T.C.

BİTLİS EREN ÜNİVERSİTESİ

MÜHENDİSLİK-MİMARLIK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

PROJENİN RAPORU

PROJENİN ADI

RSA ŞİFRELEME YÖNTEMİ

HAZIRLAYAN

Mecdiddin EBUŞERFO

**Dr.Öğr.Üyesi Songül Karakuş**

ARALIK 2023

**ONAY**

Mecdiddin EBUŞERFO

tarafından hazırlanan “**E-ÖĞRENME**”adlı projesi 29/12/2023 tarihinde Bilgisayar Mühendisliği Bölümünde **Dr.Öğr.Üyesi Songül Karakuş** tarafından ***başarılı / başarısız*** olarak kabul edilmiştir.

**ÖZET**

RSA ŞİFRELEME VE DE ŞEFRELEME YÖNTEMİ C# FORM ÜZERENDE YAPILDI

**EBUŞERFO ,Mecdiddin**

Projen Raporu

Bitlis Eren Üniversitesi Mühendislik Mimarlık Fakültesi

Bilgisayar Mühendisliği Bölümü

**Dr.Öğr.Üyesi Songül Karakuş**

**ARALIK 2023, 10 Sayfa**

**Anahtar kelimeler**: RSA ŞİFRELEME VE DE ŞEFRELEME YÖNTEMİ

**TEŞEKKÜR**

Proje çalışması sırasında her türlü bilgi, teşvik ve deneyimleri ile yardımlarını esirgemeyen

**Dr. Öğr. Üyesi Songül Karakuş**’a ve yüksek öğrenim süresince her türlü maddi ve manevi destekleri ile göstermiş oldukları sabırdan dolayı teşekkür ederim.

* **GİRİŞ**

Şifreleme olmasaydı hesaplarımız ve özel bilgisayarımız hacklenmeye açık olurdu, evimizin kilitleri ve anahtarları olmasaydı çalınırdı ama bunu engelleyen şey kilittir ki o da aynı şekilde dijital dünyamıza şifreleme denir.

* **Materyaller**

1. Text editor olarak visual studio kullanilacaktir

* **1.1 Materyaller**

Bu bölümde projede kullanılacak bilgisayar yazılımları, veri toplama araçları, veri setleri, cihazlar vs tanıtılmalıdır.

* **1.1.1** **Visual Studio**

Microsoft tarafından geliştirilen ve Windows platformunda çalışan

tümleşik bir geliştirme ortamıdır (IDE). Yazılım geliştiriciler, Windows uygulamaları, web siteleri, mobil uygulamalar, oyunlar ve daha Fazlası,için kod yazabilir, hata ayıklayabilir, test edebilir ve dağıtabilir. Visual Studio, C#, Visual Basic, C++, Python ve JavaScript gibi birçok programlama dilini destekler. Ayrıca geliştirme sürecinizi daha verimli hale getirmek için Visual Studio, Git, Azure gibi birçok entegrasyon ve diğer birçok araç sunar.[7]

**2. RSA Şifreleme Yöntemi Nedir?**

RSA, şifreleme ve dijital imza oluşturma gibi kriptografik uygulamalar için kullanılan açık anahtarlı bir şifreleme algoritmasıdır. RSA, 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir ve adını bu üç matematikçinin soyadlarının baş harflerinden almıştır.

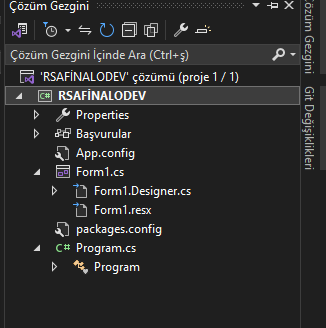
RSA'nın temel prensibi, iki büyük asal sayı seçilerek bu sayılarla bir genel anahtar (public key) ve bir özel anahtar (private key) çifti oluşturulmasıdır. Genel anahtar herkese açık bir şekilde paylaşılırken, özel anahtar sadece sahibi tarafından bilinir.

* **3. İŞ ZAMAN ÇİZELGESİ VE İŞ PAKETLERİ**

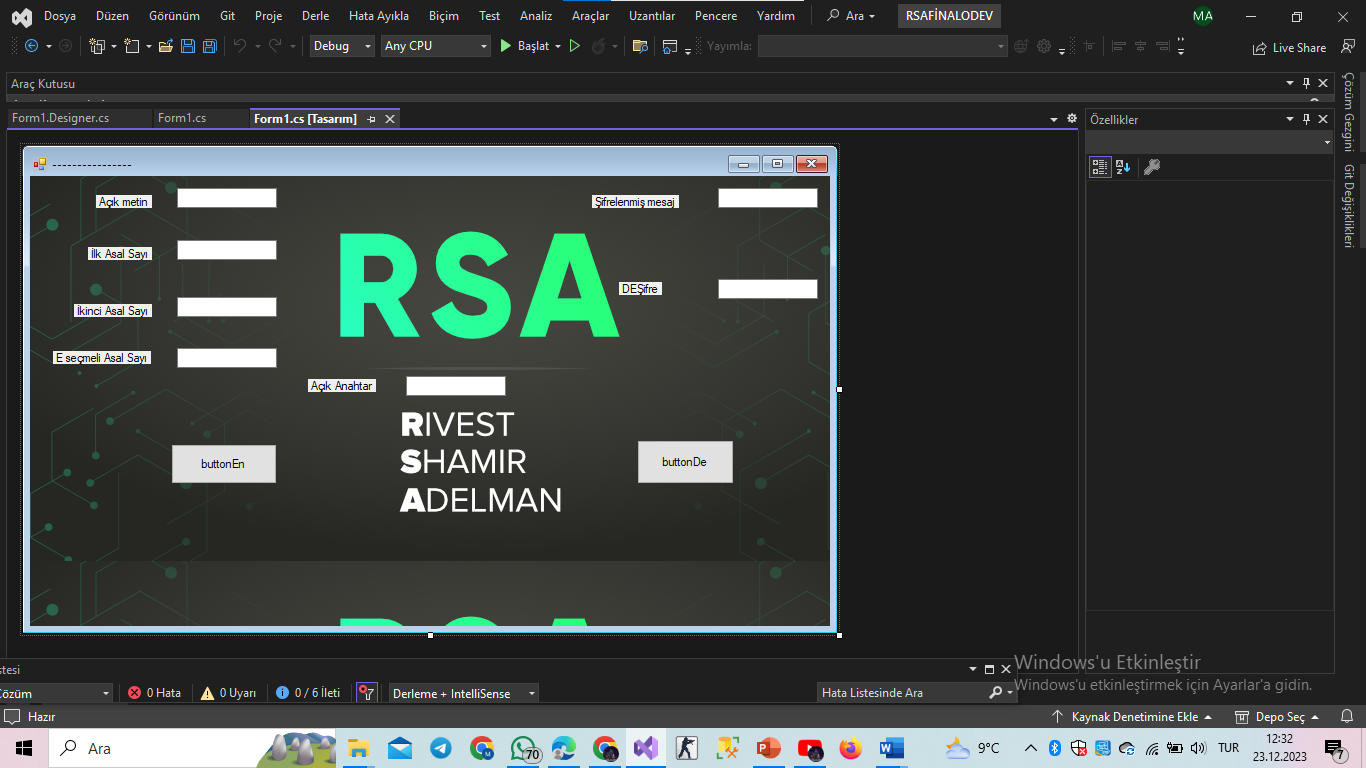
|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| İş Paketleri | **PROJE ADI:**  **RSA ŞİFRELEME YÖNTEMİ** | **ARALIK**  **İLK HAFTA** | | **ARALIK İKİNCİ HAFTA** | | | **ARALIK ÜÇÜNCÜ HAFTA** | | | | |
| PAZ | SALI | PAZ | PZT | SALI | PAZ | PZT | SALI | ÇAR | PER |
| 1 | ***Araştırması ve tasarım (C#FORM )*** |  |  |  |  |  |  |  |  |  |  |
| Tasarımın on planı  Tasarımın koda dökme sureci |  |  |  |  |  |  |  |  |  |  |
| Tasarımın responsive yapılması |  |  |  |  |  |  |  |  |  |  |
| 2 | ***Kullanılacak Program ve*** ***Kütüphanelerin Araştırılması(C#)Tarafı*** |  |  |  |  |  |  |  |  |  |  |
| Program dili araştırıp ve kararlaştırılması |  |  |  |  |  |  |  |  |  |  |
| Kütüphane araştırıp ve kararlaştırılması |  |  |  |  |  |  |  |  |  |  |
| 4 | ***Kodların Yazılması*** |  |  |  |  |  |  |  |  |  |  |
| RSA kodlarin yazilmasi |  |  |  |  |  |  |  |  |  |  |
| Tüm bileşenlerin birbiriyle bağlanması |  |  |  |  |  |  |  |  |  |  |
| Kodların test edilmesi |  |  |  |  |  |  |  |  |  |  |
| 5 | ***Dokümantasyon Hazırlanması*** |  |  |  |  |  |  |  |  |  |  |
| Rapor yazılması |  |  |  |  |  |  |  |  |  |  |
| Sunum hazırlanması |  |  |  |  |  |  |  |  |  |  |

**Çizelge 3.1.** İş paketleri ve zaman çizelgesi

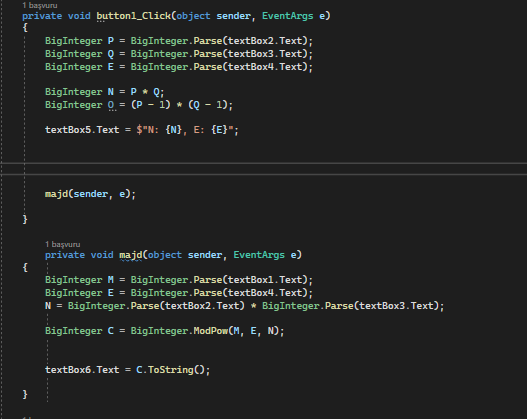
* **4. SONUÇ**



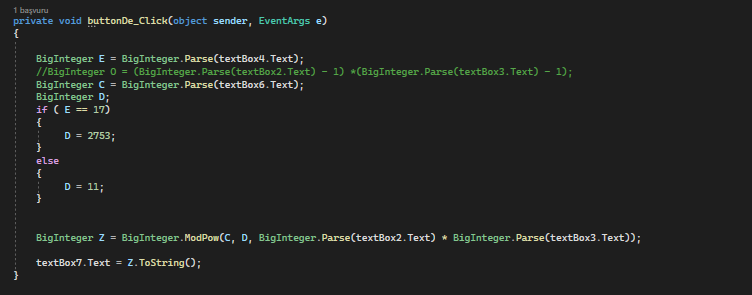
Bu resimdeki dosyaları ana dosyalar gözüküyor



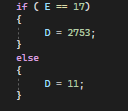
Bu resimdeki ara yüzü gösteriyor



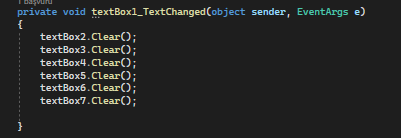
Bu resimdeki Şifreleme kodu kullanıcı arayüzünde görüntülenir



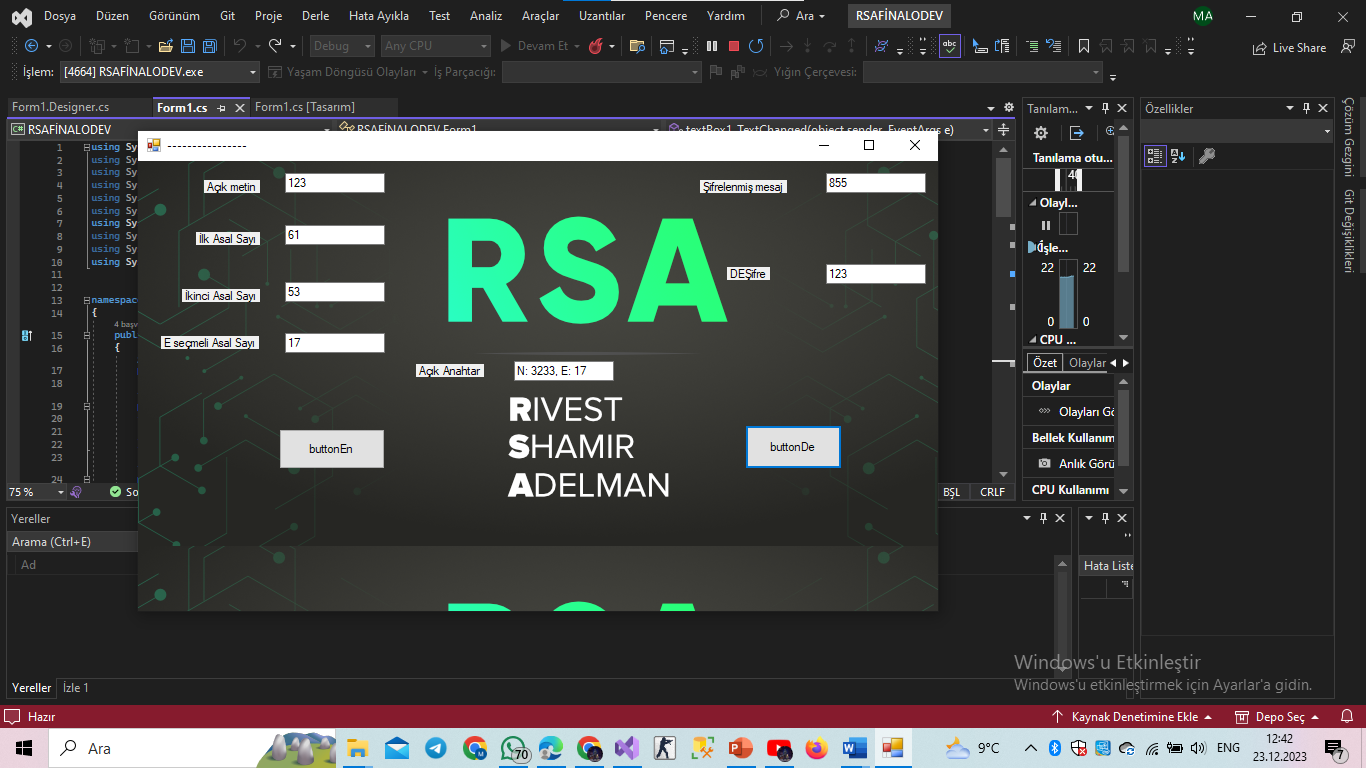
Şifre çözme kodu kullanıcı arayüzünde görüntülenir



Bu kod, belirli koşullar altında özel anahtar sağlamak amacıyla tasarlanmıştır ve yalnızca kodun sahibi bunu bilebilir ve muhatabıyla paylaşabilir.



Bu resimdeki Textbox1 içindeki herhangi bir öğe değiştirildiğinde girişleri ve çıkışları siler



Bu resimdeki Programı çalıştırdığınızda, bir kullanıcı arayüzü açılır ve şifrelenmesini istediğiniz metni açık metin kutusuna girebilirsiniz.

Daha sonra, metni şifrelemek için kullanılacak olan ilk iki asal sayıyı (P ve Q) girmeniz istenir.

Ardından, üçüncü sayıyı (E) girmeniz istenir, bu sayı genel anahtar oluşturmak için kullanılır.

Bu adımları tamamladıktan sonra, oluşturulan genel anahtar arayüzdeki ilgili kutuda görüntülenir.

Sonraki adım, şifrelemek istediğiniz sayıyı metin kutusuna girmenizdir ve ardından program, şifreli metni ilgili metin kutusunda gösterir.

"DE Şifre" butonuna tıkladığınızda, program şifrelenmiş metni çözer ve çözülmüş metni ilgili metin kutusuna yazar.

UYGULAMA:

* Anahtar Üretimi:  
  1. İki asal sayı seçin P, Q (3,7) 2. Hesaplayın n = p\*q=3\*7=21  
  3. Euler'i hesaplayın = (p-1)(q-1) = 2\*6 = 12  
  4. e, 1 <e<o seçin ve o ile eş olmalıdır (7) Anahtar (n, e) = (21, 7)  
  - Mesaj Şifreleme C = m^e mod n  
  M = 4 mesajını şifreleyin.  
  C = 4^7 mod 21 = 16384 mod 21 = 4  
  Mesaj Şifre Çözme  
  M = c^d mod n  
  D= e^-1 mod o  
  D=7^-1 mod 12 = 7  
  M = 4^7 mod 21 = 16384 mod 21 = 4
* **5. KAYNAKLAR**

**[1]** **https://www.geeksforgeeks.org/rsa-full-form/?ref=header\_search**

**[2]** https://www.rsa.com/

**[3]**  <https://tr.wikipedia.org/wiki/RSA_(%C5%9Fifreleme_y%C3%B6netimi)>

**[4]** **https://www.w3schools.com/cs/index.php**