



**T.C.**

**ERZURUM TEKNİK ÜNİVERSİTESİ  
MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ  
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**PGP ŞİFRELİ VE İMZALI  
MESAJ**

**KÜBRA DEMİR**

## PGP NEDİR?

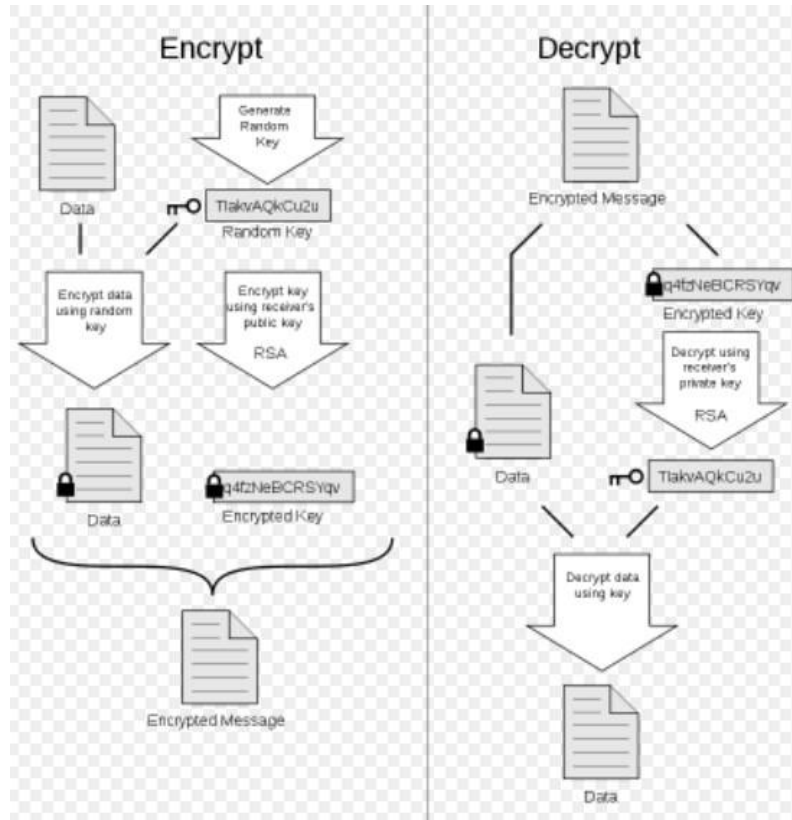
Pretty Good Privacy (PGP), 1991 yılında Phil Zimmermann tarafından geliştirilen, OpenPGP standardını kullanarak veri şifrelemek, şifreli veriyi çözmek veya veriyi imzalamak için kullanılan, gönderilen ya da alınan verinin gizliliğini ve kimlik doğrulamasını sağlayan bir bilgisayar programıdır. Genellikle text dokümanlarını, epostaları, dosyaları, klasörleri ve disk bölümlerini şifrelemek ve imzalamak için kullanılır.

**PGP ile e-mail güvenliğinin sağlanması:** E-posta güvenliği öncelikli olarak elektronik postanın hedefe güvenli iletimini temin eder. Buradaki güvenlikten kasıt; gizlilik, bütünlük, kimlik doğrulama ve inkâr edilemezliği garanti etmektir. Başka bir ifadeyle insanlar e-postalarının güvenli bir şekilde iletileceğine güvenmeyecekleri bir e-posta sistemini kullanmak istemezler.

Eğer kullanılan e-posta sistemi şifreleme, kimlik doğrulama ve elektronik imza gibi güvenli iletim teknikleri kullanmıyorsa bundan kesinlikle emin olamayız. Güvenli ve şifreli bir şekilde gönderilmeyen e-postalar herkese açık olan internet ortamından geçtiklerinden dolayı şifrelenmemiş olan her türlü verinin bilgisayar korsanları veya kötü niyetli kişiler tarafından elde edilebileceğini de unutmamak gerekir. Bu güvenlik problemlerini ortadan kaldırmak için kullanılan yöntem ise Kriptografi (Şifreleme)'dir.

PGP ile şifreleme genel olarak kriptografik özet fonksiyonu, veri sıkıştırma, simetrik anahtar algoritmaları ve açık anahtar şifrelemenin kombinasyonundan oluşan hibrit bir yapıya sahiptir. Bu yöntemle e-posta alıcının posta kutusuna gelene kadar şifreli ve içeriği yetkisiz kişilere karşı korunmuş olur.


PGP'nin genel yapısı aşağıdaki gibidir;



Bunu bir örnekle açıklamak gerekirse öncelikle bazı uygulama kurulumları ve karşılıklı olarak anlaşmak için bir servera ihtiyacımız vardır. Gerekli olan kurulumlar; gnu4win, kleopatra, Gpa dır. Örnekte server olarak ise keys.openpgp.org kullanılmıştır.

### □ Gpg4Win Kurulumu

Öncelikle aşağıdaki gibi gpg4win exesi indirilerek aşağıdaki adımlar sırasıyla gerçekleştirilir.





Yeni  
Sürüm 4 nedir

Gpg4win hakkında

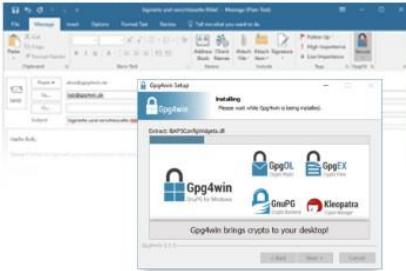
Topluluk

Destek olmak

İndirmek 



Ayrıntılar · Değişiklik Geçmişi · Bütünlüğü kontrol edin



2022-04-22

🔒 **Gpg4win 4.0.2** yayınlandı

🔒 **Gpg4win 4.0.0** yayınlandı

2021-10-19

🔒 **GnuPG 2.2.32** Güncellemesi

Arşivlenmiş Haberler

## Gpg4win - güvenli bir çözüm...

... dosya ve e-posta şifreleme için. Gpg4win (Windows için GNU Privacy Guard) Özgür Yazılımdır ve sadece birkaç fare tıklamasıyla kurulabilir.

[Ana Sayfa](#) » [İndir](#)

## Gpg4win 4.0.2'yi indirin (2022-04-26)

Bu yükleyiciyi daha eski bir sürümü güncellemek için de kullanabilirsiniz. Anahtarlar ve yapılandırma tutulacaktır.

**Bakım ve geliştirmeyi desteklemek için lütfen Gpg4win'e bağış yapın!**  
İstediyini öde! - Teşekkür ederim!

ile bağış yapın

- ☒ PayPal
- ☐ Bitcoin
- ☐ banka transferi



\$0

\$10 \$15 \$25 \$

Amerikan  
Doları

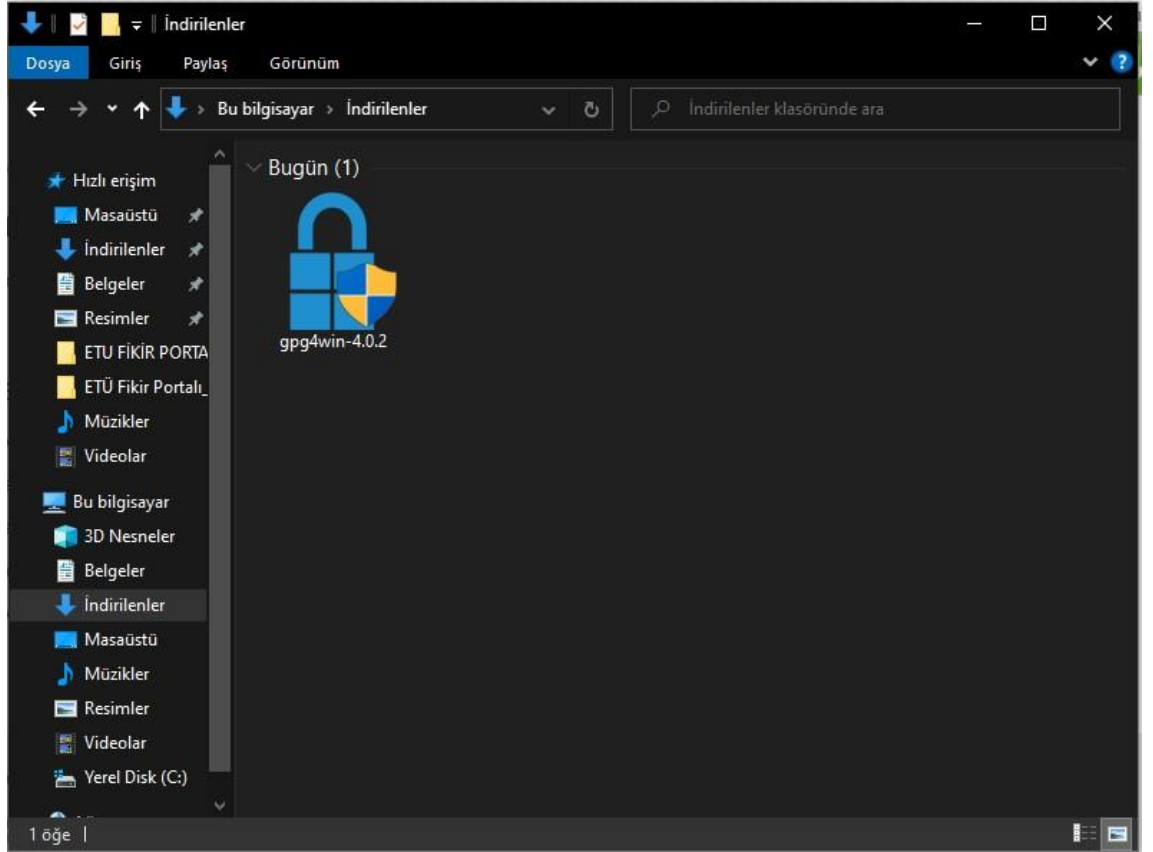
avro

bir kere

aylık

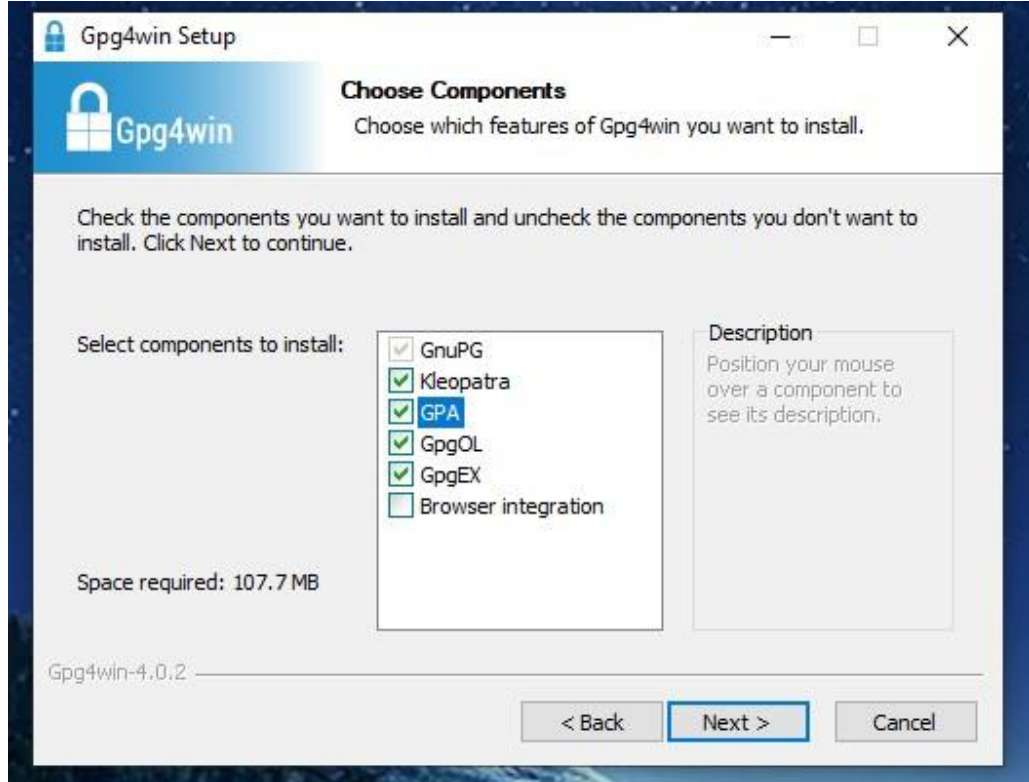
 İndirmek

[OpenPGP imzaları ve kaynak kodu paketi](#) »



## □ Kleopatra ve GPA Kurulumu

Gpg4Win exesi kurulumundan sonra içerisinde kurulacak program seçeneklerinde Kleopatra ve GPA seçilerek ileri gidilir.

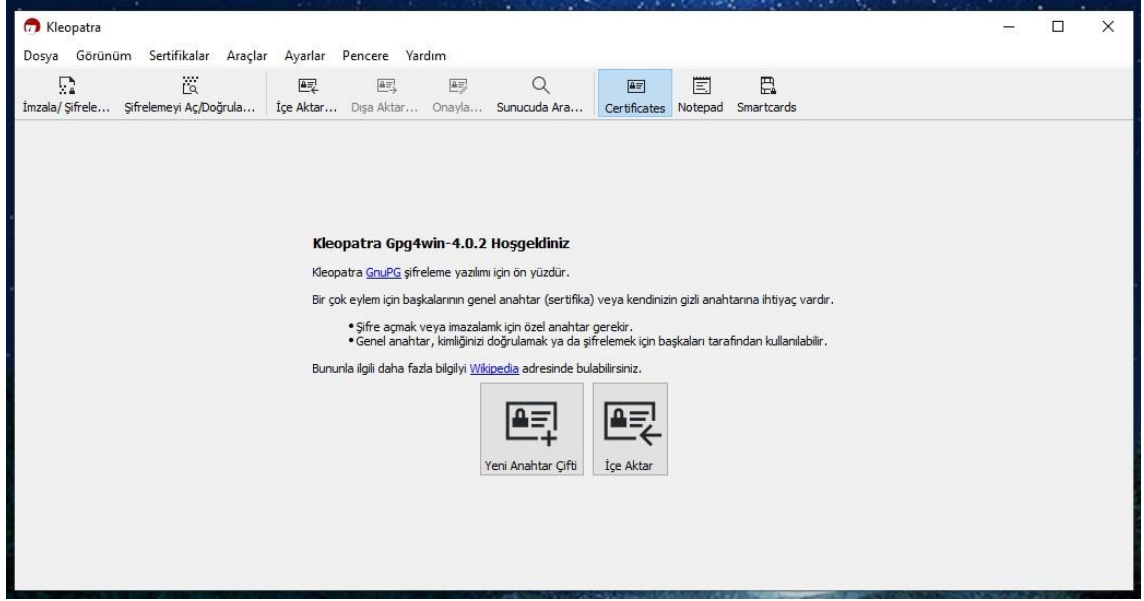




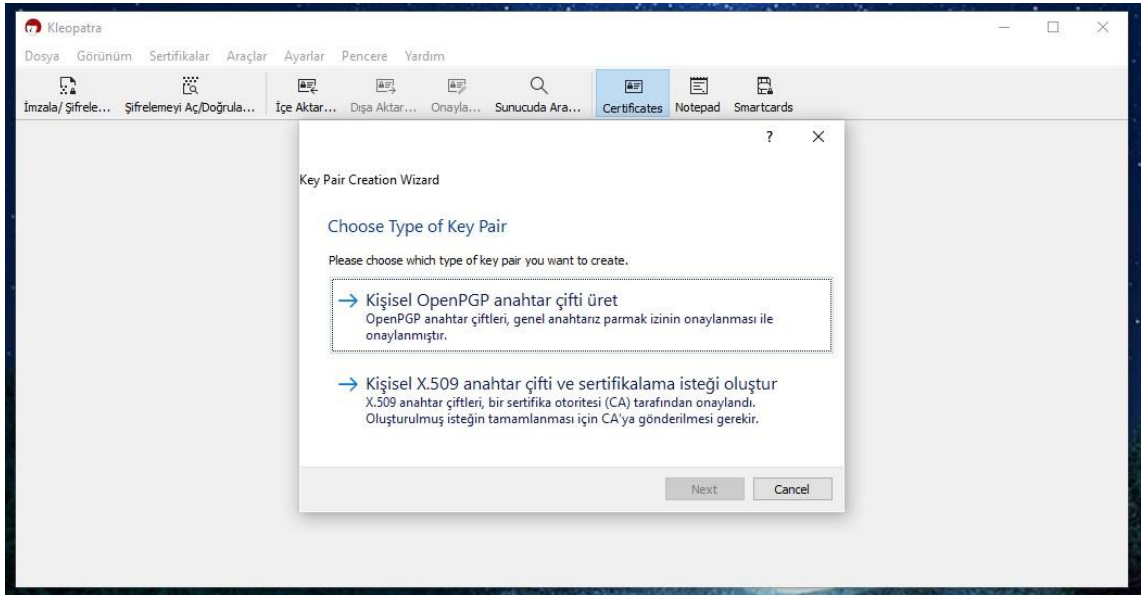
Bu şekilde kurulumlar sonucunda ařağıdaki gibi ihtiyacımız olan uygulamalar elde edilmiş olur.



Öncelikle Kleopatra uygulaması açılıp yeni anahtar çifti ile public ve private keylerimiz oluşturulmalıdır.

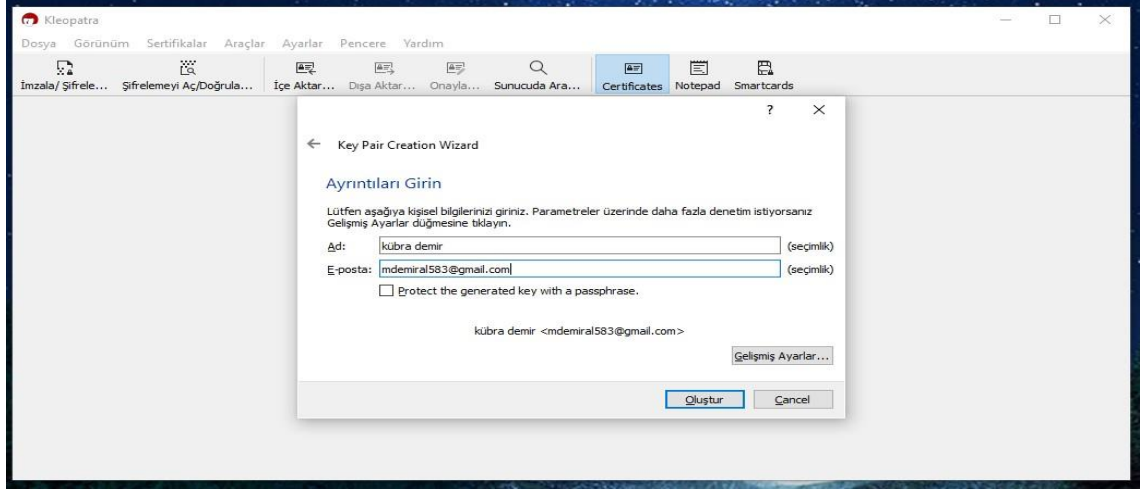


Kişisel olarak openpgp anahtar çifti üretilmelidir. Bu sayede pgp ile public ve private key yapılır. Bu keyler ile mesajlaşma gerçekleştirilir.

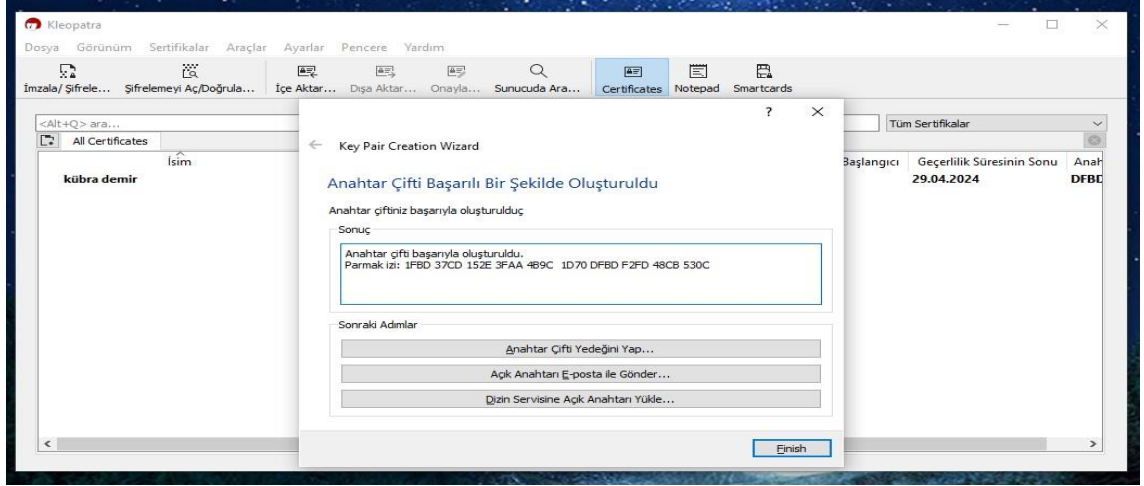


Oluşturulacak keylerle şifreli ve imzalı olarak gönderilecek olan mesaj için kullanılacak e-mail bu aşamada yeni anahtar çiftine eklenir.

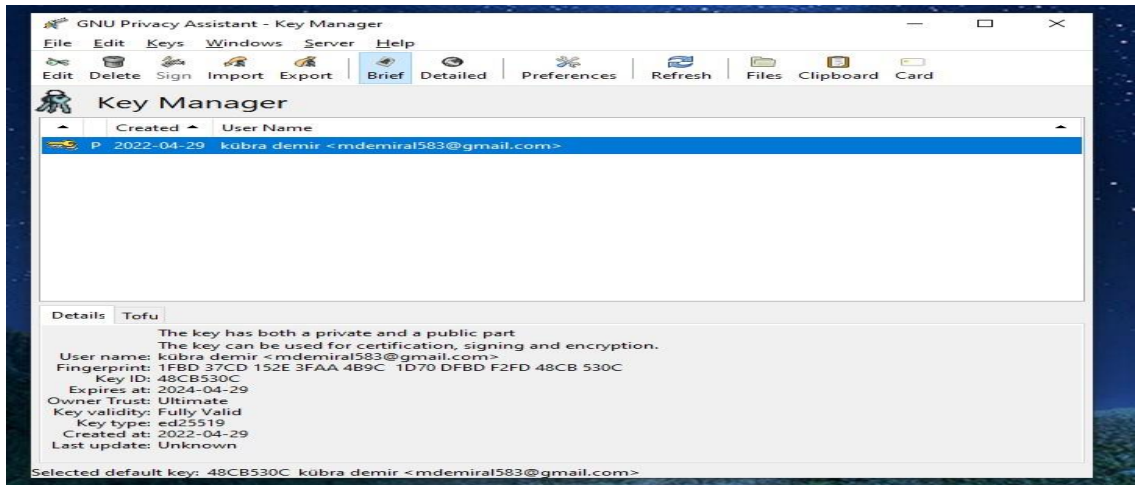




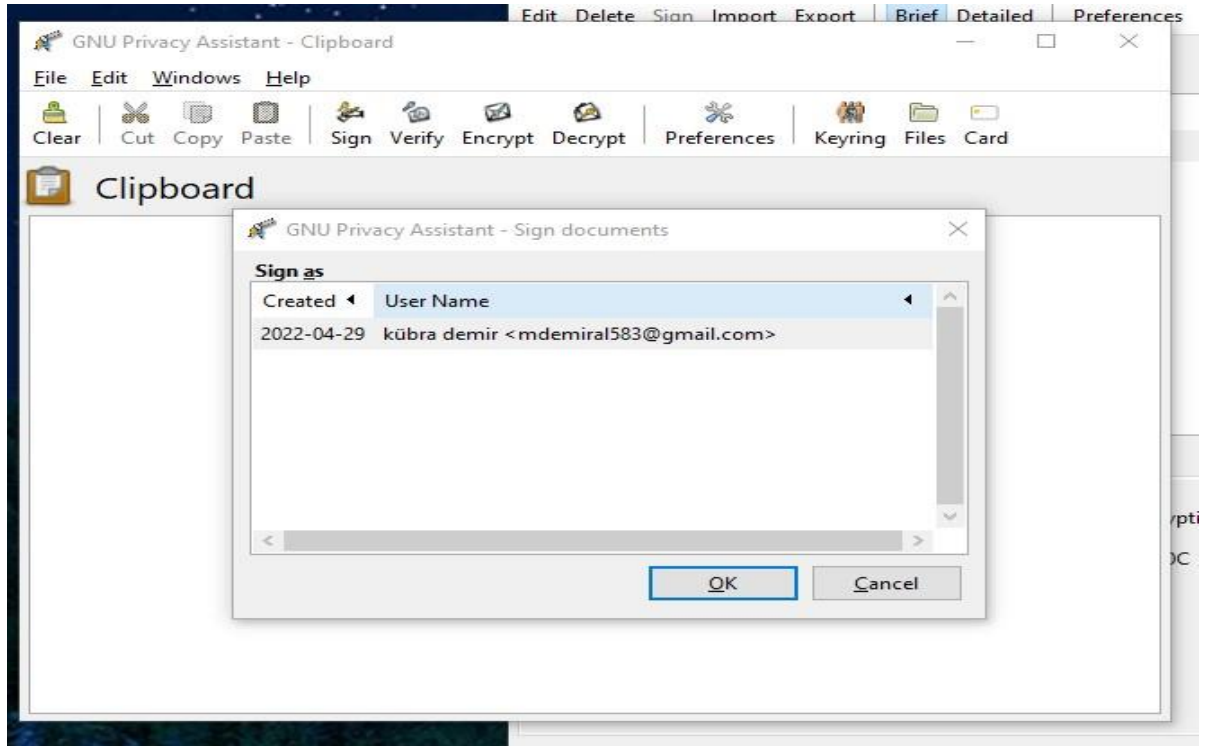
Başarılı bir şekilde oluşturulan yeni anahtar çifti yazısı sonucunda bir sonraki aşamaya geçilir.



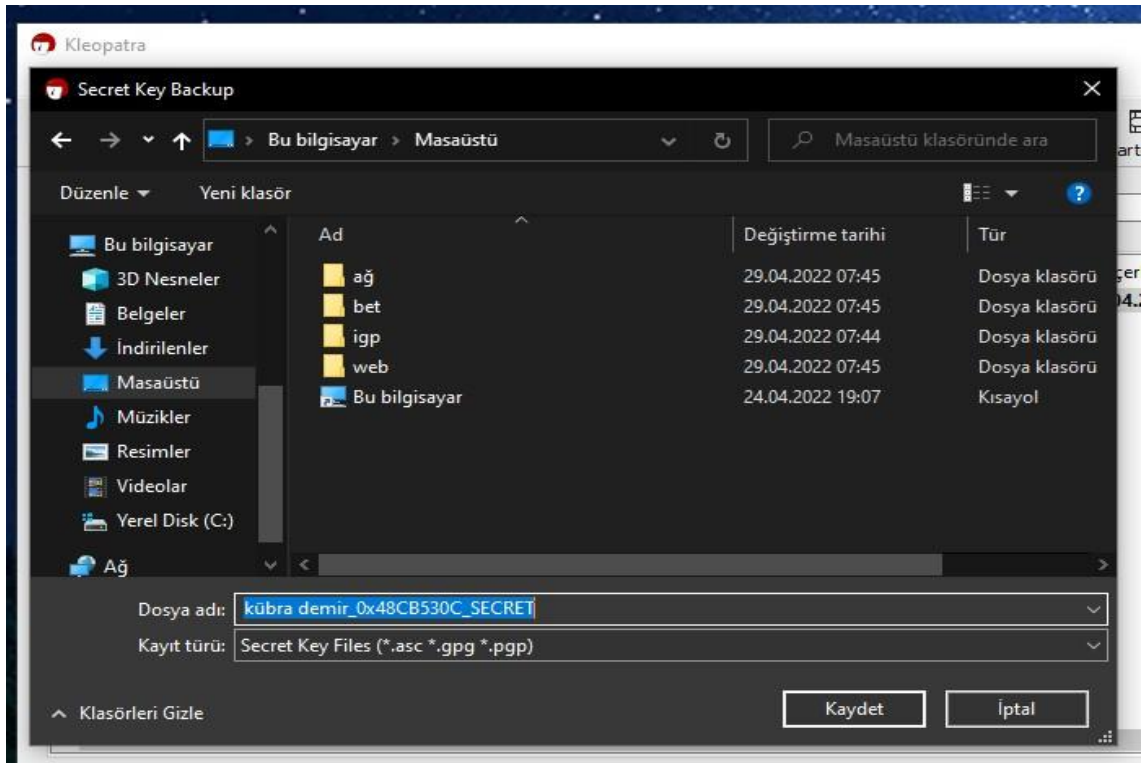
Bir sonraki aşamada GPA açılarak aynı şekilde key manager üzerinden private ve public olarak girilen e-maile uygun olarak anahtar çifti oluşturulur.



Burada ek olarak imzalama için e-mail tanımlaması yapılır. Bu sayede bir sonraki aşamalarda imzalama işleminde kullanılacak mail el edilmiş olur.



GPA ile şimdilik işimiz bitti. Bir sonraki adımda tekrar Kleopatra ekranına dönülerek oluşturulan anahtar üzerine sağ tık yapılarak “Gizli Anahtar Yedeği” seçeneği ile anahtarımızın private dosyasını .asc olarak indiririz.



Private key dosyası elde edildikten sonra public key için tekrar anahtar üzerine sağ tık yapılarak “Dışa Aktar” seçeneği ile dosya .asc olarak kullanıma hazır hale getirilir.

Bu aşamalardan sonra artık server kısmına geçilebilir. Yani karşıdaki kişi ile oluşturduğumuz public ve private keyleri kullanarak şifreli, şifreli-imzalı veya sadece imzalı mesaj gönderme işlemine başlayabiliriz.

+ İlk aşama keys.openpgp.org sitesine girilerek server ekranına ulaşılır.

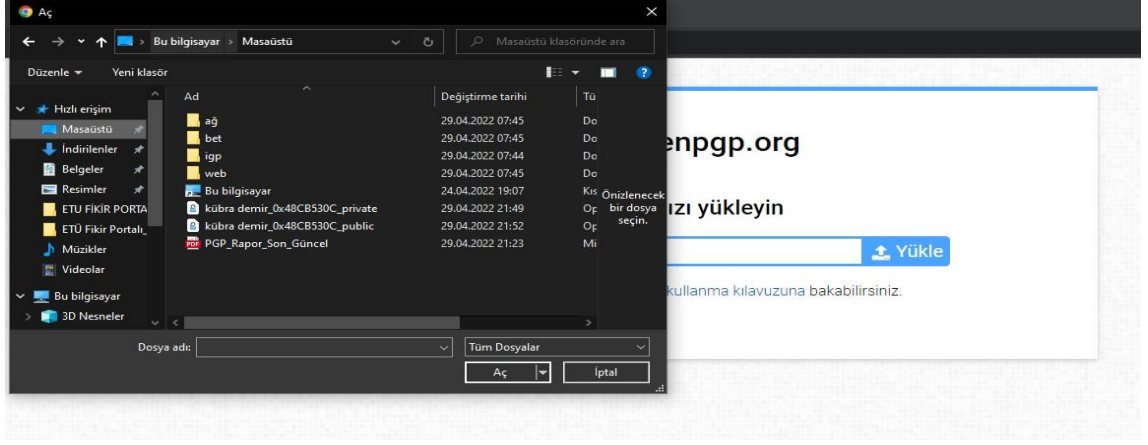


The screenshot shows the homepage of keys.openpgp.org. At the top, the domain name 'keys.openpgp.org' is displayed. Below it is a search bar with the placeholder text 'E-posta adresi / Anahtar Kimliği / Parmak İzi ile arama' and a blue 'Ara' button. Under the search bar, there are two links: 'Ayrıca anahtarınızı yükleyebilir veya yönetebilirsiniz.' and 'Bu hizmet hakkında daha fazlasını öğrenin.' At the bottom, there is a news section titled 'Haberler: 100.000 doğrulanmış adresi kutluyoruz' with a checkmark icon and the date '(2019-11-12)'.

+İkinci aşama public dosyasını “yükleyebilir” kısmına tıkladığımızda ekrana gelen “dosya seç” ile servera eklemektir.



The screenshot shows the 'Anahtarınızı yükleyin' (Upload your key) page on keys.openpgp.org. The page title is 'Anahtarınızı yükleyin'. Below it is a button labeled 'Dosya Seç' (Select File) and a blue 'Yükle' (Upload) button. At the bottom, there is a link: 'Daha fazla bilgi içintanıtım veya kullanma kılavuzuna bakabilirsiniz.'



+Daha sonra public dosyası eklenerek anahtar kullanıma hazır hale getirilir. Ekleme sonucunda elde edilen çıktı aşağıdaki gibidir.

## keys.openpgp.org

1FB037CD152E3FAA4B9C1D70DFBDF2FD48CB530C anahtarını yüklediniz.

Bu anahtar şimdi sadece kimlik olmayan bilgiyle yayınlandı (bunun anlamı nedir?)

Anahtarı e-posta adresiyle bulunabilir yapmak için, size ait olduğunu doğrulamanız gerekiyor:

mdemiral583@gmail.com Doğrulama E-postasını Gönder

Not: Bazı sağlayıcılar istenmeyen e-postaları önlemek amacıyla e-postaları 15 dakikaya kadar geciktirebiliyor. Lütfen sabırla bekleyin.

+Bu çıktı üzerinden “doğrulama e-postası gönder” butonuna tıklanarak aktif olarak kullandığımız maile doğrulama kod gönderilir. Doğrulama gelene kadar beklemeye alınır.

## keys.openpgp.org

1FB037CD152E3FAA4B9C1D70DFBDF2FD48CB530C anahtarını yüklediniz.

Bu anahtar şimdi sadece kimlik olmayan bilgiyle yayınlandı (bunun anlamı nedir?)

Anahtarı e-posta adresiyle bulunabilir yapmak için, size ait olduğunu doğrulamanız gerekiyor:

mdemiral583@gmail.com Doğrulama Bekleniyor

Not: Bazı sağlayıcılar istenmeyen e-postaları önlemek amacıyla e-postaları 15 dakikaya kadar geciktirebiliyor. Lütfen sabırla bekleyin.

+Sonraki adım doğrulama için mail ekranına gitmek ve oluşturulan anahtar parmak izini almaktır.



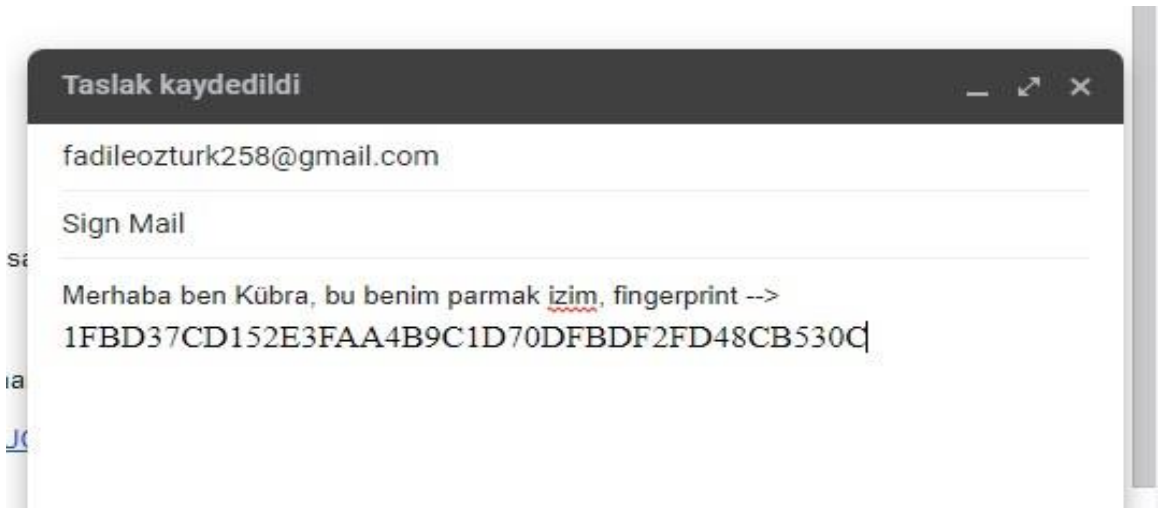
+Mail ekranında belirtilen “OpenPGP anahtarı” mailimiz için tanımlanmış server anahtarıdır. Bu anahtar kullanılarak bir sonraki aşamaya geçilir.



+Sonraki aşamada öncelikle anahtar bilgisi kopyalanır.



+Daha sonra karşıdaki kişinin mailine fingerprint olarak gönderilir.

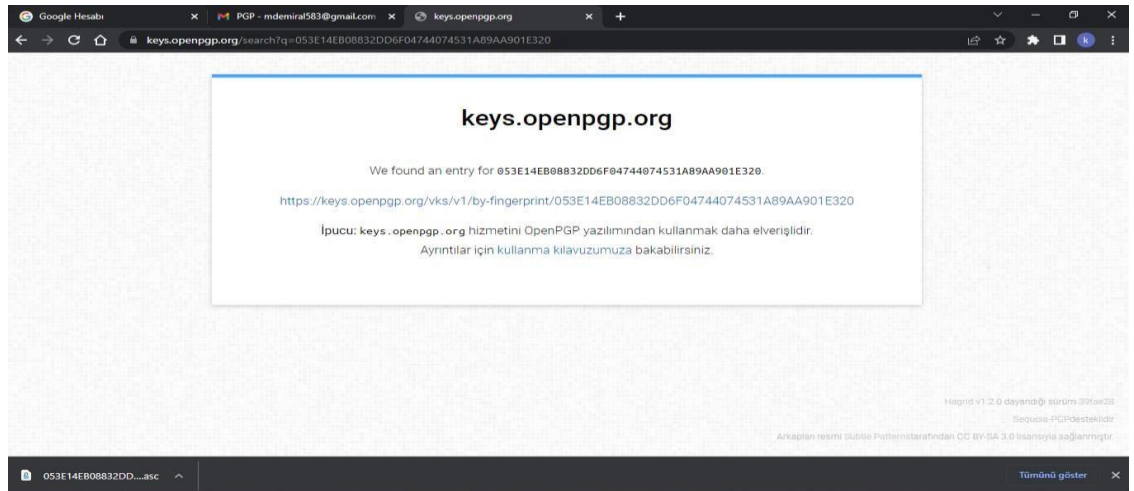


+Bu gönderim yapıldıktan sonra karşı tarafında fingerprinti istenerek karşılıklı mesajlaşma için uyum sağlanmış olur.

+ Karşı taraftan gelecek olan fingerprint bilgisi kopyalanarak karşı tarafın public key dosyasını indirmek için tekrar keys.openpgp.org ekranına gelinir.



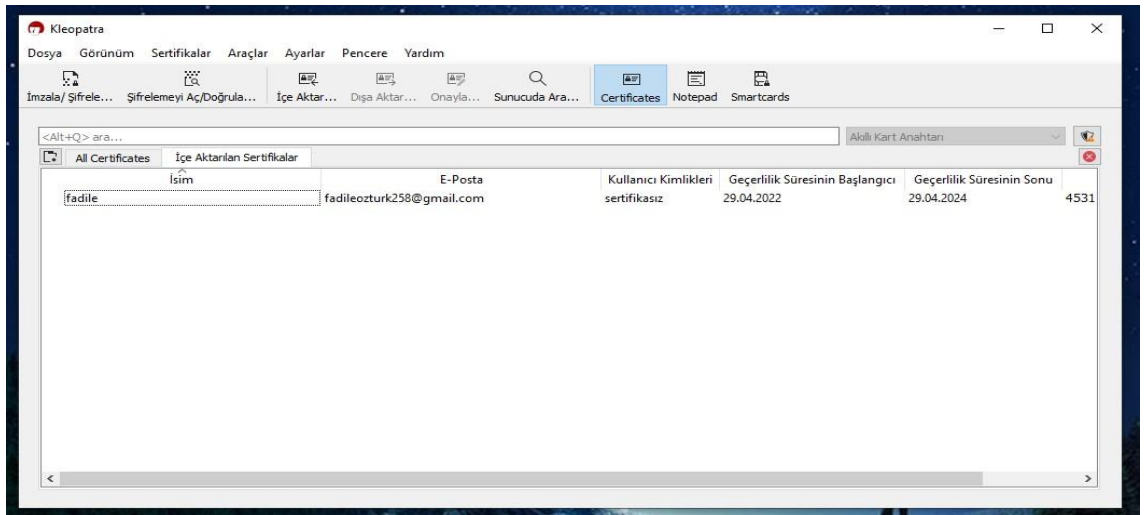
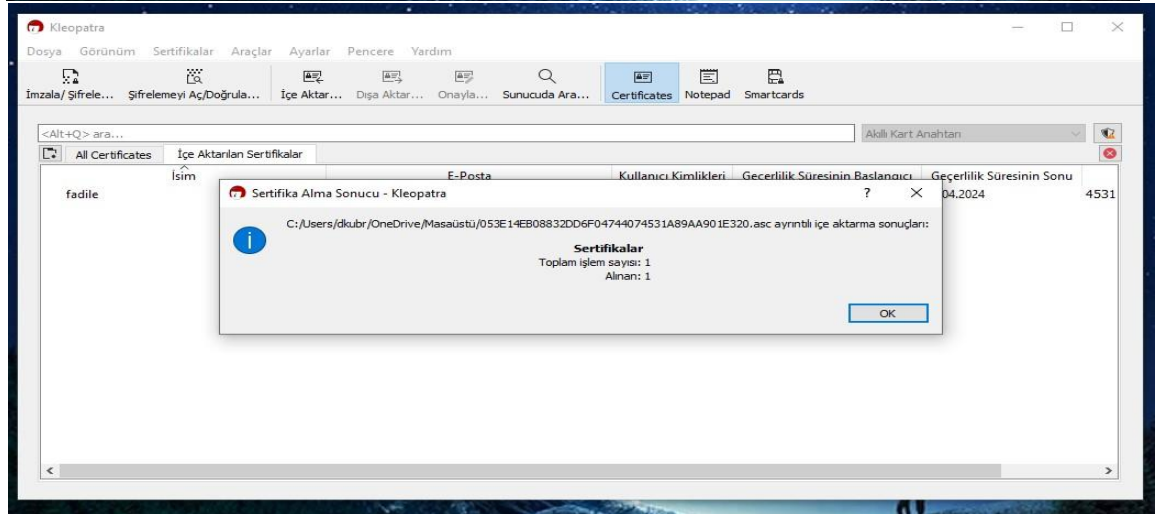
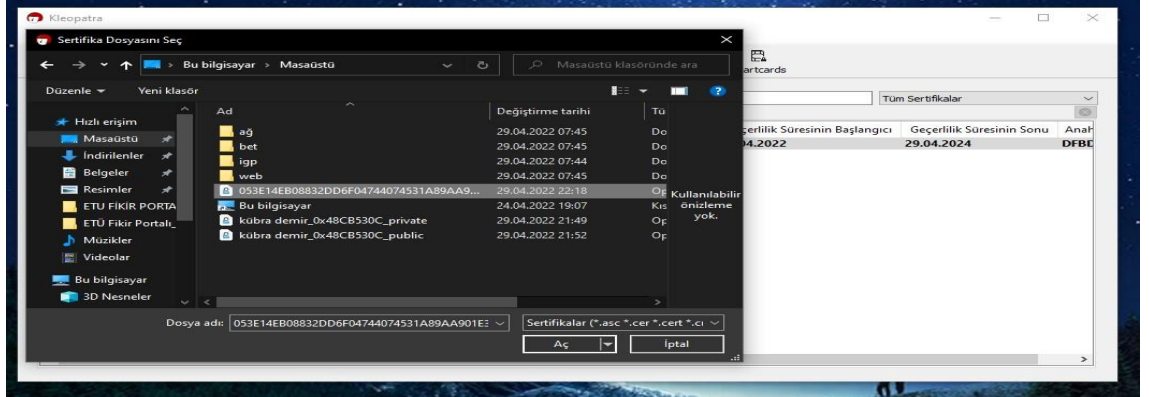
+Tekrar server ekranına gelindiğinde anahtar kısmına karşı tarafın anahtarı eklenir daha sonra ekrana gelen linke tıklanarak indirme başlatılır.





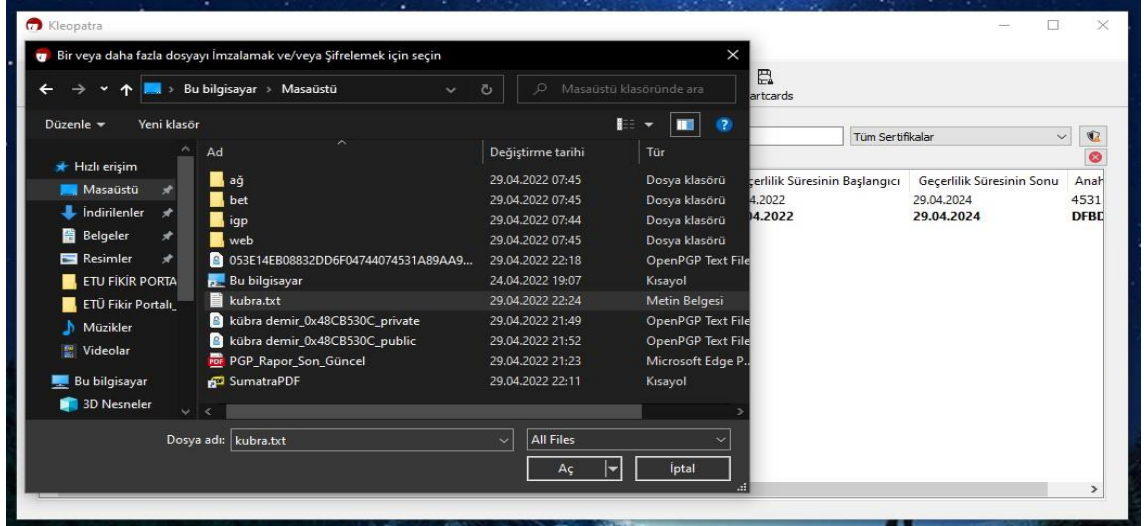
Server ile elde edilen karşı tarafın public keyini kullanmak için Kleopatra uygulamasına geçilir.

+İlk yapılacak olan Kleopatra ekranından “file” kısmına gelinerek dosya seçme işlemidir. Yeni indirilen .asc uzantılı dosya alınır ve “içe aktar” seçeneği ile Kleopatra içerisinde bir anahtar olarak elde edilir.

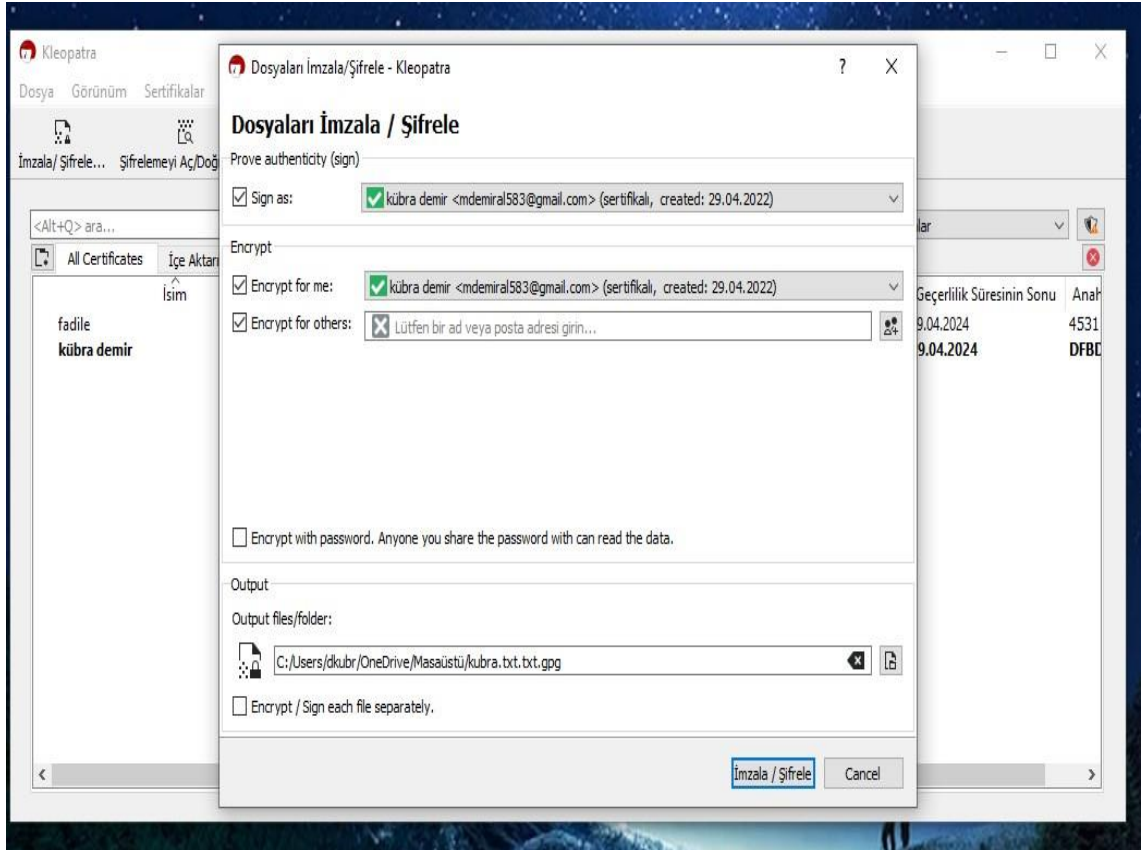


Buraya kadar temel işlemler halledilmiş oldu. Sonraki aşama ise karşı tarafa bir txt dosyasını şifreli olarak göndermek ve karşı tarafın Kleopatrasında entegre edilmiş kendi anahtarımızla okunması için şifreleme işlemi yapmaktır.

+Öncelikle kübra.txt isimli bir txt dosyası oluşturulur

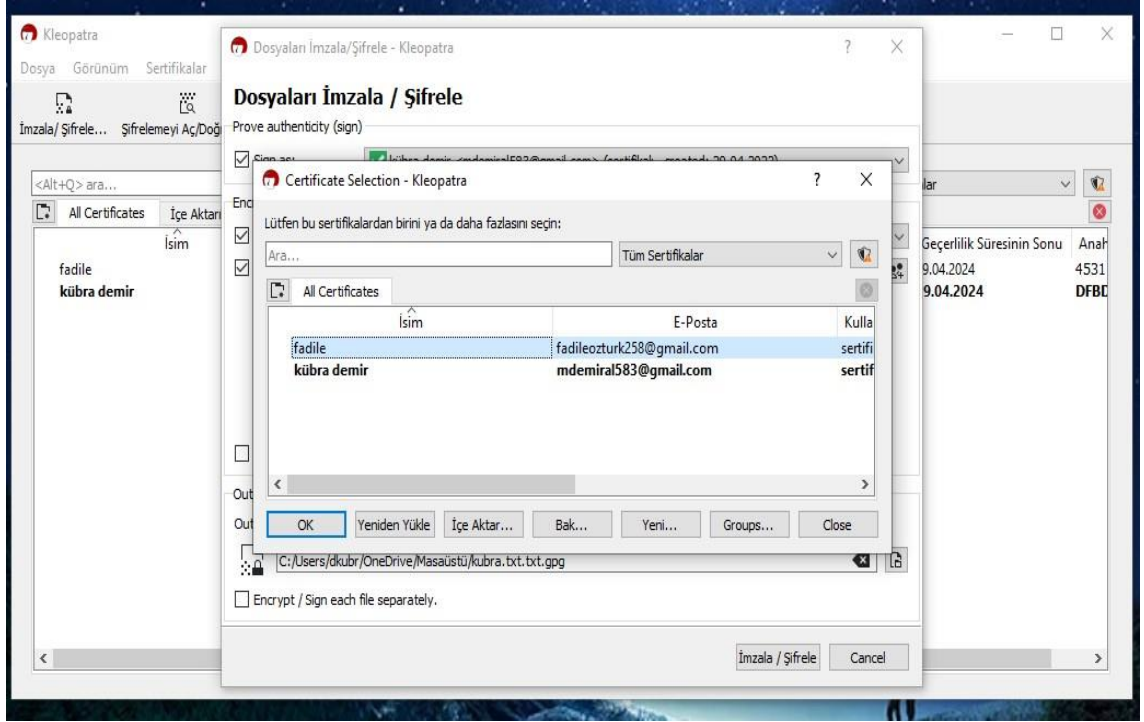


+Alınan .txt dosyası “imzala/şifrele” yapılarak daha sonrasında “encrypt for others” kısmına karşı tarafın e-maili yazılarak imzalı ve şifreli hale getirilir.

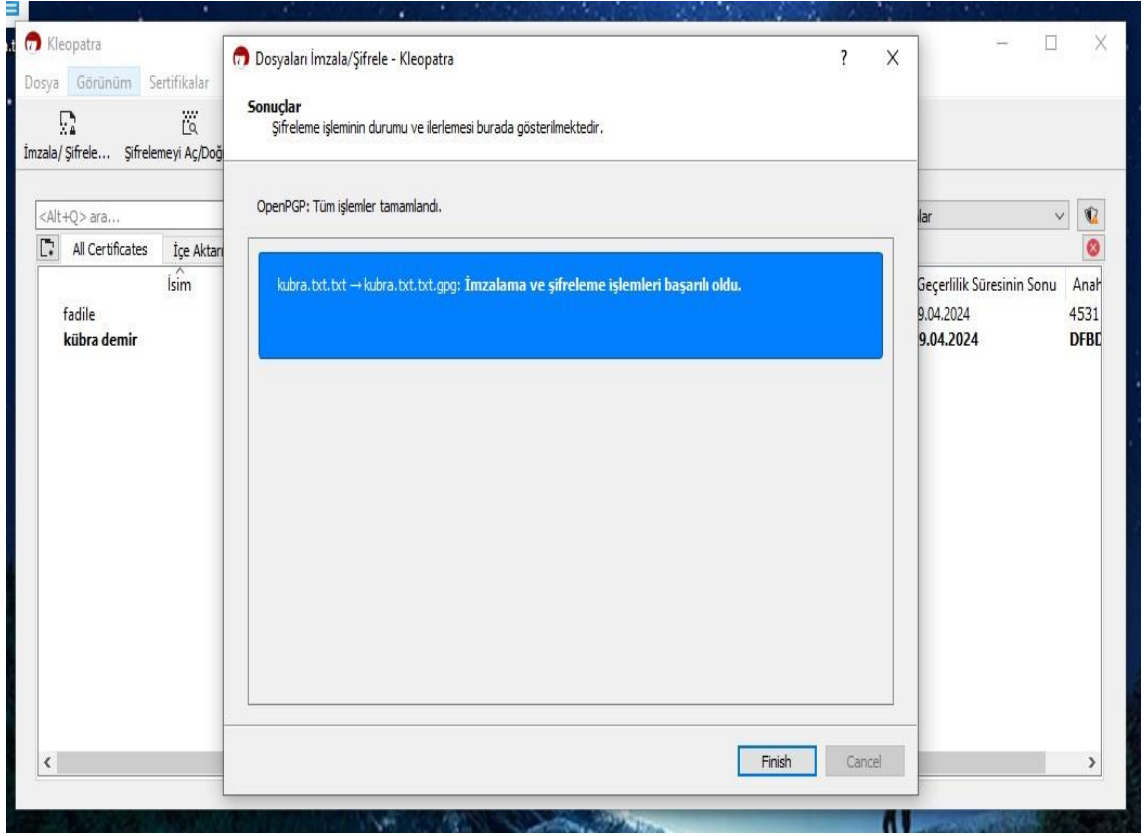




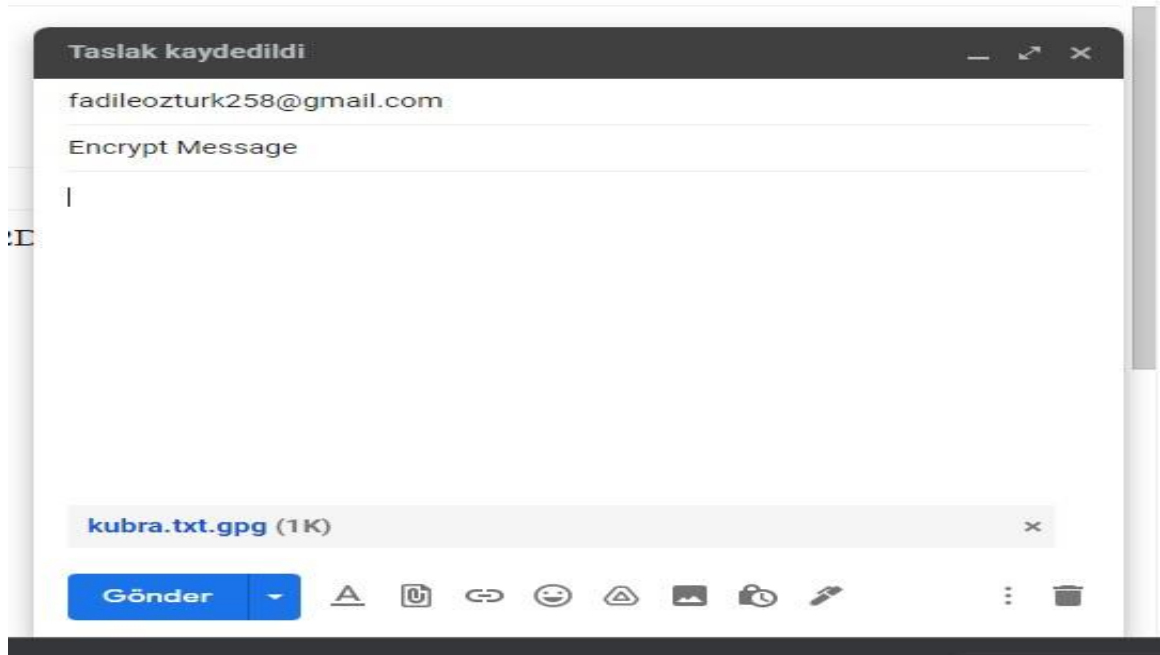
+İmzala ve şifreleye basılmadan önce seçilen karşı taraf maili için onay verilmesi gerekir.



+Aşağıda gösterildiği gibi işlem başarılı bir şekilde yapılmış ve .txt uzantılı dosyamız şifreli/imzalı olarak elde edilmiştir. Yolu desktop olduğu düşünülürse bir tane kübra.txt bir tane de kübra.txt.gpg dosyası oluşturulmuştur.



+Her şey tamamlandığına göre şimdi karşı tarafa mail olarak bu dosyayı atmamız ve karşı tarafında bizden aldığı public key ile şifreyi çözerek gönderilen texti okuması beklenmektedir.



+Gönderilen mesajdaki dosya indirildikten sonra tekrar Kleopatra ekranına gelinerek dosyanın içeriğini açmak için decrypt edilmelidir.

## Şifreli Mesaj ;

Gelen Kutusu x



**Fadile Öztürk**

Alici: ben ▼

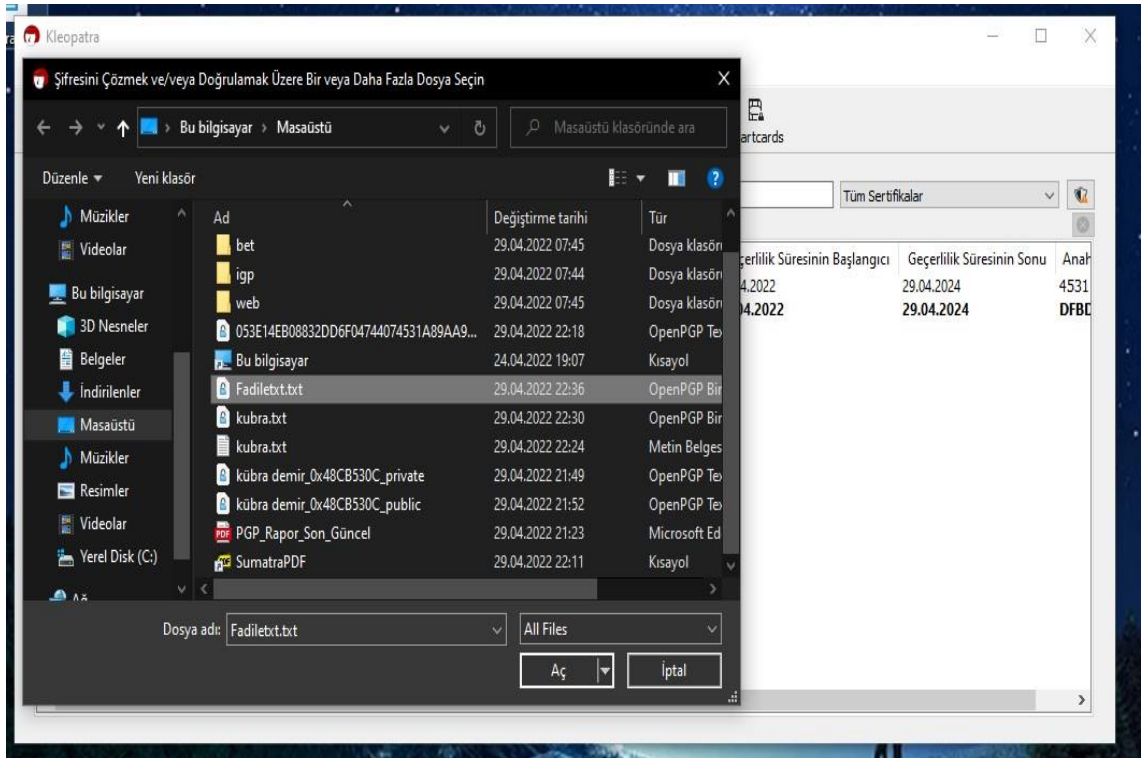
Windows için [Posta](#) ile gönderildi



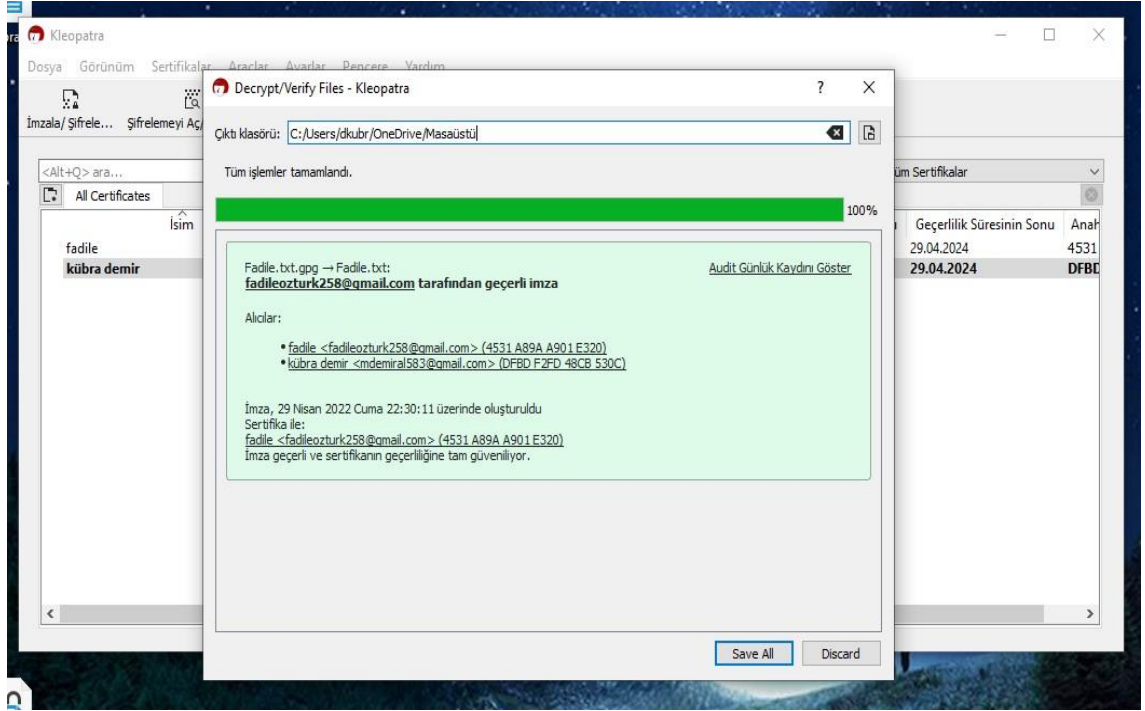
Yanıtla

Yönlendir

+Decrypt işlemi için Kleopatra ekranından “file” ile elimizdeki şifreli .gpg uzantılı dosya “içeri aktar” yapılmalıdır.



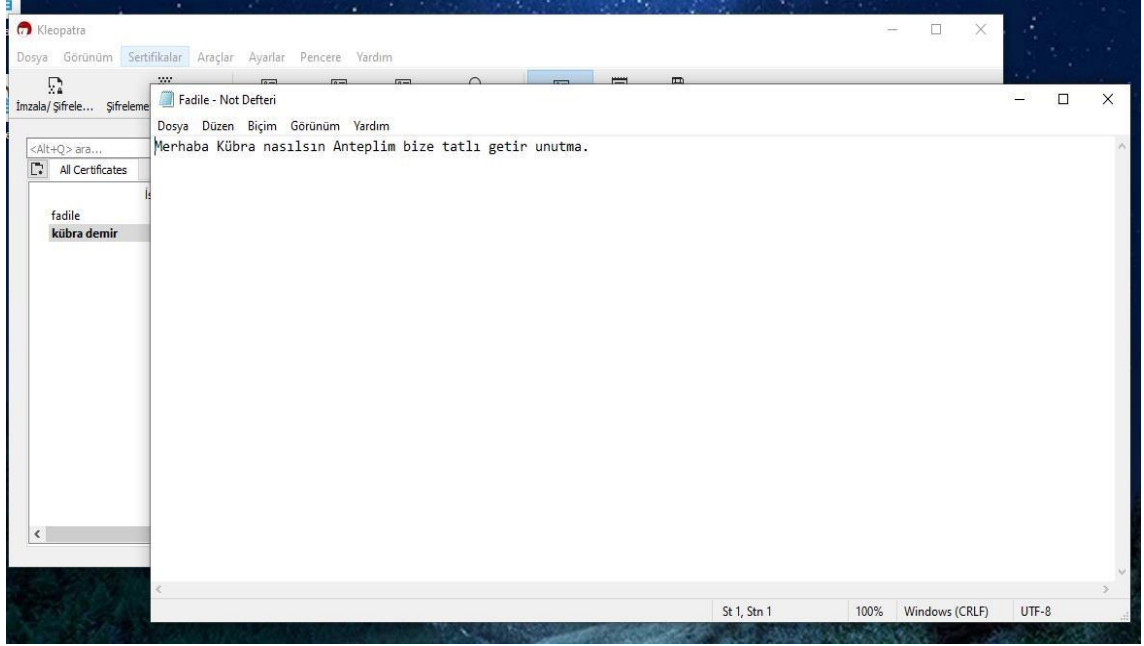
+Seçilen dosyanın üzerinden decrypt için “şifreyi çöz” kısmı kullanılmalı ve dosyanın şifresi public key entegresi sayesinde çözülmelidir. Daha sonrasında ekrana aşağıdaki gibi başarılı olduğuna dair bilgi mesajı gelecek ve bu aşamadan da sonra txt dosyasının içeriği okunacaktır.



+Bunun sonundan desktop üzerinde çözülmü txt dosyası şifresiz olarak belirtilecektir. Çözülen dosya “Fadile” olarak çıktı verir. Bu dosyaya tıklandığında ekrana içerik getirilmiş olacaktır.



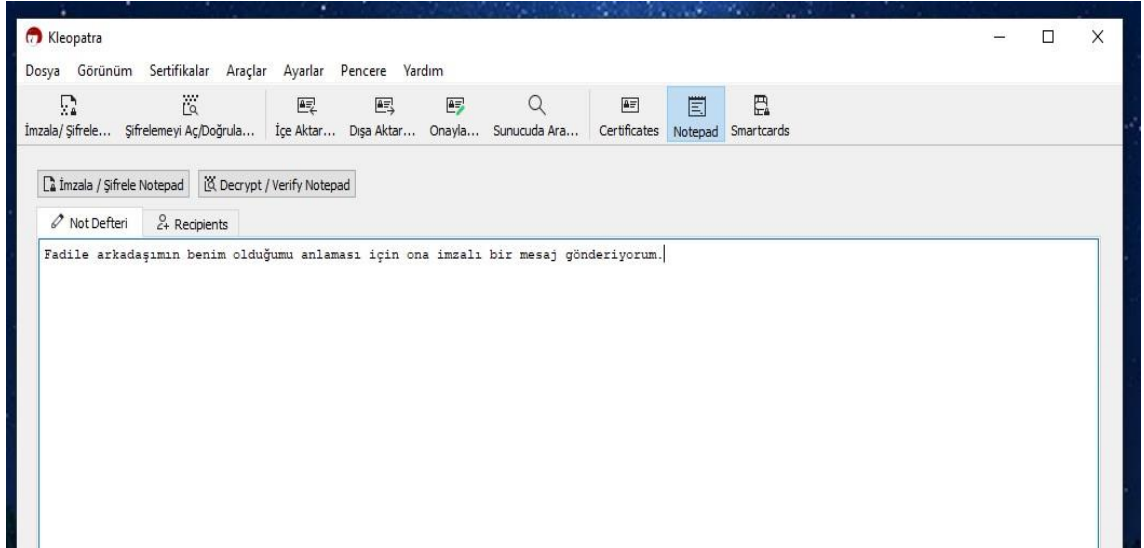
+Sonuç olarak elde edilen şifresiz mesaj aşağıdaki gibidir.



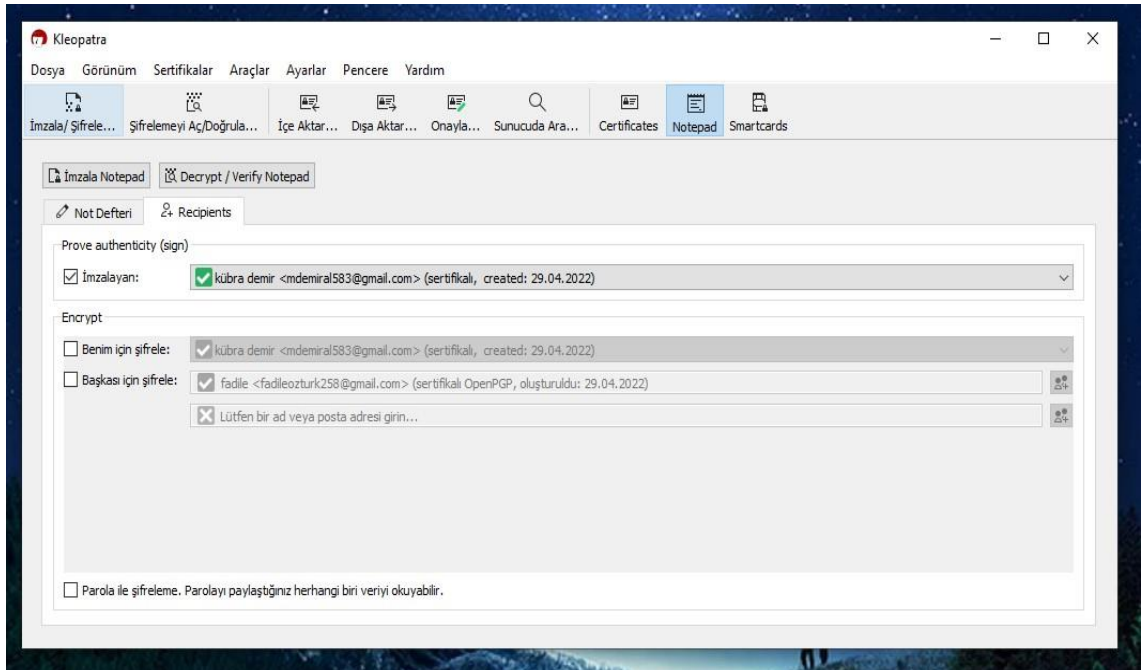
Buraya kadar anlatılan kısım uygulamalı olarak karşı tarafla yapılmıştır. Bundan sonraki kısımlarda üç ana başlığı Kleopatra içerisinde nasıl yapabileceğimizi öğreneceğiz.

### 1-) KLEOPATRA KULLANILARAK İMZALI MESAJ OLUŞTURMA

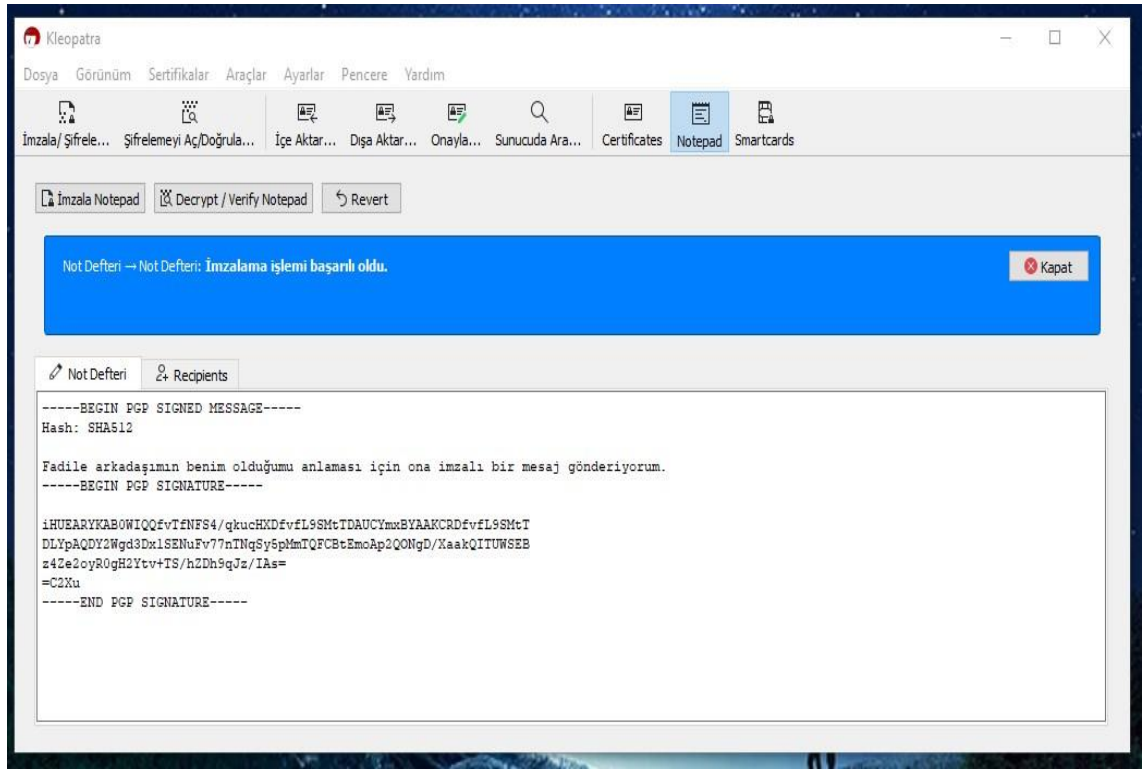
--Bu işlem için ilk adım Kleopatra ekranındaki “Notepad” kısmına gelerek imzalamak istediğimiz mesajı yazmaktır.



--Mesaj oluşturulduktan sonraki kısım “Recipients” kısmına gelerek sunulan 3 seçenektan sadece “sign as” kısmını seçmek ve “imzala Notepad” e tıklanarak mesajı imzalı hale getirmektir.

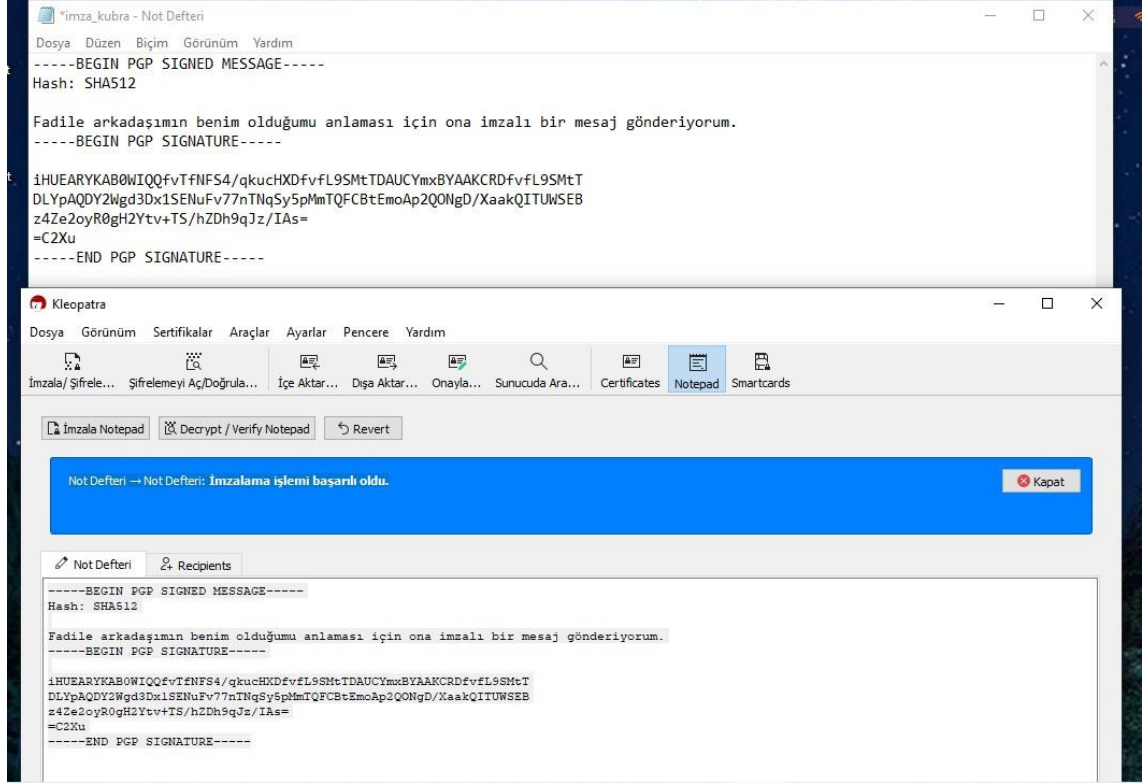


--Tıklama sonucunda elde edilen imzalama işleminin başarılı bir şekilde yapılmış olmasıdır.



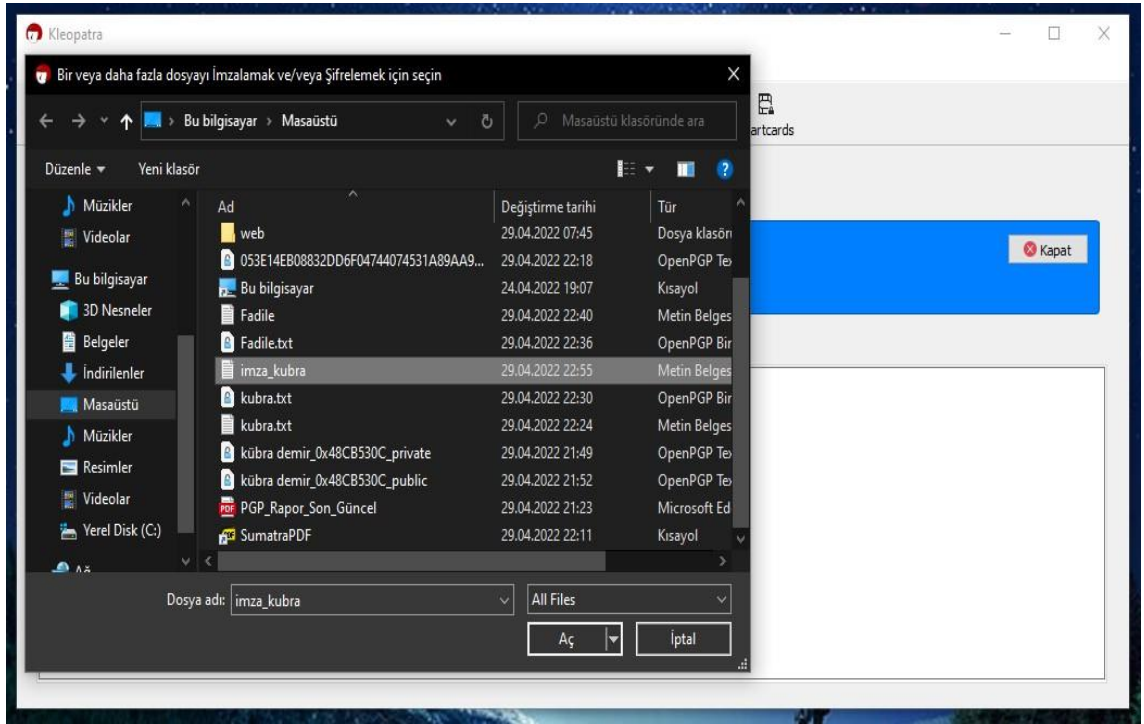
--

Başarılı işlemin sonucunda elde edilen “begin pgp signed message” texti kopyalanır. Daha öncesinde desktop üzerinde oluşturulmuş örneğin imza\_kubra.txt dosyasına yapıştırılır.

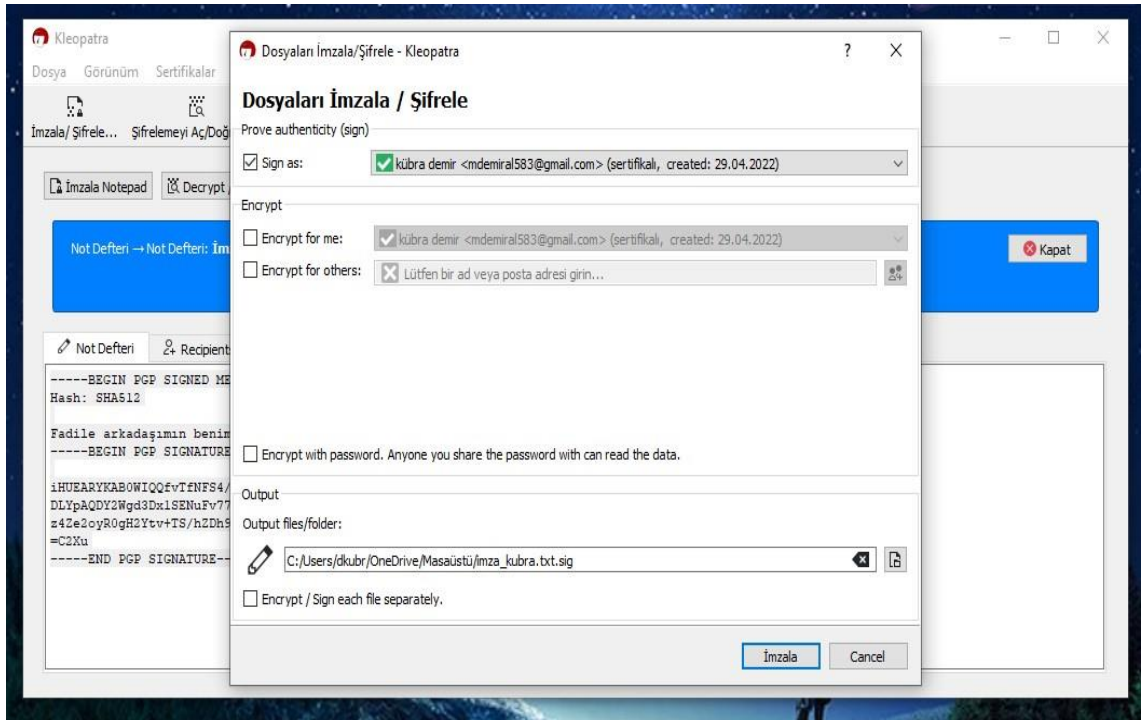


--Burada oluşturulan txt dosyasını imzalamak için Kleopatra ekranına gelinerek imza\_kubra.txt dosyası için “içeri aktar” işlemi yapılmalıdır.





İçeri aktar işleminden sonra tekrar “imzala” işlemi yapılmalı ve seçeneklerden sadece “sign as” seçilmelidir. Bu sayede imza\_kubra.txt dosyasıyla beraber imza\_kubra.sig dosyası oluşturulmuştur.



--Yani imzalama işlemi başarılı olmuştur.

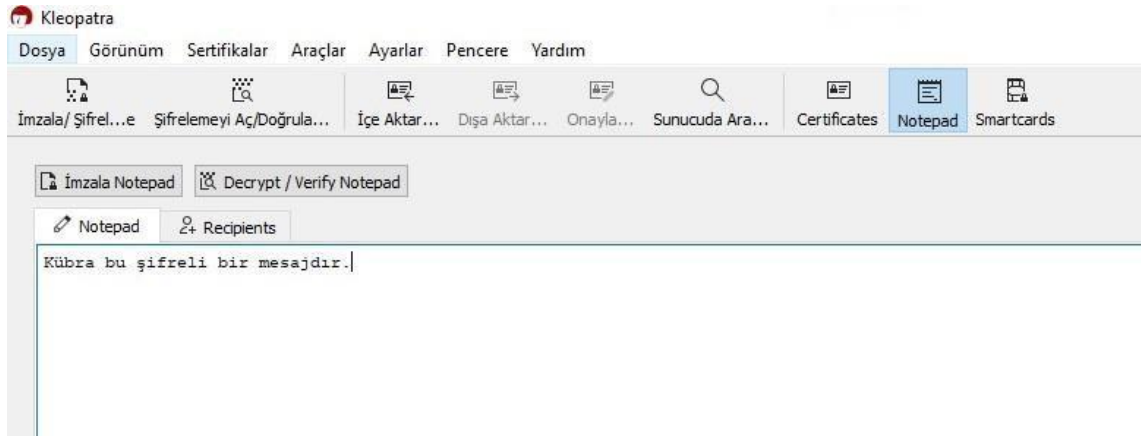


--

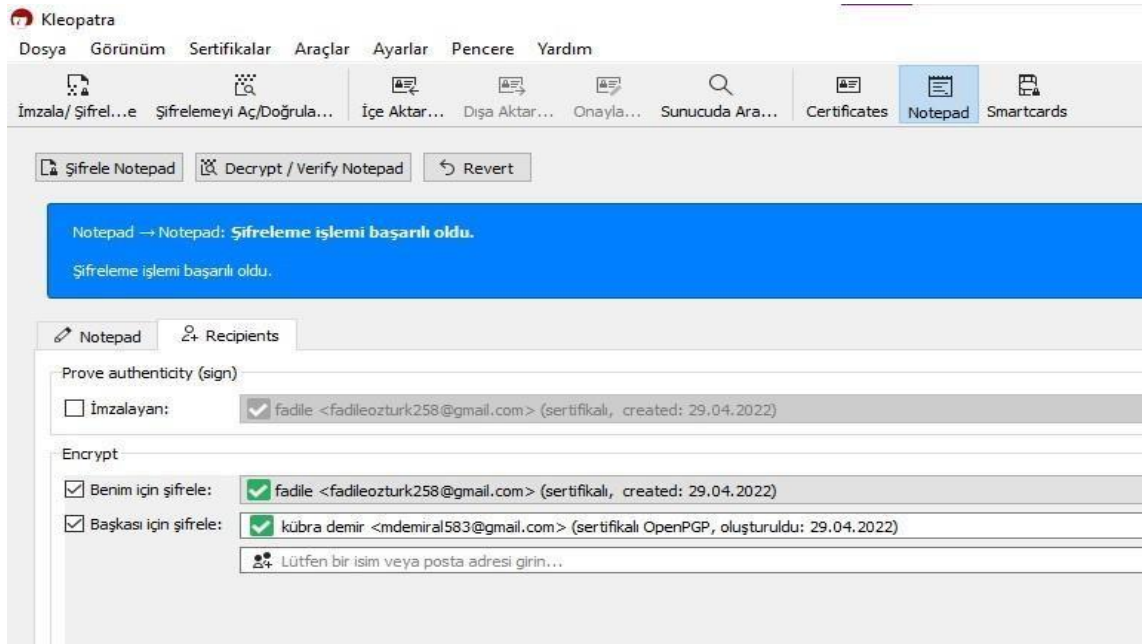
## 2-) KLEOPATRA KULLANILARAK ŞİFRELİ MESAJ OLUŞTURMA

PGP şifrelemesi, ortak anahtar şifrelemesini kullanarak metni şifreleme ve şifreyi çözme işlemidir. Herkese iki anahtar atanır: herkesle paylaşabileceğiniz genel bir anahtar (public) ve kendimize saklamış olduğumuz özel bir anahtar (private). Bu sistemi mümkün kılan ise kodların sadece tek yönlü çalışmasıdır. Örneğin X Anahtarı bir metni şifrelerse, X Anahtarı metnin şifresini çözemez. Sadece onun çifti olan Anahtar Y bunu yapabilir. Genellikle şu şekilde çalışır:

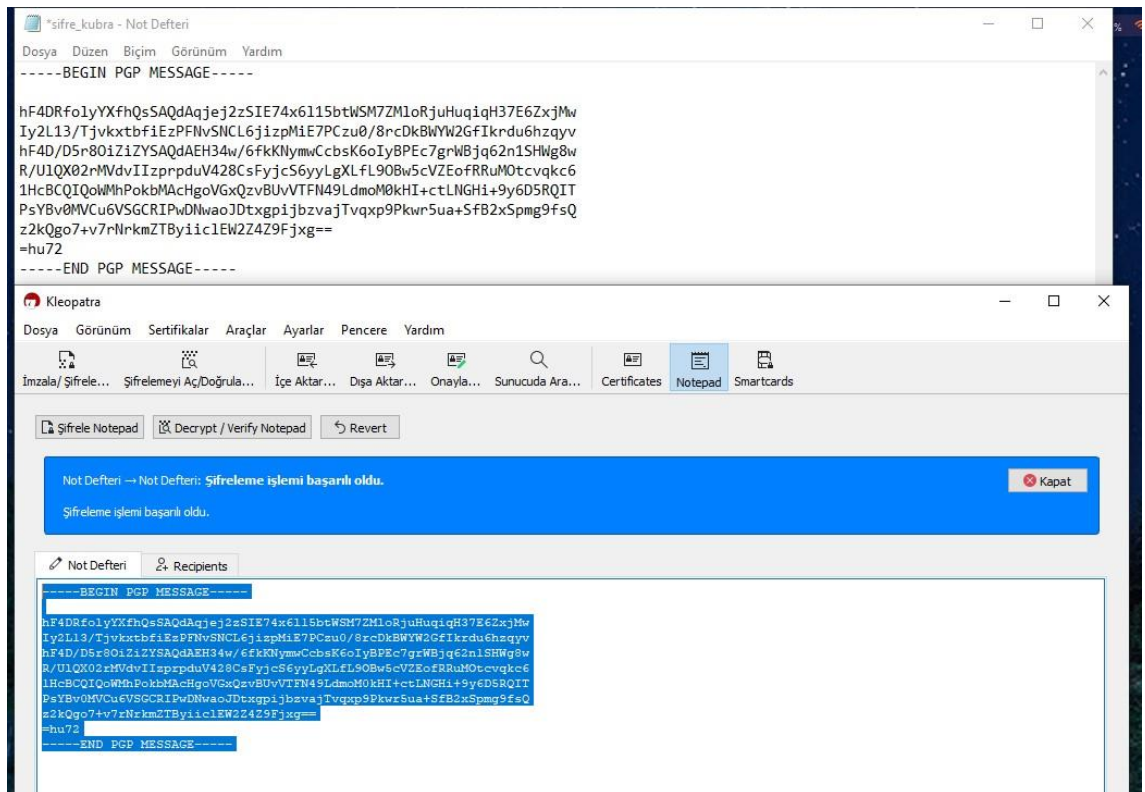
--Kleopatra uygulamasına gelip “Notepad” kısmında şifrelenmesini istediğimiz metni yazalım daha sonra “Recipients” seçeneğine tıklayıp imzalayan, benim için şifrele ve başkası için şifrele seçeneklerinden metnin sadece şifreli olmasını istediğimiz için benim için şifrele ve başkası için şifrele seçeneklerini aktifleştirip şifreyi çözmesini istediğimiz arkadaşımızın mail adresini giriyoruz.



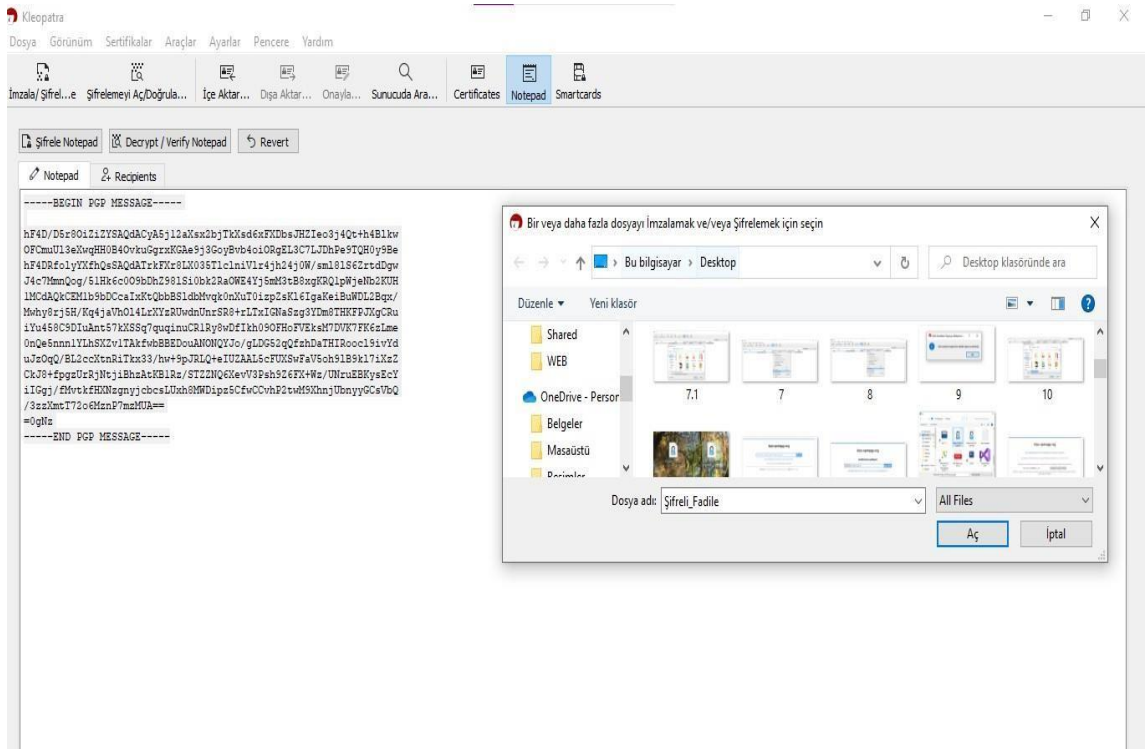
--Mail işlemlerini hallettikten sonra “Şifrele Notepad” kısmından şifreleme işlemini gerçekleştiriyoruz. Böylelikle bizim anlamlı olarak oluşturduğumuz mesaj karşı tarafın anlamayacağı şekilde kodlanmış oldu.



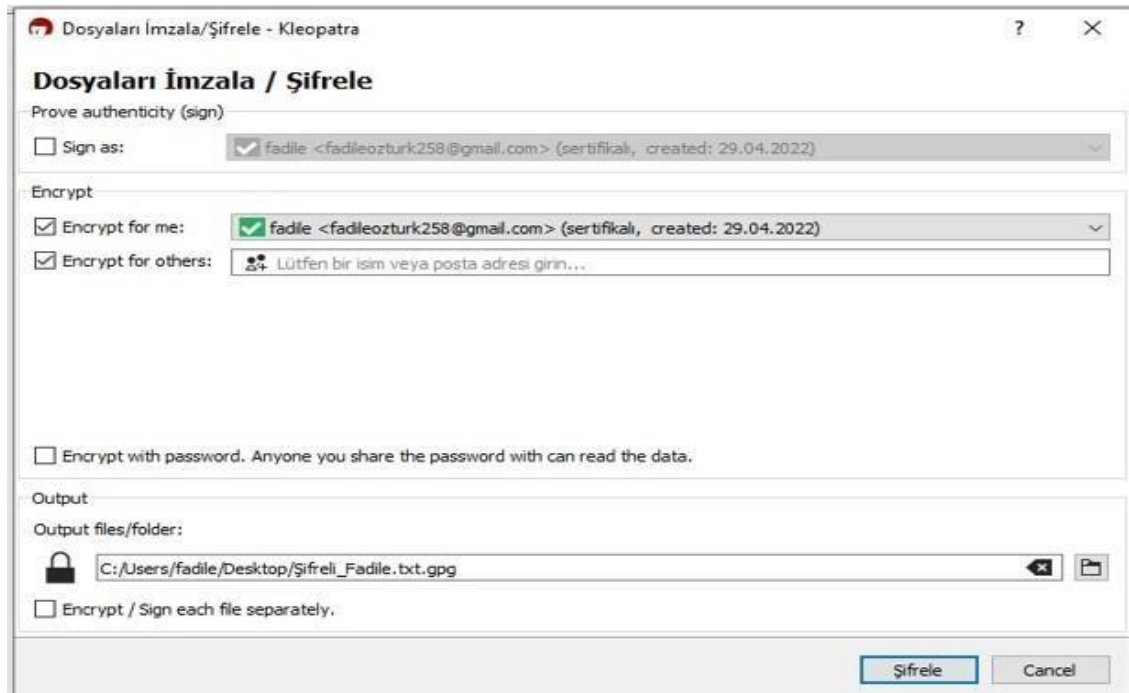
--Notepad kısmında şifreli mesajı kopyalayıp masaüstüne txt şeklinde kaydediyoruz. Daha sonra tekrar Kleopatra uygulamasına gelip şifrelediğimiz txt dosyasını imzala şifrele kısmından içe aktararak karşı tarafa iletmek için şifreleme yapıyoruz.

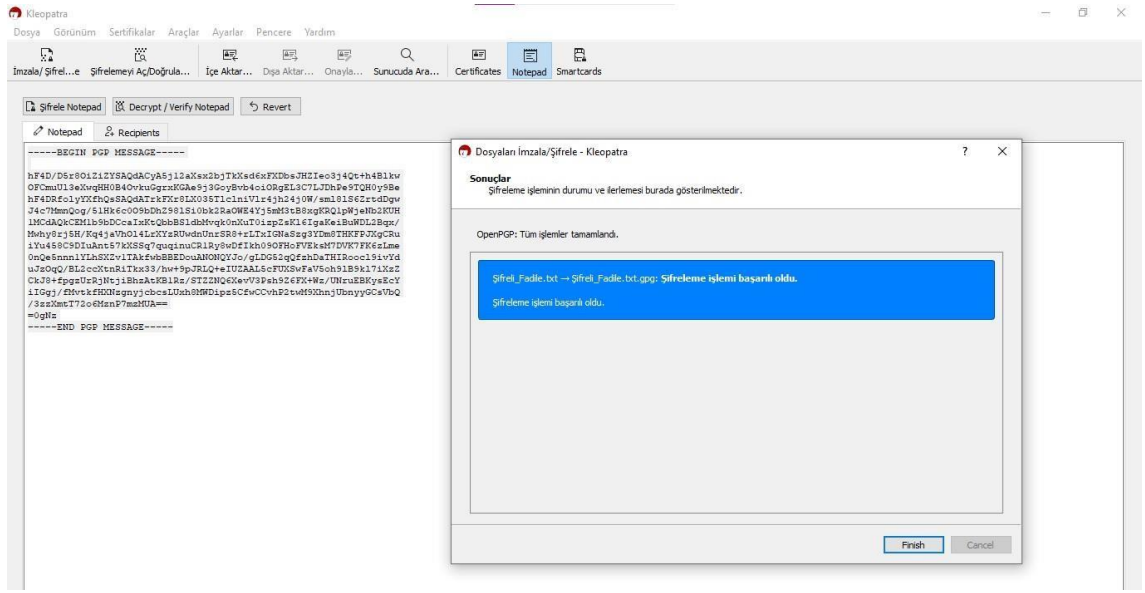


-- Şifrelenen mesaj masaüstüne şifreli\_Fadile.txt şeklinde ekleniyor.



--Daha sonra “sign as” haricindeki iki seçenek seçilerek şifrele işlemi yapılıyor





--Şifrelemiş olduğumuz metinleri karşılıklı olarak arkadaşımızla birbirimize attık ve birbirimizin şifresini çözmeyi başardık.



## Encrypt



Rastgele Mail <mdemiral583@gmail.com>

23:32



Kime: fadileozturk258@gmail.com



sifre\_kubra.txt.gpg  
914 bayt

Kimden: fadileozturk258@gmail.com



Kime: mdemiral583@gmail.com;



Bilgi ve Gizli

Şifreli Mesaj ;

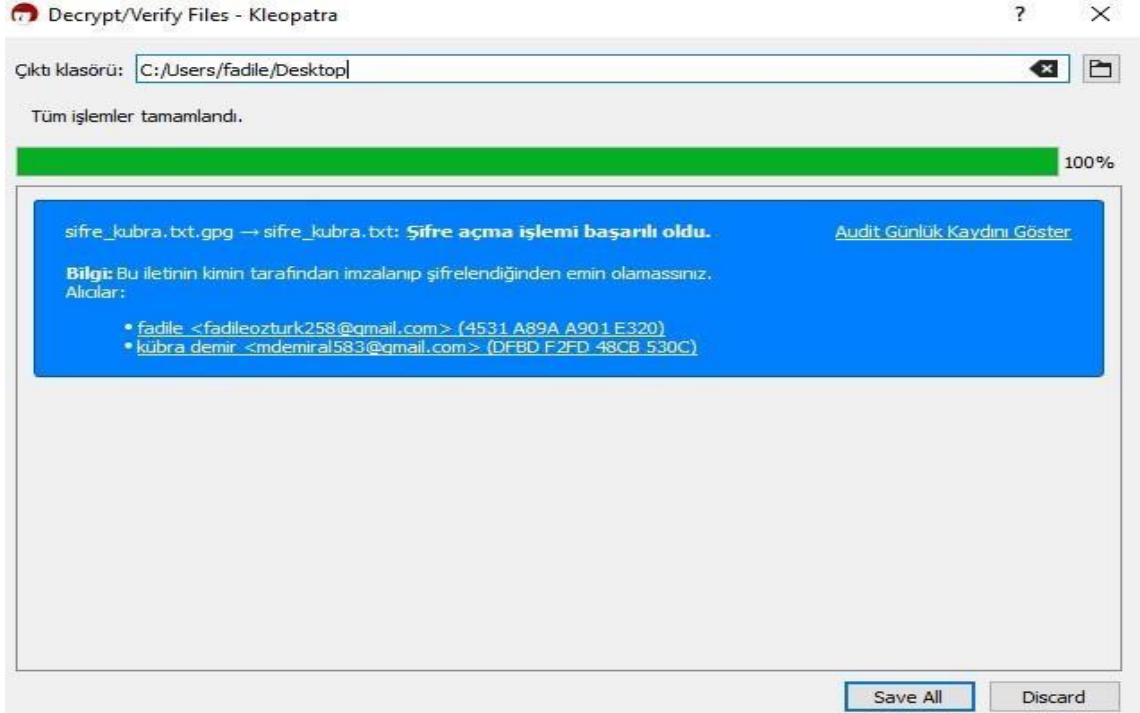
Ekler



Şifreli\_Fadile.txt.gpg  
819 bayt



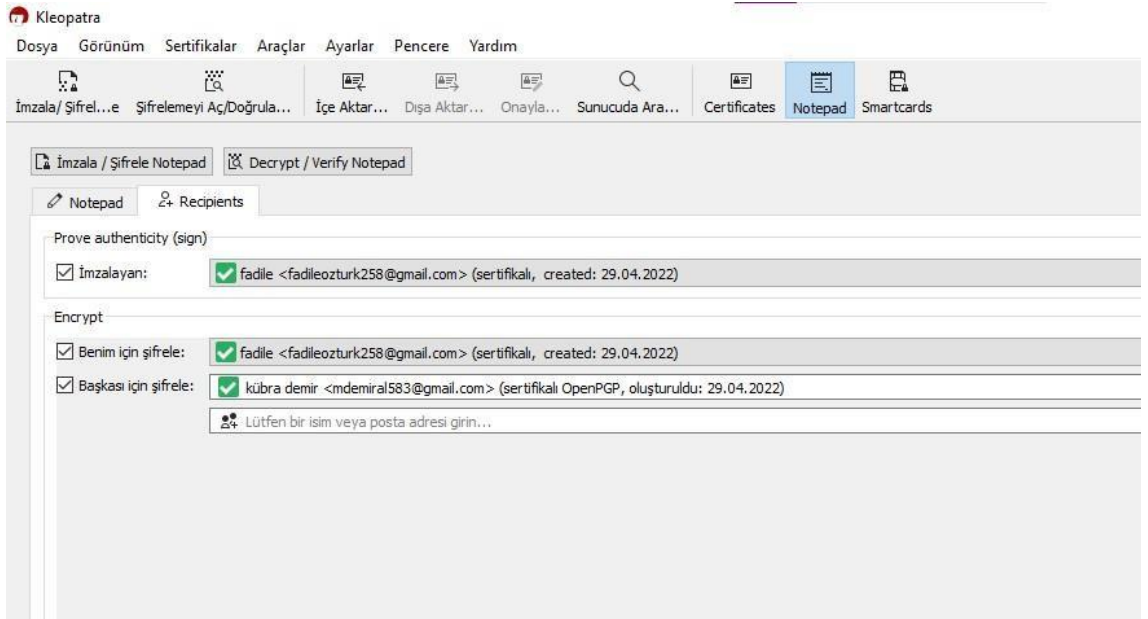
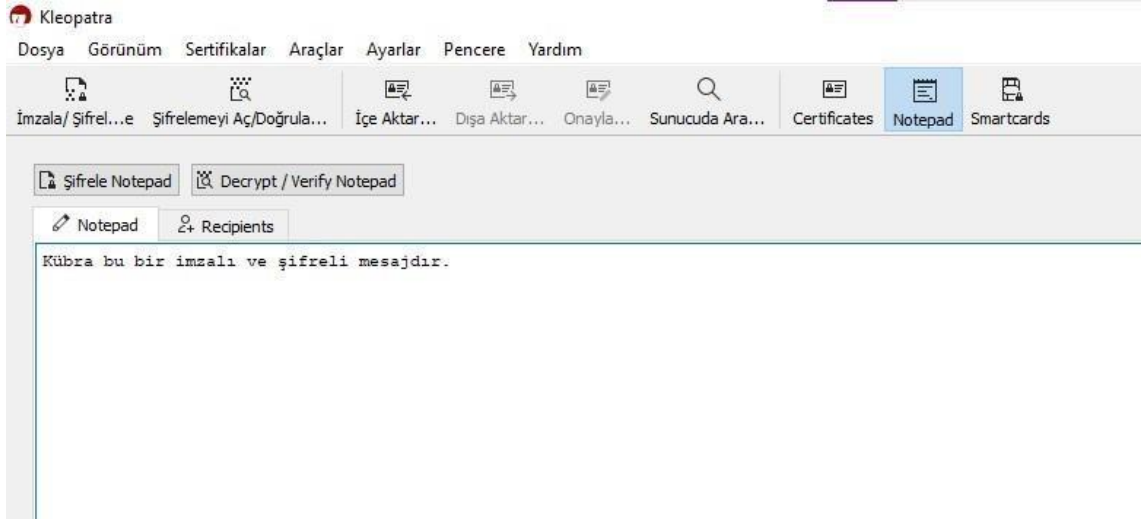
Windows için [Posta](#) ile gönderildi

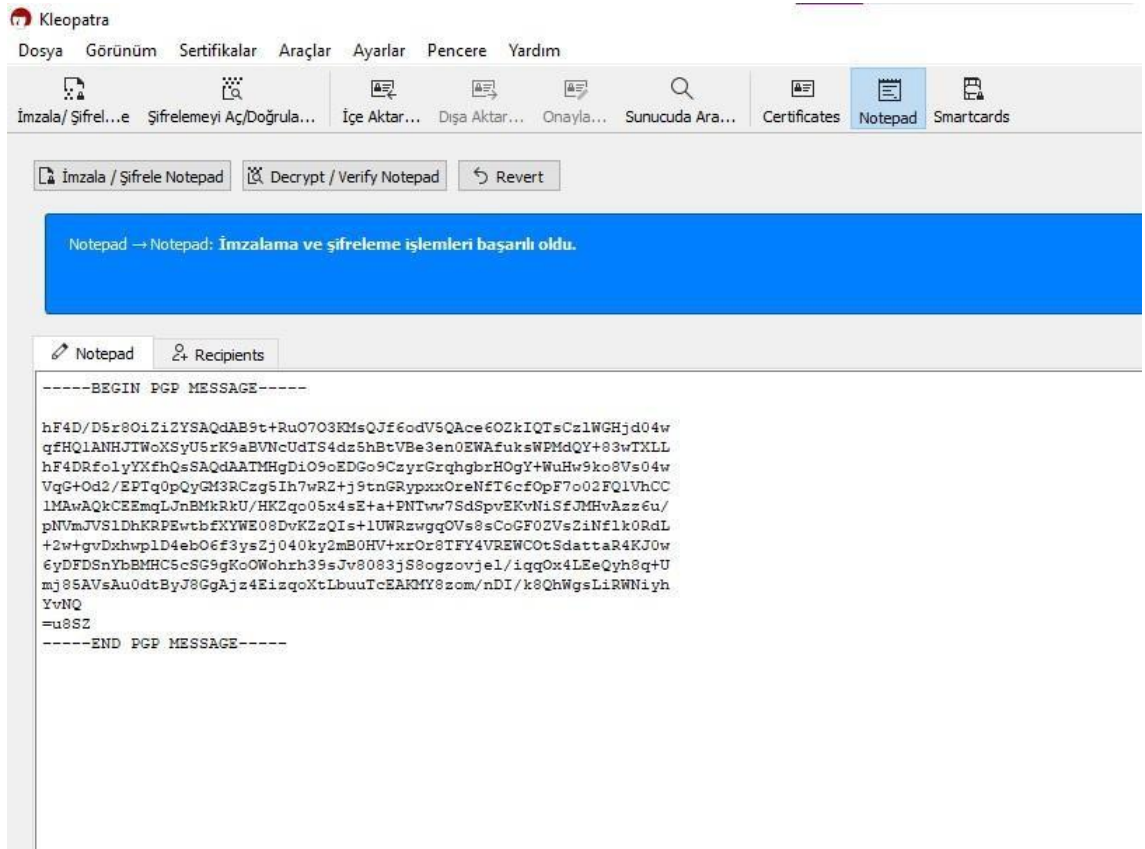
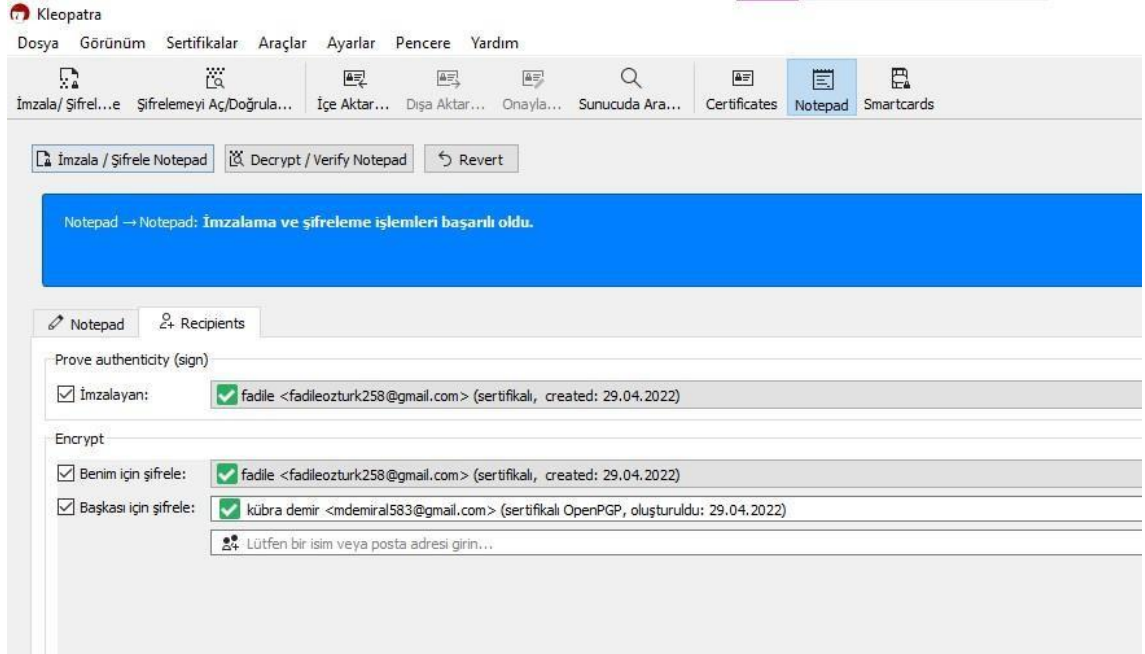




### 3-) KLEOPATRA KULLANILARAK ŞİFRELİ VE İMZALI MESAJ OLUŞTURMA

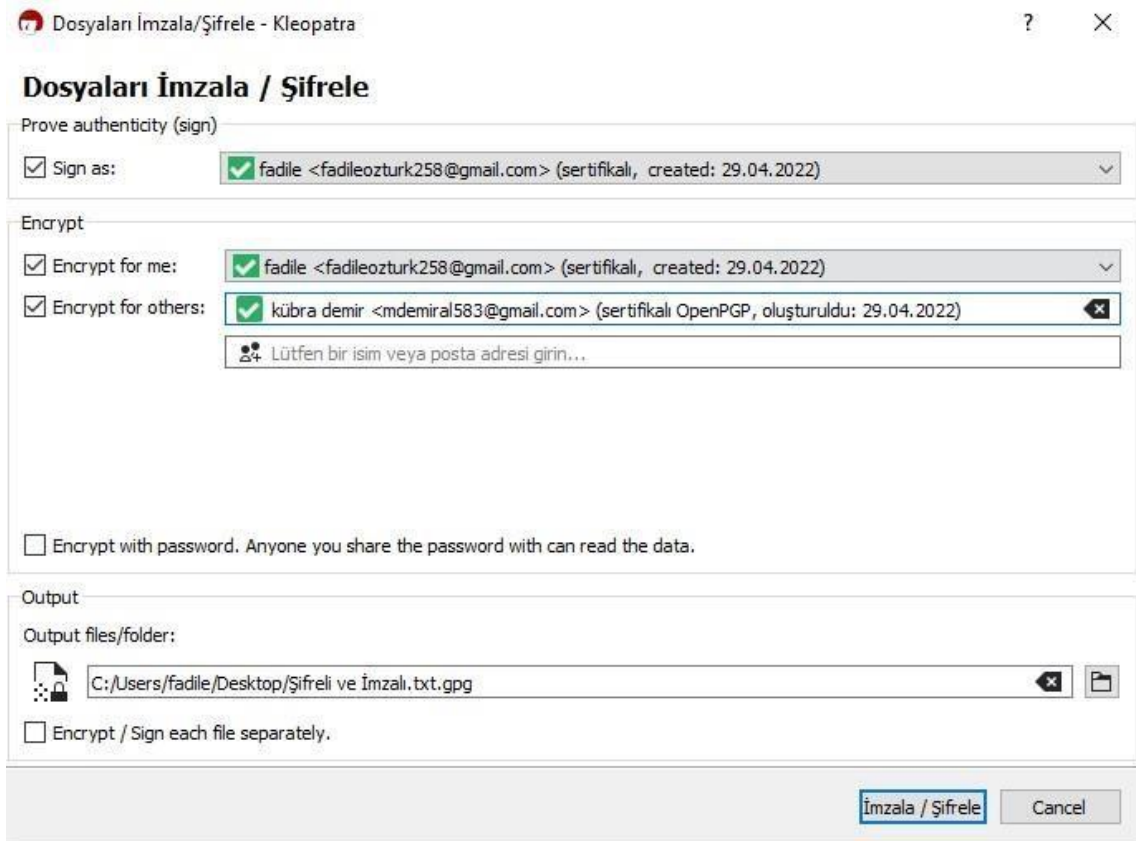
Şimdide Kleopatra ve OpenPGP sertifikalarını kullanarak yazmış olduğumuz metni hem şifreleyip hem de imzalama işlemlerini gerçekleştirelim. Öncelikle şifreleyip imzalamak istediğimiz metni Kleopatra uygulamasının Notepad kısmına yazıyoruz. Daha sonra tekrar Recipients sekmesine tıklayıp oluşturduğumuz metni sertifika kullanarak imzala ve şifrele sekmelerini aktifleştiriyoruz ve başkası için şifrele kısmına karşı tarafın mail adresini giriyoruz. Üst kısımda beliren “İmzala/ Şifrele Notepad” seçeneğine tıklıyoruz böylelikle metnimiz şu an hem şifreli hem de imzalı hale gelmiş oluyor.

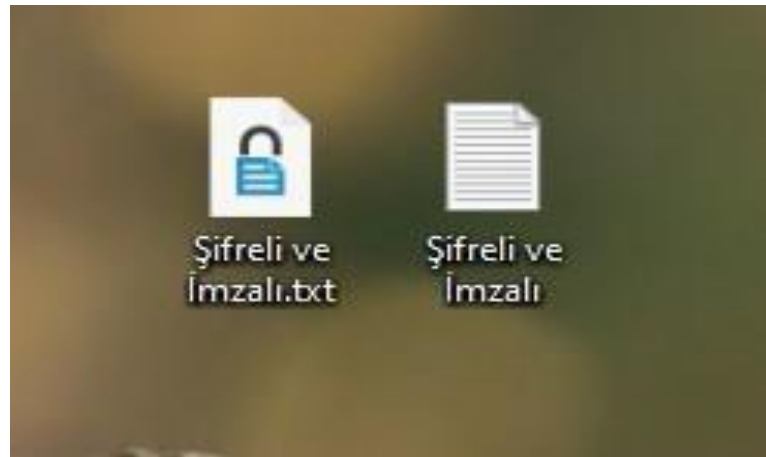
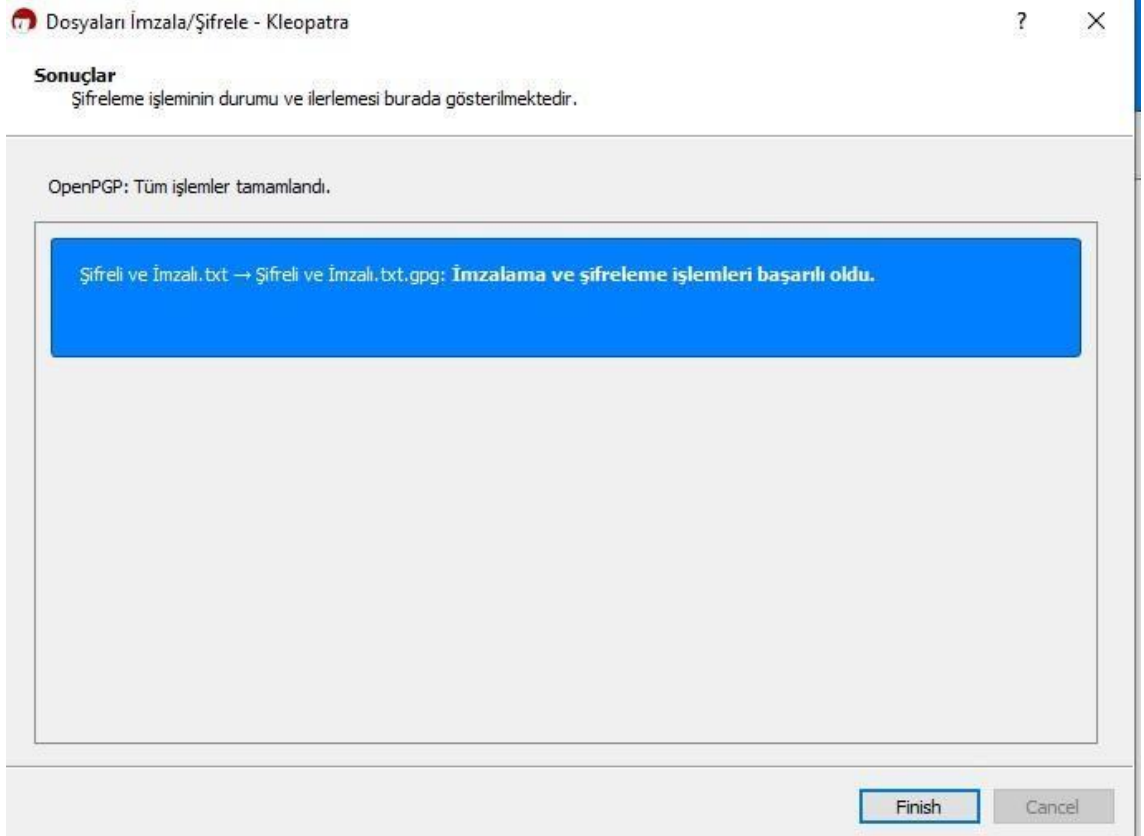




Daha sonra imzalayıp şifreleme de olduğu gibi burada da imzaladığımız ve şifrelediğimiz metni bir txt dosyası içine kaydediyoruz. Diğer işlemlerde olduğu gibi burada da şifrelediğimiz txt dosyasını kleopatraya aktarıp dosyaları imzala ve şifrele seçeneğine

tıkıyoruz böylelikle metnimizin hem normal txt dosyası hem de şifreli ve imzalı txt dosyası masaüstüne eklenmiş oluyor.





Son olarak metnimizin şifreli ve imzalı halini de arkadaşımızla karşılıklı paylaşarak birbirimizin metinlerini açmayı deniyoruz ve işlem başarıyla gerçekleştiriliyor.

Kimden: fadileozturk258@gmail.com



Kime: mdemiral583@gmail.com;



Bilgi ve Gizli

Şifreli Ve İmzalı ;

Ekler



Şifreli ve imzalı.txt.gpg  
978 bayt



Windows için [Posta](#) ile gönderildi

Kimden: fadileozturk258@gmail.com



Kime: mdemiral583@gmail.com;



Bilgi ve Gizli

Şifreli Ve İmzalı ;

Ekler



Şifreli ve imzalı.txt.gpg  
978 bayt



Windows için [Posta](#) ile gönderildi



