RSA Şifreleme Uygulaması Proje Raporu

- ***Proje Tanımı ve Amacı:***

RSA Şifreleme Uygulaması, RSA (Rivest-Shamir-Adleman) şifreleme algoritmasını kullanarak metin ve dosyaları şifrelemek ve çözmek için bir arayüz sağlar. Bu uygulama, public ve private key yöntemleri kullanılarak kullanıcıların verilerini güvenli bir şekilde iletmelerini ve depolamalarını sağlayarak veri güvenliği ve bütünlüğü sağlar.

- ***Kullanım Özellikleri:***

Anahtar Oluşturma: Kullanıcı, istediği anahtar boyutunu belirterek RSA anahtar çiftleri oluşturabilir.

Metin Şifreleme ve Çözme: Kullanıcılar, metinleri belirledikleri anahtarlarla şifreleyebilir ve şifrelenmiş metinleri çözebilir.

Dosya Şifreleme ve Çözme: Kullanıcılar, metin dosyalarını şifreleyebilir ve şifreli dosyaları çözebilir.

Kullanıcı Arayüz: Python'da Tkinter kütüphanesi kullanılarak basit bir arayüz tasarlanmıştır.

Hata Kontrolü: Kullanıcı girişleri ve dosya işlemleri sırasında hata kontrolü sağlanmıştır.

- ***Kullanılan Programlama Dili ve Kütüphaneleri:***

Proje, Python programlama dili kullanılarak geliştirilmiştir.

Kullanıcı arayüzü için Tkinter kütüphanesi kullanılmıştır.

Asal sayı üretimi ve modüler ters alma gibi matematiksel işlemler için SymPy kütüphanesi kullanılmıştır.

Ek olarak random ve hashlib modülülleri kullanılmıştır.

- ***Güvenlik:***

Veri Güvenliği: RSA algoritması, güçlü bir şifreleme algoritması olarak bilinir ve kullanıcıların verilerini güvenli bir şekilde iletmelerini sağlar.

Hata Kontrolü: Kullanıcı girişleri ve dosya işlemleri sırasında hata tespitleri yapılmıştır.

Anahtar Yönetimi: Kullanıcıların oluşturduğu anahtarlar güvenli bir şekilde saklanmalı ve yönetilmelidir.

- ***Sonuç:***

RSA Şifreleme Uygulaması, kullanıcıların metin ve metin dosyalarını şifrelemelerini ve çözmelerini sağlar. Çok büyük anahtar boyutu tercih edildiğinde metin kutusuna girilen metnin programı yavaşlattığı görülmüştür. Bu yüzden test aşamasında metin kutusuna girilen metinler kısa tutulmuştur. Programın dosya şifreleme ve şifre çözme kısmında ise şifreleme esnasında herhangi bir zaman gecikmesi ve uzunluk sınırı olmadan metin dosyasını rahatlıkla şifrelediği, şifreli dosyayı çözerken ise aynı metin şifreleme ve şifre çözümündeki yavaşlık tespit edilmiştir. Bu yüzden test aşamalarında küçük anahtar boyutu ile testler gerçekleştirilmiştir. İlerleyen süreçte algoritma iyileştirilip daha verimli ve hızlı hale dönüştürülebilir.

- ***Kaynak:***

https://www.youtube.com/watch?v=ZkWW21k1QTw

https://medium.com/albaraka-tech-global/rsa-ile-encryption-decryption-i%CC%87%C5%9Flemleri-5fa70d15f3e6

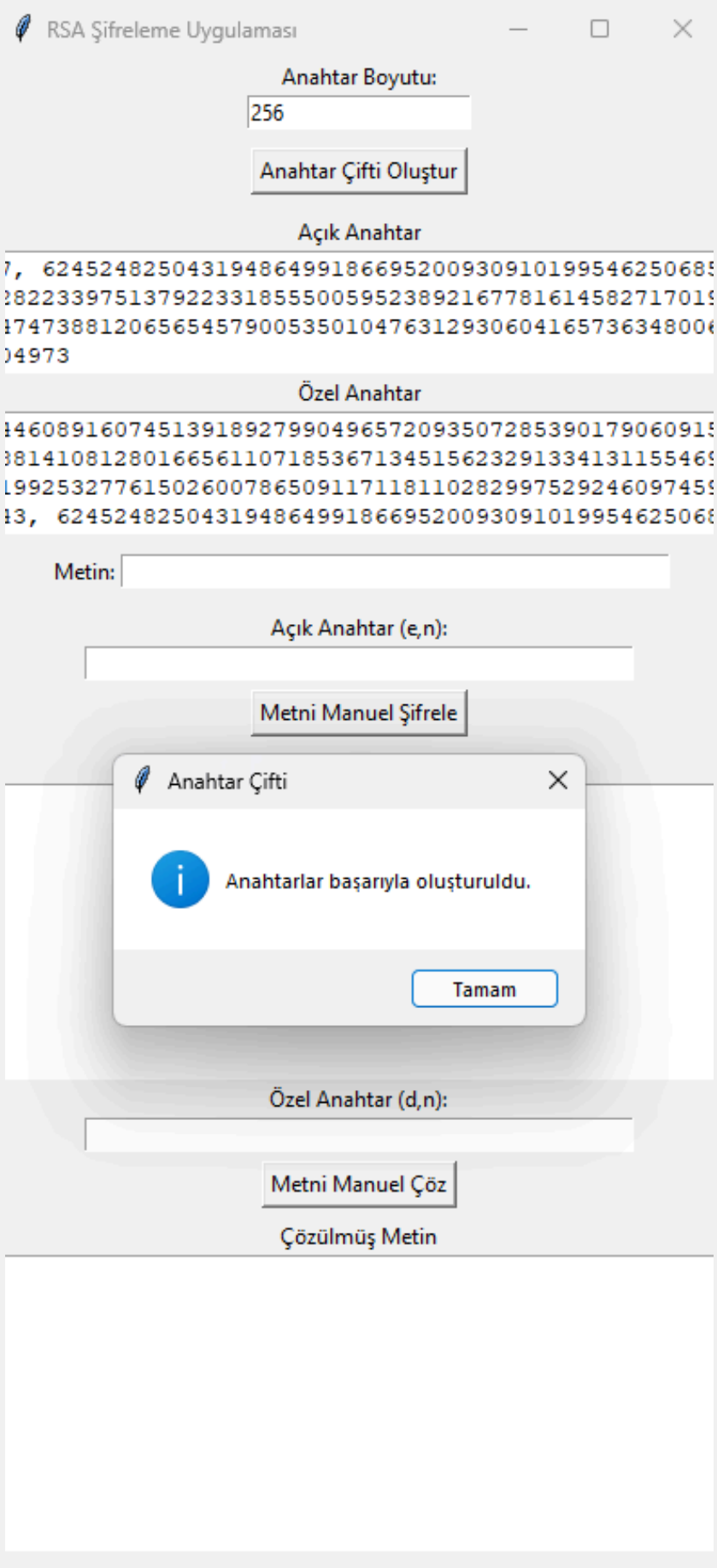
https://feyzatopcu.medium.com/rsa-%C5%9Fi%CC%87freleme-algori%CC%87tmasi-78347f748ed2

https://www.clickssl.net/blog/what-is-rsa

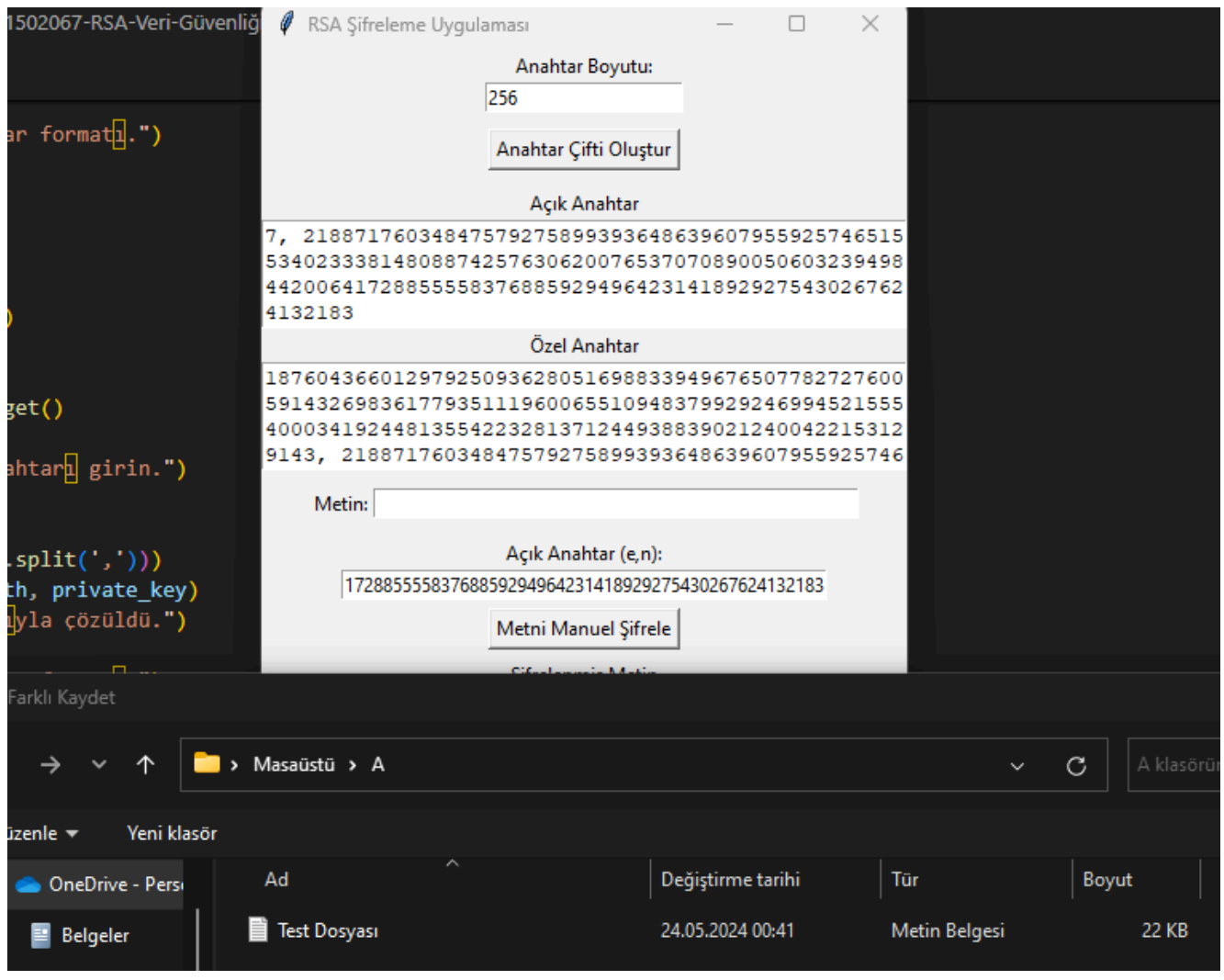
Gemini

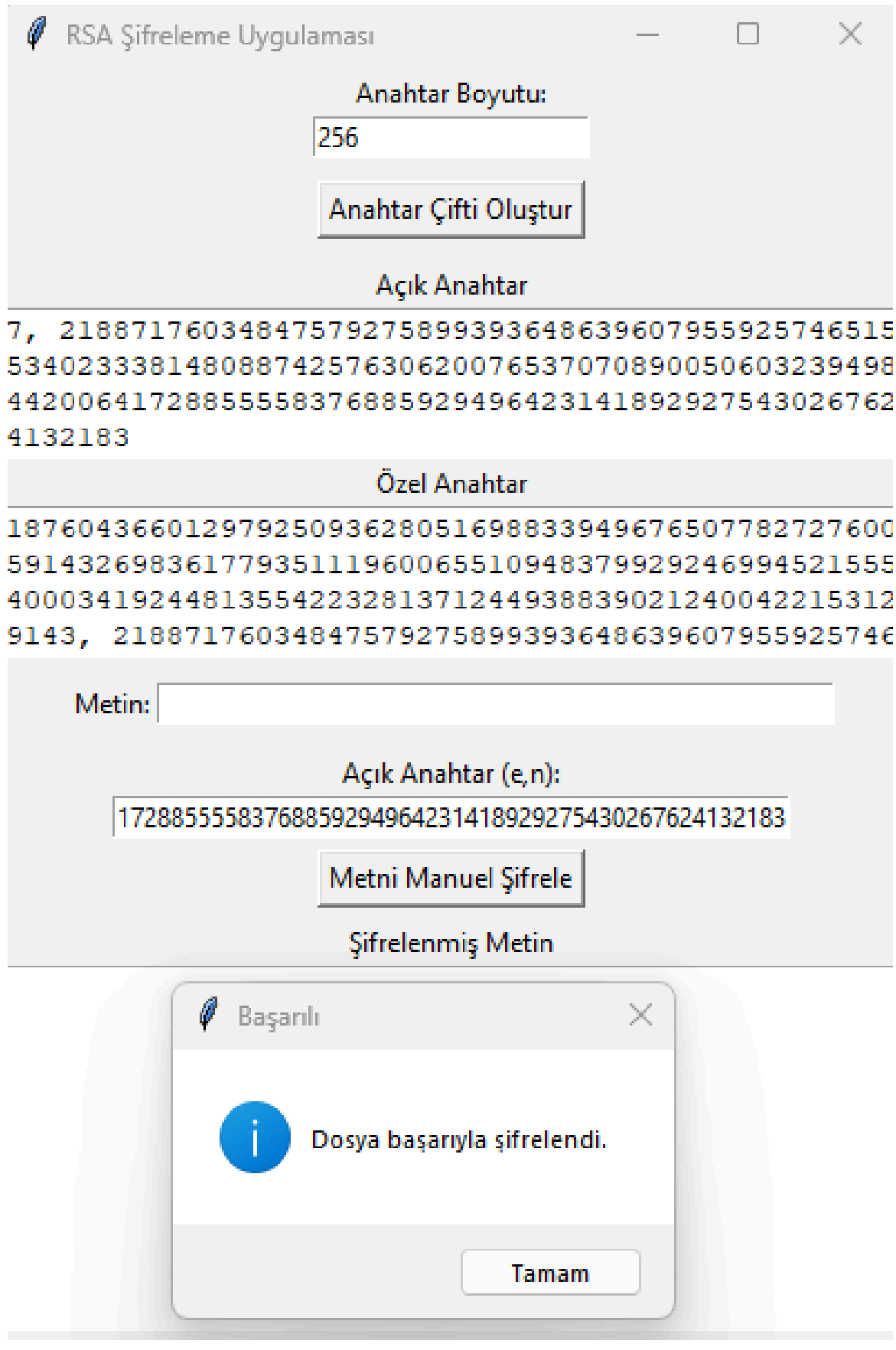
ChatGPT

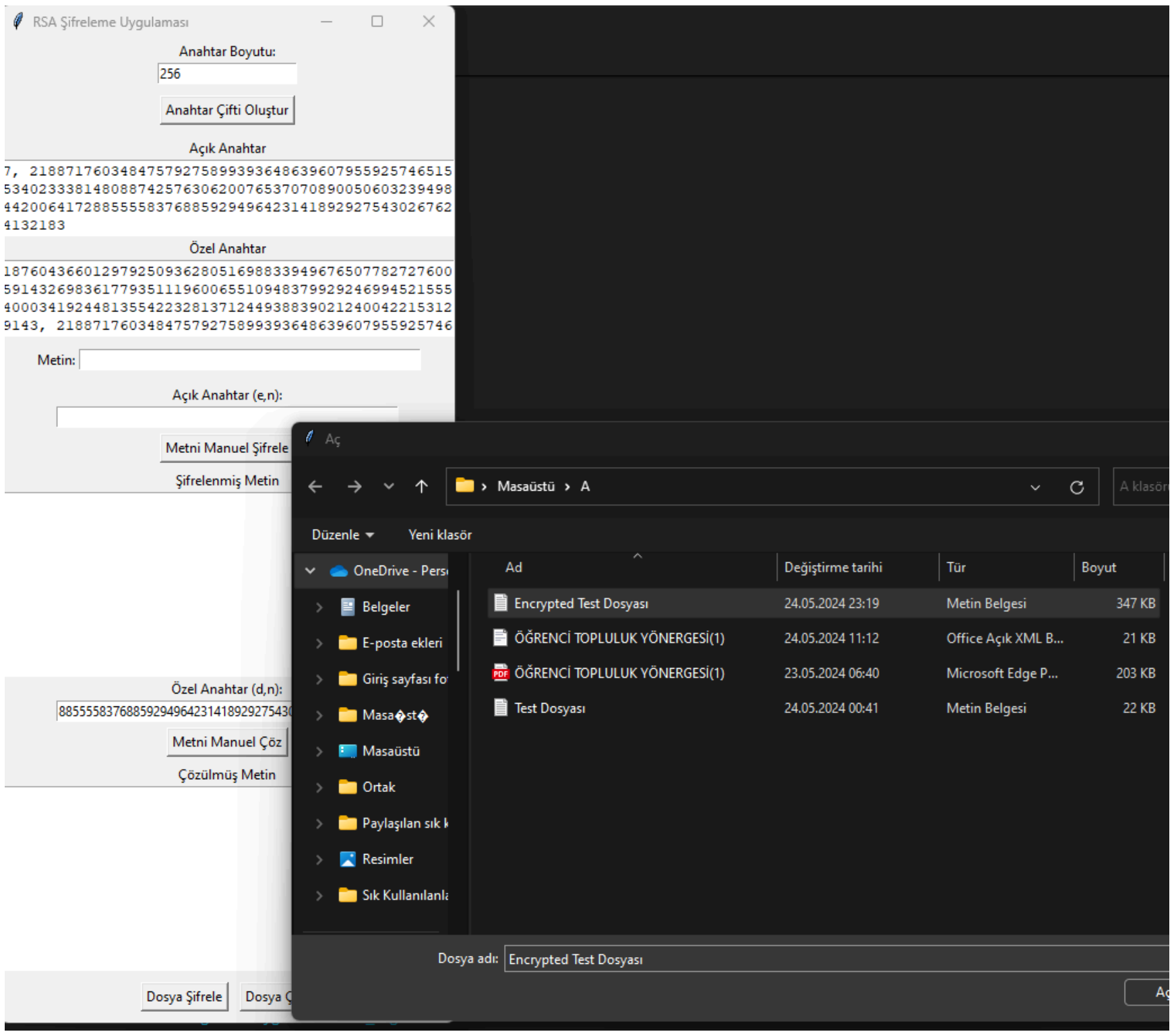
Metin kutusu kullanarak Şifreleme - Şifre Çözme

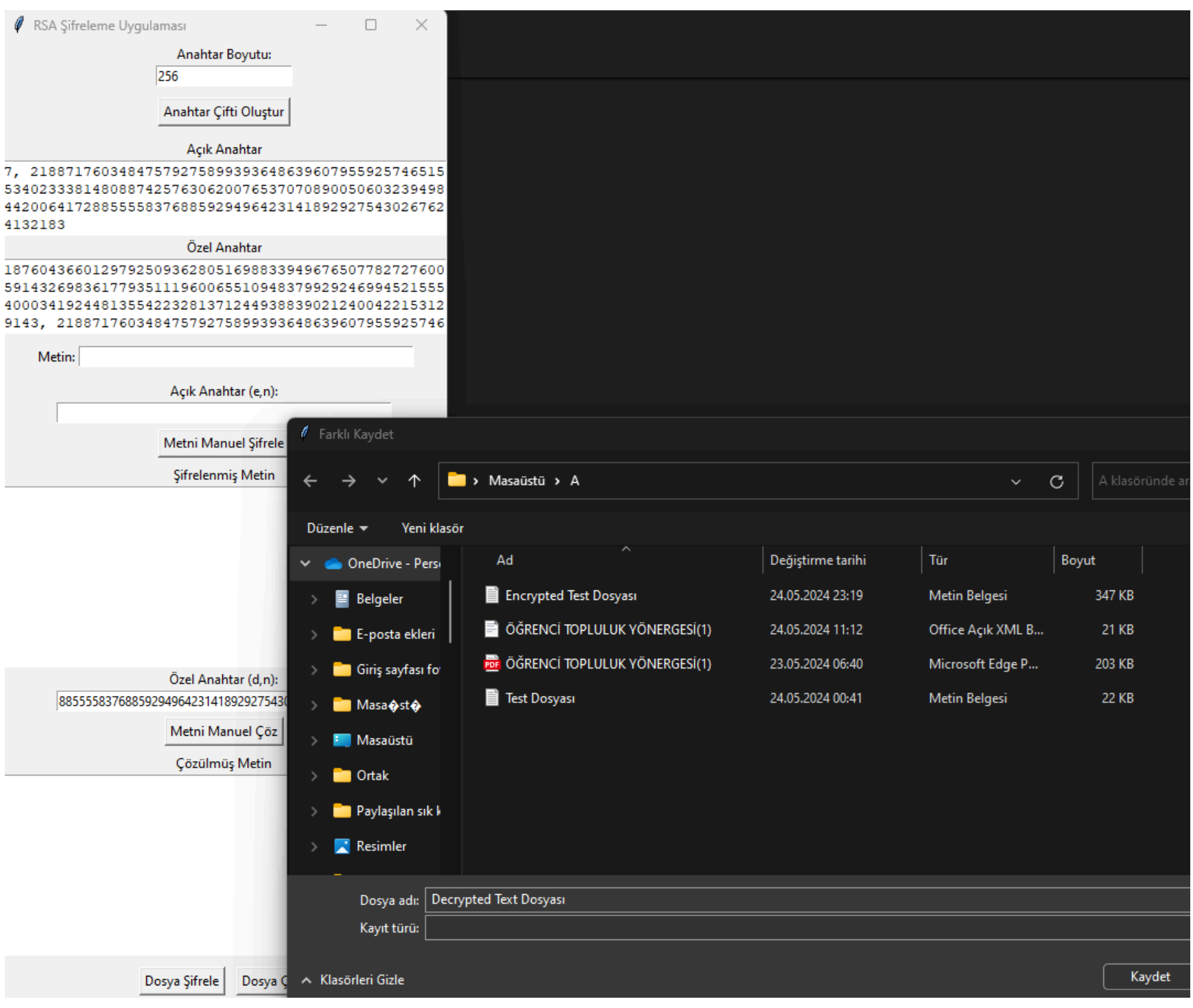


Metin belgesi kullanarak Şifreleme - Şifre Çözme






RSA Şifreleme Uygulaması
Anahtar Boyutu:
256
Anahtar Çifti Oluştur
Açık Anahtar
7, 218871760348475792758993936486396079559257465155340233381480887425763062007653707089005060323949844200641728855558376885929496423141892927543026762413218 3
Özel Anahtar
1876043660129792509362805169883394967650778272760059143269836177935111960065510948379929246994521555400034192448135542232813712449388390212400422153129143, 218871760348475792758993936486396079559257465
Metni Manuel Şifrele
Şifrelenmiş Metin
Özel Anahtar (d,n):
Metni Manuel Çöz
Çözülmüş Metin
Dosya Şifrele
Aç
Masaüstü › A
Düzenle
Yeni klasör
OneDrive - Pers
Belgeler
E-posta ekleri
Giriş sayfası fo
Masa st
Masaüstü
Ortak
Paylaşılan sık k
Resimler
Sık Kullanılanl
Ad
Değiştirme tarihi
Tür
Boyut
Encrypted Test Dosyası
24.05.2024 23:19
Metin Belgesi
347 KB
ÖĞRENCİ TOPLULUK YÖNERGESİ(1)
24.05.2024 11:12
Office Açık XML B...
21 KB
ÖĞRENCİ TOPLULUK YÖNERGESİ(1)
23.05.2024 06:40
Microsoft Edge P...
203 KB
Test Dosyası
24.05.2024 00:41
Metin Belgesi
22 KB
Dosya adı:
Encrypted Test Dosyası


RSA Şifreleme Uygulaması
Anahtar Boyutu:
256
Anahtar Çifti Oluştur
Açık Anahtar
7, 218871760348475792758993936486396079559257465155340233381480887425763062007653707089005060323949844200641728855558376885929496423141892927543026762413218 3
Özel Anahtar
1876043660129792509362805169883394967650778272760059143269836177935111960065510948379929246994521555400034192448135542232813712449388390212400422153129143, 218871760348475792758993936486396079559257465
Metni Manuel Şifrele
Şifrelenmiş Metin
Özel Anahtar (d,n):
Metni Manuel Çöz
Çözülmüş Metin
Dosya Şifrele
Farklı Kaydet
Masaüstü › A
Düzenle
Yeni klasör
OneDrive - Pers
Belgeler
E-posta ekleri
Giriş sayfası fo
Masa st
Masaüstü
Ortak
Paylaşılan sık k
Resimler
Ad
Değiştirme tarihi
Tür
Boyut
Encrypted Test Dosyası
24.05.2024 23:19
Metin Belgesi
347 KB
ÖĞRENCİ TOPLULUK YÖNERGESİ(1)
24.05.2024 11:12
Office Açık XML B...
21 KB
ÖĞRENCİ TOPLULUK YÖNERGESİ(1)
23.05.2024 06:40
Microsoft Edge P...
203 KB
Test Dosyası
24.05.2024 00:41
Metin Belgesi
22 KB
Dosya adı:
Decrypted Text Dosyası
Kayıt türü:
Klasörleri Gizle
Kaydet

RSA Şifreleme Uygulaması

Anahtar Boyutu:

256

Anahtar Çifti Oluştur

Açık Anahtar

```
7, 218871760348475792758993936486396079559257465 15
534023338148088742576306200765370708900506032394 98
442006417288555583768859294964231418929275430267 62
4132183
```

Özel Anahtar

```
187604366012979250936280516988339496765077827276 00
591432698361779351119600655109483799292469945215 55
400034192448135542232813712449388390212400422153 12
9143, 218871760348475792758993936486396079559257 46
```

Metin:

Açık Anahtar (e,n):

Metni Manuel Şifrele

Şifrelenmiş Metin

Başarılı

Dosya başarıyla çözüldü.

Tamam

Özel Anahtar (d,n):

88555583768859294964231418929275430267624132183

Metni Manuel Çöz

Çözülmüş Metin

Dosya Şifrele

Dosya Çöz