Programın Çalıştırılması

Proje klasörünün içine girdikten sonra bin/debug klasörün de “exe” dosyası çalıştırılarak direk kullanılabilir.

Proje klasörünün içinde ki “sln” dosyası çalıştırılarak Visual Studio aracılığıyla düzenlenebilir ve çalıştırılabilir.

Fonksiyonlar

- bool isPrime(long x) : Bir sayı alır ve eğer bu sayı asalsa true, değilse false döndürür.
- long findPrime(long x = 1) : Eğer argümansız çalıştırılırsa 2 ile 100 arasında bir asal sayı döndürür eğer bir argümanla çalıştırılırsa o değer dışında bir asal sayı döndürür.
- long findQ_n(long first, long sec): 2 sayı alır ve q(n) yada t(n) hesaplar.
- long findN(long first, long sec): 2 sayı alır ve N sayısını hesaplar.
- bool Coprime(long first, long sec): 2 sayı alır ve aralarında asal olup olmadıklarını kontrol eder eğer aralarında asal iseler true, değil iseler false döndürür.
- long findEncKey(long Q_n): Q(n) değerini alır ve Encrypted Key’i (e değeri) hesaplar.
- long findD(long EncKey, long Q_n): Q(n) ve Encrypted Key değerlerini alır ve Decrypted Key’i (d değeri) hesaplar.
- long c_dmodn(long c, long d, long n) : Şifrelenecek yada şifrelenmiş metini, e yada d’yi ve N değerini alır ve geriye şifrelenmesi istenen metinin şifreli halini yada şifrelenmiş metinin çözülmüş halini döndürür.

Algoritma

RSA Algoritması RSA algoritması 1978 yılında Ron Rivest, Adi Shamir, Leonard Adleman kişileri tarafından bulunup, ismini bu kişilerin soyadlarının baş harflerinden almıştır. Güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür açık anahtarlı şifreleme yöntemidir. Simetrik şifreleme yapan algoritmalara göre güvenlik açısından daha başarılıdır ancak hız ve donanımsal uygunluk bakımından dezavantajı vardır. DH(Diffie-Helman) ve RSA algoritmaları asimetrik şifreleme algoritmaları gurubunda yer alır. Şifreleme ve elektronik imza uygulamalarında kullanılmaktadır. Bu algoritma için iki anahtara ihtiyaç vardır. Şifreli mesaj gönderebilmek için kullanılan açık anahtar ve mesajı alan tarafın şifreli metni açabilmesi için gönderilen şifreli metnin açılabilmesi için ise gizli anahtara sahip olması gerekir.