircan@ug.bilkent.edu.tr>
sub   rsa4096 2025-03-11 [E] [son kullanma tarihi: 2028-03-10]
```

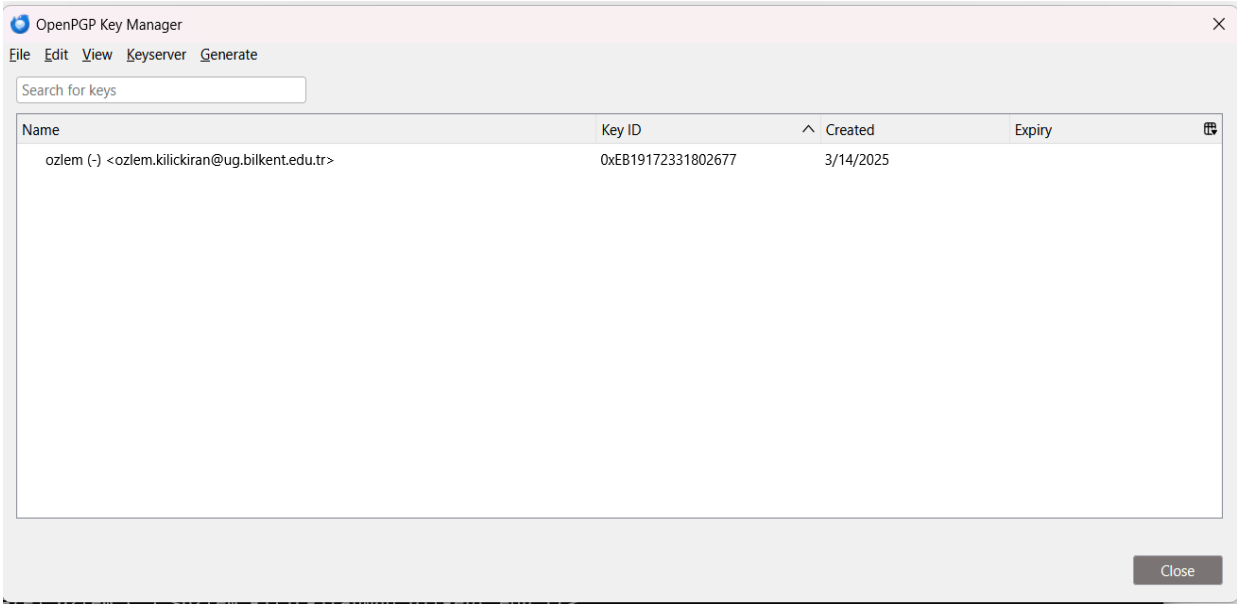
Özlem’s Public Key to Keyserver on https://pgp.circl.lu/

Emircan’s Public Key to Keyserver on https://pgp.circl.lu/

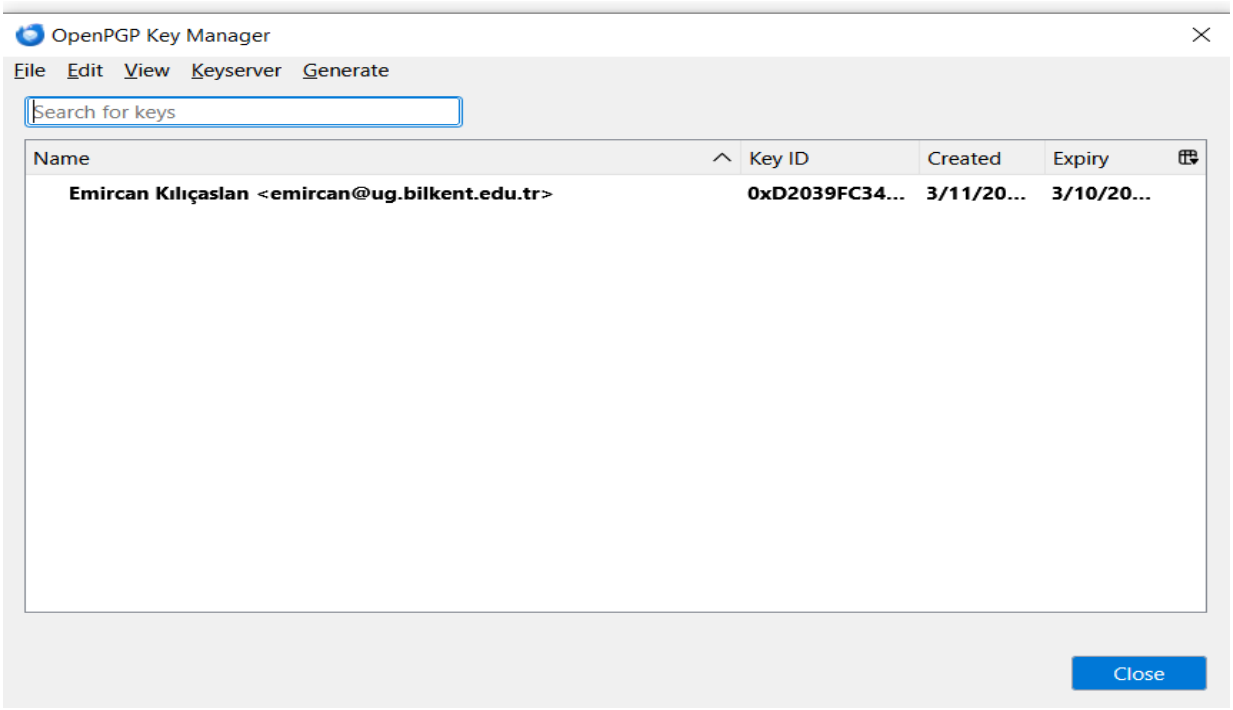
```
pub rsa4096/efd354934bc43f6329611034d2039fc3427fcb6c 2025-03-11T12:46:10Z
        Hash=23b981b350c93359b13fa9e2f57516ba

uid Emircan Kılıçaslan <emircan@ug.bilkent.edu.tr>
sig  sig  d2039fc3427fcb6c 2025-03-11T12:46:11Z 2028-03-10T12:46:10Z _____ [selfsig]



sub rsa4096/6b3b99c27501b6866458cf98cb960d3418e67be8 2025-03-11T12:46:12Z
sig sbind d2039fc3427fcb6c 2025-03-11T12:46:13Z _____ 2028-03-10T12:46:10Z []
```

iii)

Ozlem’s screen:

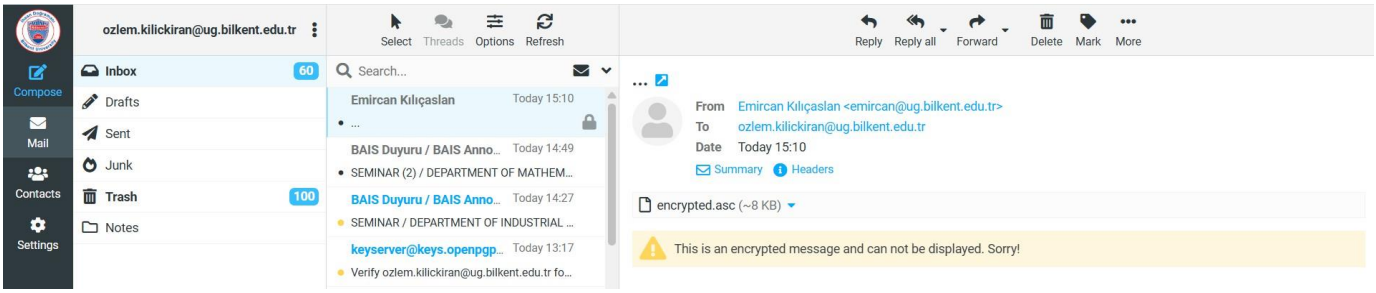


Emircan’s Screen

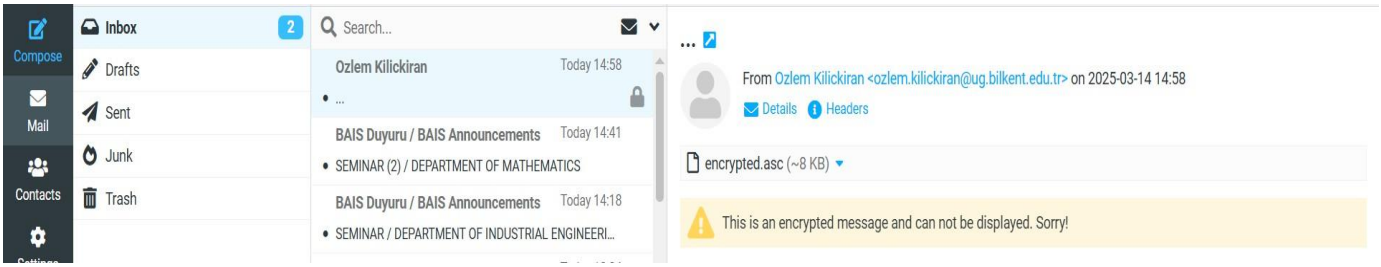


iv)

Özlem’s Screen



Emircan’s Screen



v) **Security Goals Provided by PGP**

1. Confidentiality

PGP ensures the confidentiality of data by encrypting the email message so that it can only be read by the intended recipient. The sender encrypts the email content using the recipient’s public key, ensuring that only the recipient can decrypt the message with their private key. This ensures that the message remains confidential and prevents third parties from reading the email.

2. Integrity

PGP ensures the integrity of the message by using digital signatures. The sender computes a **hash value** of the message and signs it using their private key. The recipient can verify the signature using the sender’s public key. If the message content is altered in any way, the digital signature becomes invalid, allowing the recipient to detect the change. This ensures the integrity of the message.

3. Authentication

PGP provides authentication by using digital signatures to verify the identity of the sender. When the sender signs the message with their private key, the recipient can verify the authenticity of the sender using the sender's public key. This confirms that the message was indeed sent by the claimed sender and not someone else impersonating them.

vi)

User	Key Type	Used by User	Used by Other Member to Verify/Decrypt
Özlem	Public Key	No	Emircan uses Özlem's public key to verify the signature and decrypt the message
Özlem	Private Key	Yes	Özlem uses her private key to sign and encrypt the message
Emircan	Public Key	No	Özlem uses Emircan’s public key to encrypt the message
Emircan	Private Key	Yes	Emircan uses his private key to decrypt the message and verify Aylin’s signature

Explanation:

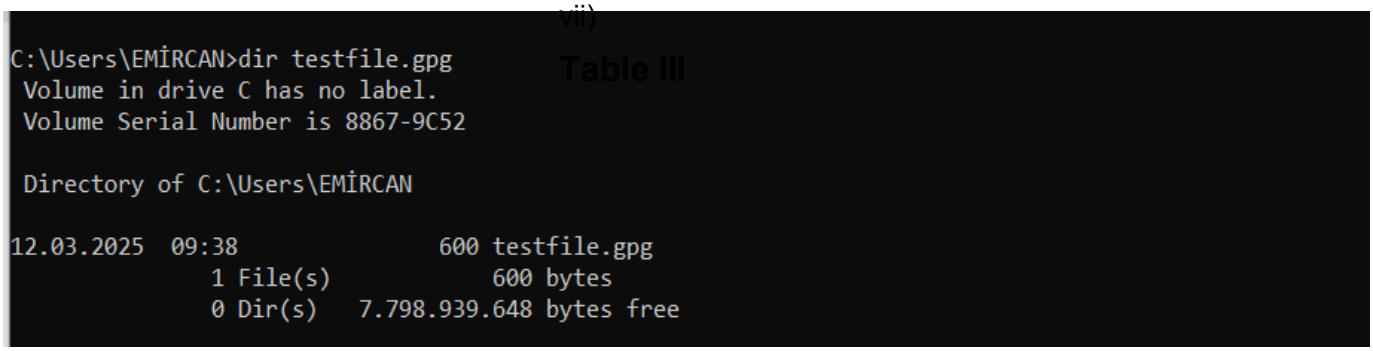
- **Emircan Kılıçaslan's Private Key**: Emircan uses his private key to sign and encrypt the message.
- **Özlem Kılıçkıran's Public Key**: Emircan uses Özlem's public key to encrypt the message for Özlem.
- **Emircan Kılıçaslan's Public Key**: Özlem uses Emircan's public key to verify the signature and decrypt the message.
- **Özlem Kılıçaslan's Private Key**: Özlem uses her private key to decrypt the message and verify Emircan's signature.

Emircan	gpg --encrypt --recipient ozlem.kilickiran@ug.bilkent.edu.tr --output testfile.gpg testfile.txt	This command encrypts testfile.txt using Özlem's public key and outputs testfile.gpg
Özlem	gpg --encrypt --recipient emircan@ug.bilkent.edu.tr --output testfile.gpg testfile.txt	This command encrypts testfile.txt using Emircan's public key and outputs testfile.gpg

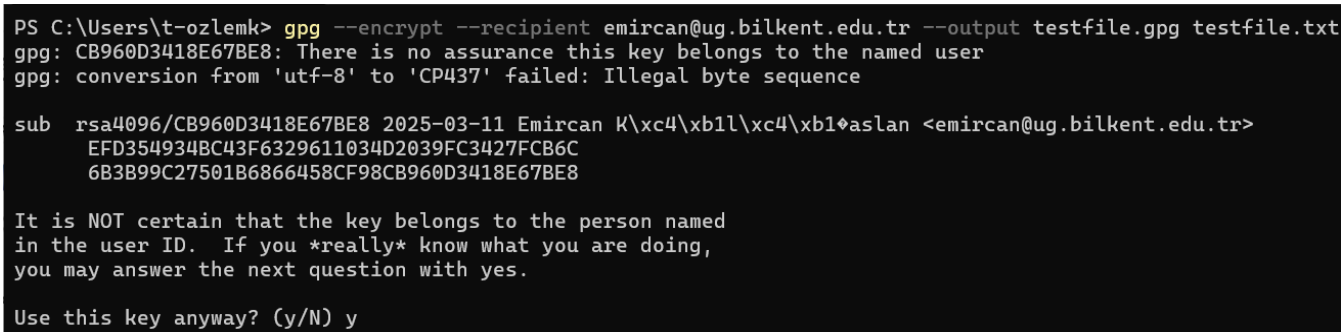
Emircan's Screen

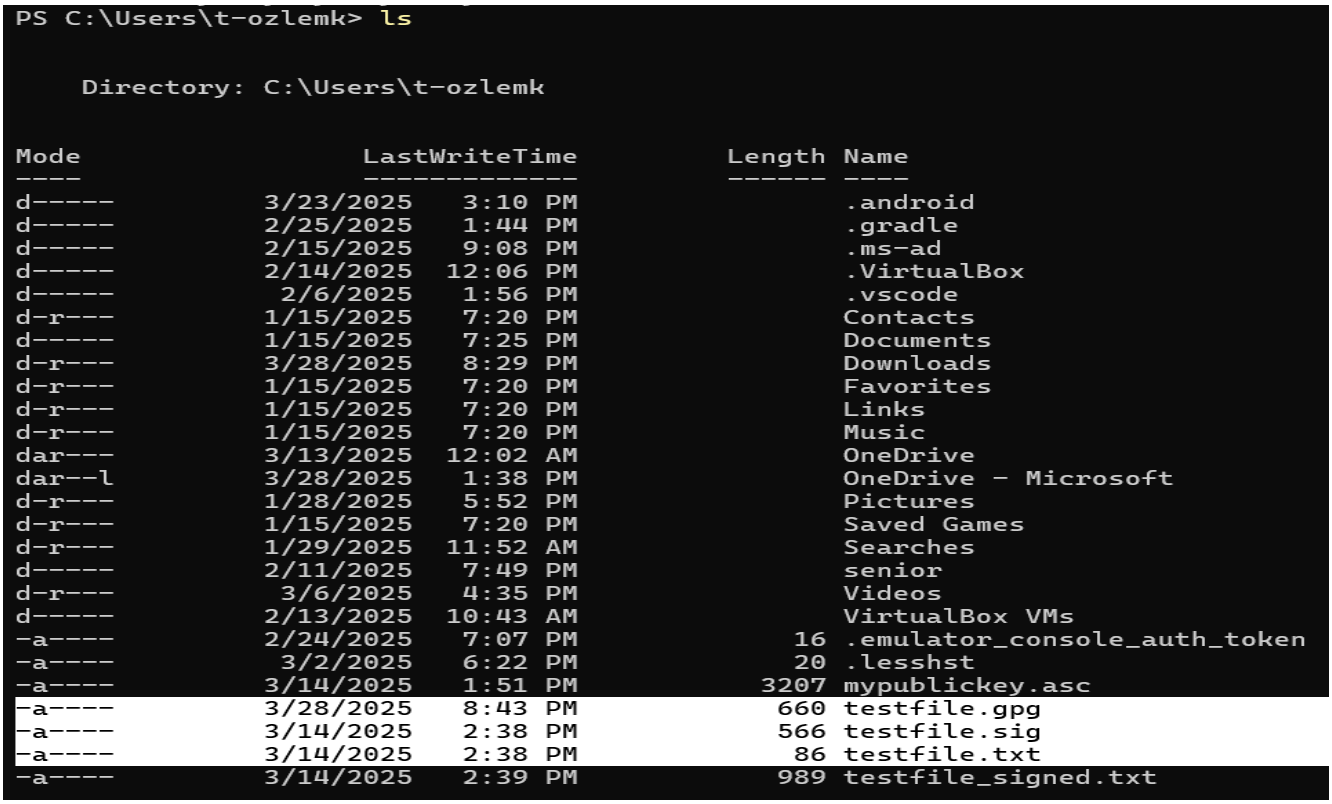
vii)

Table III



Özlem's Screen





```
PS C:\Users\t-ozlemk> ls


    Directory: C:\Users\t-ozlemk


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/23/2025   3:10 PM                .android
d-----         2/25/2025   1:44 PM                .gradle
d-----         2/15/2025   9:08 PM                .ms-ad
d-----         2/14/2025  12:06 PM                .VirtualBox
d-----          2/6/2025   1:56 PM                .vscode
d-r---         1/15/2025   7:20 PM                Contacts
d-----         1/15/2025   7:25 PM                Documents
d-r---         3/28/2025   8:29 PM                Downloads
d-r---         1/15/2025   7:20 PM                Favorites
d-r---         1/15/2025   7:20 PM                Links
d-r---         1/15/2025   7:20 PM                Music
dar---         3/13/2025  12:02 AM                OneDrive
dar--l         3/28/2025   1:38 PM                OneDrive - Microsoft
d-r---         1/28/2025   5:52 PM                Pictures
d-r---         1/15/2025   7:20 PM                Saved Games
d-r---         1/29/2025  11:52 AM                Searches
d-----         2/11/2025   7:49 PM                senior
d-r---          3/6/2025   4:35 PM                Videos
d-----         2/13/2025  10:43 AM                VirtualBox VMs
-a----         2/24/2025   7:07 PM             16 .emulator_console_auth_token
-a----          3/2/2025   6:22 PM             20 .lesshst
-a----         3/14/2025   1:51 PM           3207 mypublickey.asc
-a----         3/28/2025   8:43 PM            660 testfile.gpg
-a----         3/14/2025   2:38 PM            566 testfile.sig
-a----         3/14/2025   2:38 PM             86 testfile.txt
-a----         3/14/2025   2:39 PM            989 testfile_signed.txt
```

viii)

User	Command	Explanation
Emircan	gpg --output decrypted_testfile.txt --decrypt testfile.gpg	This decrypts the file `encrypted_testfile.txt.gpg` using Emircan's private key and outputs the result to `decrypted_testfile.txt`

		.
Özlem	gpg --output decrypted_testfile.txt --decrypt testfile.gpg	This decrypts the file `encrypted_testfile.txt.gpg` using Özlem's private key and outputs the result to `decrypted_testfile.txt`

IX)

gpg --armor --output signed_testfile.asc --sign testfile.txt
gpg --armor --output signed_testfile.asc --sign testfile.txt

Emircan's Screen:

```
C:\Users\EMİRCAN>gpg --list-packets signed_testfile.asc
# off=0 ctb=a3 tag=8 hlen=1 plen=0 indeterminate
:compressed packet: algo=1
# off=2 ctb=90 tag=4 hlen=2 plen=13
:onepass_sig packet: keyid 38F48EF5338CBAA3
        version 3, sigclass 0x00, digest 10, pubkey 22, last=1
# off=17 ctb=cb tag=11 hlen=2 plen=18 new-ctb
:literal data packet:
        mode b (62), created 1741954839, name="testfile.txt",
        raw data: 0 bytes
# off=37 ctb=88 tag=2 hlen=2 plen=117
:signature packet: algo 22, keyid 38F48EF5338CBAA3
        version 4, created 1741954839, md5len 0, sigclass 0x00
        digest algo 10, begin of digest a1 c2
        hashed subpkt 33 len 21 (issuer fpr v4 272A761DBBEF54D21599692C38F48EF5338CBAA3)
        hashed subpkt 2 len 4 (sig created 2025-03-14)
        subpkt 16 len 8 (issuer key ID 38F48EF5338CBAA3)
        data: [256 bits]
        data: [255 bits]
```

```
C:\Users\EMİRCAN>gpg --armor --export 427FCB6C
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGfQMJIBEACYfotKLLaw4fJg74DFA4JOmHhyN0t5K6/161z4BCNxtevC+5/S
P30tqE0XXX/ES5mcbXDpJeDo0POv9G/JcB82tzGOzaA5ngWRGr29tiJaoOz9HN2O
S7wNi5vGrMWvM6z/Ro2H9zfPYyRIM4hKBBqn5u+A9ODbC6HvAr+4rhbWUakbjKI6
alnk16F5rR2r+BFe5yF1gIkzQRiWECrBTHJfAwA4cm/2H7lnoX9dhDiAALK9I6eW
3e2PG8IEYvURI/a6v3eiVZUQsLL272PvhKIiI8o+2YjHNjLQWILzrh4OtpQicu5m
1Q8muFKFMxOxJNrQZIlYS6795uUbtgm/yHY2nGufZPNGF1h4C9Z5ccKhUt4845M0
ZDHZRTPnvP0LTC7rmRaq4h+Y1TvrWc23jhWQ6+i8iUwrX4en5VKVySmgnCJwCGZa
T6ZCO6Vav0hP26dGja8mCTdpCeaoKI3dSSNHHzB/XUDleEa9LQTD4zMeBEixurEw
Z8PSp23NrogQGJllupMIFjRGH91fRxaCbK0KvaZu7FjMYrvioT8xqpjos43/s34t
Y66abSLqy9HTvGRIPP6kvdJIkMs4MjyWVGFlTke8rL49bnEepf3yDWXHGzp87H7I
8+DGlIRYB427FIL+430DJbLV6DCoE0ocJPo+UEGCG6TuXnHyrxR9T5uEqwARAQAB
tDFFbWlyY2FuIEvEsWzEscOnYXNsYW4gPGVtaXJjYW5AdWcuYmlsa2VudC5lZHUu
dHI+iQJNBBMBCAA3FiEE79NUk0vEP2MpYRA00gOfw0J/y2wFAmfQMJMFCQWjmoAC
GwMECwkIBwUVCAkKCwUWAgMBAAAKCRDSA5/DQn/LbERTD/911Cmd5F+99ODs67jS
A9vEpEVifC9N4yQApswsk2MhjQh5fHmmo6MGlEDyR3eR5zQL82nhEfgP0xgOVqvu
OT2j/5xP3cj8lgAAK/vaBCOHcWSDv8HtZIIU9F+WLqhceo+xsxg/F9kR+bhet58U
dxr3cZrNIXR+QH5CKy0IOCj1Sj+D4tAl+++3NJ7VgWcRqMTKdgbgacqdxe7SGTmU
KIPy9a0j8gQznEeqJ2WLaFgIEpAPEETYTJFidqAhUZFHbtqc2NG21QDEEU8arvdp
kVKbpxGQIWf6LqyO7H467XAJitG9yK2UjAa+zIwyIXCWNip7m/GGCWosePK/fBsp
tHg7nzzmFN4DtB1MzUmw+XcF+x84BK0c1RfjcTPIQmO3WDiJz64b2Be8tl//OtgQ
mfKQ88cgZQPKH07DCEV8VnIoOki6xHsOSTeDx4pTqDDcNImq3dVwHSPjczMtwCM/
rYDuAzA/kbNKbXihxtoXvtgkDQvLKAYN2EUobhiJJI0oXZYzqJLUvL7ndy8B5V/u
HLqaW9ysU6VEn5ZyNaZ43P6W9XDl4KlnlSljtGudkB0Q/6Vncq/LeFrsEB6cePZE
pHatLfR5oB9NdLahIA3GKqJ0PjjTZXTxTNZPzz7tjj6iqYLFB8SDILIEvN9RPpn1
9cx6Uij2oBtZv0V6dVssVFy5C7kCDQRn0DCUARAA60k478gtlyiflx9YF6vUnHga
BjqfB/hm73SdZx8ywJ84Udy74ubcZZyi0eaRbj8FEW7YxttTczwxG3vEnF5ikDuX
zVBWsnqlnJg6jvL4H9Zs5K+sOSp+jvml+8jWmaehvpohRRMcMeACZFPZIoC/JhPJ
cSeUrRbT1Nf5gpPxIOP0UDaczHhcL1cuNx4/ULPh5rSyP/gEw9Gz9uuZe1Shaihb
fxzrcdex70Ope2gRkCUGx42J7dv+d3Cb8AH1SrhzbKbC583+pKkNIwTcZkAFVu5R
PtlEjZi54eWsVZK0m7xUf+0+X3PVfLbSsGh/nWT4/6EZDrUjf6ZFdDMvTKSgGSM0
jYuZAA/ayEsKJqXrsG7EauSkr4luwJO1e52sWYwSzLx6GpvQijGVwnsGQlNqHYXf
zfSjzteAvjWtSUmioPmdsMH0uXIDuoOpLb/ImMlJPZGYfceNXTlvQbgNsgjWgpWU
5bvclm/6P00GO9cKbnVL9KKSAgV2qhuvN8tchjsv0k+Gsfe3FeohUyESKRttxAPb
QP+wM00k9NB4aAcmmFYUZn+kFXCBKJXu+fpHNCeiXipCKODijQFLcs9dhmG70zQf
mDobrnRzgA0TbHTGhjfSk2NlQ8zse5SBs8fEzyO7drBECSECBGhkIIP9/ST9MIEX
Q8ql6VBg9N44G6IcqNsAEQEAAYkCPAQYAQgAJhYhBO/TVJNLxD9jKWEQNNIDn8NC
f8tsBQJn0DCVBQkFo5qAAhsMAAoJENIDn8NCf8tsRuIP/ikFKyw8Avxez8bj625B
3jIwV7Ph6zpQXJoy1oDS0QH/OoXhPE/LXbKvRnsaJPiXSY8cxMIxfrjSfWUMatL5
rBzW6oTWV5RXynD5HCzZVmix4/4jHFiQ2GD25CJ33mM9w+mrTMi2VbXiXNN89ia/
6ayC9I91DYQiTqRCy5CUhitovIMXEDPmY6z+87a/aW66mjbjHg66BLjhddSllXEi
Rxv27eLAvKclj2fZRqo6L9oQZh7TJUaifap2j1d9x5/YaB/Br+PRvEzMmvhG2uIN
xEtLONM8XdCpMIjH0xMRHkC5lVsGxzF3nxguWd0Wn2oms0OOVTIAxiI+FuNgH/cp
8RUNnVoF7N8npdfVSna2y3IS0n2XA53Z1S0AOXO0p0FBdkEA74Z/Pc602KLxPrly
FJAd65Qou5nKREWZE99EKoSGdAI7qT46yzA5U7RcYTaTQE2qXJW6k2102GZwkbpR
QlUVJW/1t9rUD7WJwfrj6Qi7sSoyf86T1DASQpQdh+oWkL2JvXmpbGfBKvCRiX+V
qFNNXXvVpW5XWDKi9BKfZwGHN+aOEefox2Ivqb2BSPT4MqRwbNfETCHrIiSQJD6P
ipNILPBHSsYqfbAM6191VzJfeQJiiPaaRNe4Lbgs3uN4ta+qQDOsnsWoebV8fyci
0WogxMebgbeCa474nt7n/rO+
=2rVz
-----END PGP PUBLIC KEY BLOCK-----
```

Özlem's Screen:

```
PS C:\Users\t-ozlemk> gpg --armor --output signed_testfile.asc --sign testfile.txt
PS C:\Users\t-ozlemk> gpg --armor --output signed_testfile.asc --sign testfile.txt
File 'signed_testfile.asc' exists. Overwrite? (y/N) y
PS C:\Users\t-ozlemk> gpg --armor --output signed_CTIS_496_FirstHW.asc --sign "testfile.txt"
PS C:\Users\t-ozlemk>
PS C:\Users\t-ozlemk>
PS C:\Users\t-ozlemk> ls


    Directory: C:\Users\t-ozlemk


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/23/2025   3:10 PM                .android
d-----         2/25/2025   1:44 PM                .gradle
d-----         2/15/2025   9:08 PM                .ms-ad
d-----         2/14/2025  12:06 PM                .VirtualBox
d-----          2/6/2025   1:56 PM                .vscode
d-r---         1/15/2025   7:20 PM                Contacts
d-----         1/15/2025   7:25 PM                Documents
d-r---         3/28/2025   9:21 PM                Downloads
d-r---         1/15/2025   7:20 PM                Favorites
d-r---         1/15/2025   7:20 PM                Links
d-r---         1/15/2025   7:20 PM                Music
dar---         3/13/2025  12:02 AM                OneDrive
dar--l         3/28/2025   1:38 PM                OneDrive - Microsoft
d-r---         1/28/2025   5:52 PM                Pictures
d-r---         1/15/2025   7:20 PM                Saved Games
d-r---         1/29/2025  11:52 AM                Searches
d-----         2/11/2025   7:49 PM                senior
d-r---          3/6/2025   4:35 PM                Videos
d-----         2/13/2025  10:43 AM                VirtualBox VMs
-a----         2/24/2025   7:07 PM             16 .emulator_console_auth_token
-a----          3/2/2025   6:22 PM             20 .lesshst
-a----         3/14/2025   1:51 PM           3207 mypublickey.asc
-a----         3/28/2025  10:09 PM           1003 signed_CTIS_496_FirstHW.asc
-a----         3/28/2025  10:08 PM           1007 signed_testfile.asc
-a----         3/28/2025   8:43 PM            660 testfile.gpg
-a----         3/14/2025   2:38 PM            566 testfile.sig
-a----         3/14/2025   2:38 PM             86 testfile.txt
-a----         3/14/2025   2:39 PM            989 testfile_signed.txt
```

X)

Özlem	gpg --verify signed_testfile.asc
Emircan	gpg --verify testfile.txt.asc testfile.txt

Emircan's screen:

```
C:\Users\EMİRCAN>gpg --verify testfile.txt.asc testfile.txt
gpg: İmza 03/14/25 14:25:31 Trkiye Standart Saati içinde
gpg:                EDDSA kullanılarak 272A761DBBEF54D21599692C38F48EF5338CBAA3 anahtarı ile yapılmış
gpg: "Emircan <emircan@ug.bilkent.edu.tr>" konumundaki imza iyi [son derece]
```

Özlem's Screen:

```
PS C:\Users\t-ozlemk> gpg --verify signed_testfile.asc
gpg: Signature made 03/28/25 22:08:54 Turkey Standard Time
gpg:                using RSA key E1A210AE0875FF9C375C3E1BEB19172331802677
gpg: Good signature from "ozlem (-) <ozlem.kilickiran@ug.bilkent.edu.tr>" [ultimate]
```

XI)

Why because: This level of trust indicates that you **completely trust** the keyholder not only to verify and authenticate your communications but also to sign and validate the keys of others. When you assign **ultimate trust**, you are essentially telling GPG that you fully believe this person can be relied upon for cryptographic security.

xii)

Emircan's Screen

```
pub rsa4096/efd354934bc43f6329611034d2039fc3427fcb6c 2025-03-11T12:46:10Z
        Hash=23b981b350c93359b13fa9e2f57516ba

uid Emircan Kılıçaslan <emircan@ug.bilkent.edu.tr>
sig  sig  d2039fc3427fcb6c 2025-03-11T12:46:11Z 2028-03-10T12:46:10Z ____________________ [selfsig]



sub rsa4096/6b3b99c27501b6866458cf98cb960d3418e67be8 2025-03-11T12:46:12Z
sig sbind d2039fc3427fcb6c 2025-03-11T12:46:13Z ____________________ 2028-03-10T12:46:10Z []
```

Özlem's Screen

```
pub rsa4096/a34c5a5a8ad80b150e5d80af12cd686e4b2d0734 2025-03-11T13:59:00Z
        Hash=389ccd1a0ff27c62a8ff18fb1c85f281

uid Ozlem Kilickiran <ozlem.kilickiran@ug.bilkent.edu.tr>
sig  sig  12cd686e4b2d0734 2025-03-11T13:59:02Z 2028-03-10T13:59:00Z ____________________ [selfsig]



sub rsa4096/9c6bf60be7a85ebe8288025df644a43b016adac2 2025-03-11T13:59:03Z
sig sbind 12cd686e4b2d0734 2025-03-11T13:59:04Z ____________________ 2028-03-10T13:59:00Z []
```

Özlem	gpg --sign-key emircan@ug.bilkent.edu.tr	gpg --send-keys emircan@ug.bilkent.edu.tr --keyserver hkp://pgp.circl.lu
Emircan	gpg --sign-key ozlem.kilickiran@ug.bilkent.edu.tr	gpg —send-keys ozlem.kilickiran@ug.bilkent.edu.tr --keyserver hkp://pgp.circl.lu

Q2)
From the GNU SOFTARE WEBSITE, we downloaded the following files (https://gnupg.org/download/):

Name	Version	Date	Size	Tarball	Signature
GnuPG	2.4.7	2024-11-25	7822k	download	download

- **gnupg-2.4.5.tar.bz2**
- **gnupg-2.4.5.tar.bz2.sig**

Step	Command/Action	URL/File
1	Download the GnuPG tarball and signature	https://gnupg.org/download/
2	Import GnuPG public key 1 (Werner Koch)	gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys 6DAA6E64A76D2840571B4902528897B826403ADA
3	Import GnuPG public key 2 (Niibe Yutaka)	gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
4	Verify the downloaded GnuPG tarball using the signature file	gpg --verify gnupg-2.4.5.tar.bz2.sig gnupg-2.4.5.tar.bz2
5	(Optional) Certify and trust the keys locally	gpg --edit-key 6DAA6E64A76D2840571B4902528897B826403ADA and gpg --edit-key AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD

```
C:\Users\EMİRCAN>gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys 6DAA6E64A76D2840571B4902528897B826403ADA
gpg: 528897B826403ADA anahtarı: "Werner Koch (dist signing 2020)" değiştirilmedi
gpg: İşlenen toplam sayı: 1
gpg:                değiştirilmeyen: 1

C:\Users\EMİRCAN>gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
gpg: E98E9B2D19C6C8BD anahtarı: "Niibe Yutaka (GnuPG Release Key)" değiştirilmedi
gpg: İşlenen toplam sayı: 1
gpg:                değiştirilmeyen: 1

C:\Users\EMİRCAN>gpg --verify gnupg-2.4.7.tar.bz2.sig gnupg-2.4.7.tar.bz2
gpg: İmza 11/25/24 14:05:26 Trkiye Standart Saati içinde
gpg:                EDDSA kullanılarak 6DAA6E64A76D2840571B4902528897B826403ADA anahtarı ile yapılmış
gpg: "Werner Koch (dist signing 2020)" konumundaki imza iyi [bilinmeyen]
gpg: UYARI: Bu anahtar güven dereceli bir imza ile sertifikalanmamış!
gpg:          Bu imzanın iyesine ait olduğuna dair bir belirti yok.
    Asıl anahtar parmak izi: 6DAA 6E64 A76D 2840 571B  4902 5288 97B8 2640 3ADA
gpg: İmza 11/26/24 08:13:48 Trkiye Standart Saati içinde
gpg:                EDDSA kullanılarak AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD anahtarı ile yapılmış
gpg: "Niibe Yutaka (GnuPG Release Key)" konumundaki imza iyi [bilinmeyen]
gpg: UYARI: Bu anahtar güven dereceli bir imza ile sertifikalanmamış!
gpg:          Bu imzanın iyesine ait olduğuna dair bir belirti yok.
    Asıl anahtar parmak izi: AC8E 115B F73E 2D8D 47FA  9908 E98E 9B2D 19C6 C8BD

C:\Users\EMİRCAN>gpg --edit-key AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
gpg (GnuPG) 2.4.7; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  ed25519/E98E9B2D19C6C8BD
     oluşturuldu: 2021-05-19  son kullanma tarihi: 2027-04-04  kullanım: SC
     güvencesi: bilinmeyen    geçerliliği: bilinmeyen
[    bilinmeyen    ] (1). Niibe Yutaka (GnuPG Release Key)
```

```
PS C:\Users\t-ozlemk> gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys 6DAA6E64A76D2840571B4902528897B826403ADA
gpg: key 528897B826403ADA: "Werner Koch (dist signing 2020)" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\t-ozlemk> gpg --keyserver hkps://keyserver.ubuntu.com --recv-keys AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
gpg: key E98E9B2D19C6C8BD: "Niibe Yutaka (GnuPG Release Key)" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\t-ozlemk>
PS C:\Users\t-ozlemk> gpg --verify gnupg-2.4.5.tar.bz2.sig gnupg-2.4.5.tar.bz2
gpg: can't open 'gnupg-2.4.5.tar.bz2.sig': No such file or directory
gpg: verify signatures failed: No such file or directory
PS C:\Users\t-ozlemk> gpg --verify gnupg-2.4.7.tar.bz2.sig gnupg-2.4.7.tar.bz2
gpg: can't open 'gnupg-2.4.7.tar.bz2.sig': No such file or directory
gpg: verify signatures failed: No such file or directory
PS C:\Users\t-ozlemk> cd "$env:USERPROFILE\Downloads"
PS C:\Users\t-ozlemk\Downloads> gpg --verify gnupg-2.4.7.tar.bz2.sig gnupg-2.4.7.tar.bz2
gpg: Signature made 11/25/24 14:05:26 Turkey Standard Time
gpg:                using EDDSA key 6DAA6E64A76D2840571B4902528897B826403ADA
gpg: Good signature from "Werner Koch (dist signing 2020)" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
      6DAA6E64A76D2840571B4902528897B826403ADA
gpg: Signature made 11/26/24 08:13:48 Turkey Standard Time
gpg:                using EDDSA key AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
gpg: Good signature from "Niibe Yutaka (GnuPG Release Key)" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
      AC8E115BF73E2D8D47FA9908E98E9B2D19C6C8BD
```