|  |
| --- |
| Kriptoloji Proje Ödevi |
| Rsa Şifreleme Algoritması |
|  |
|  |

|  |
| --- |
|  |

**Leventcan Şençamlar b141210026**

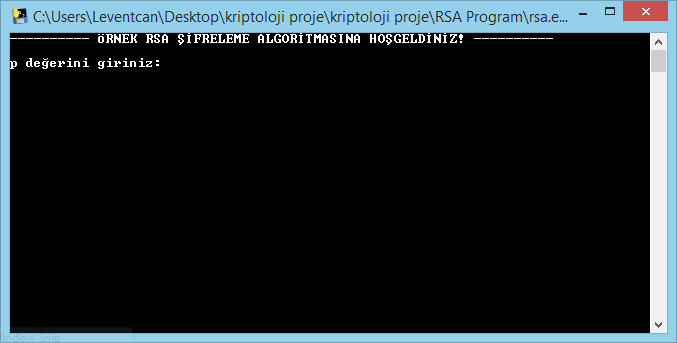
**Erbil Nas b151210053**

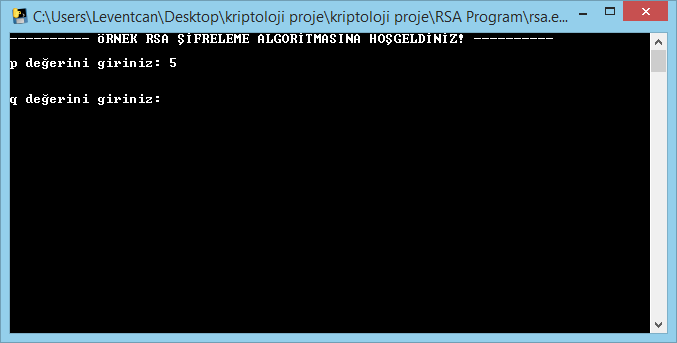
**RSA ŞİFRELEME ALGORİTMASI**

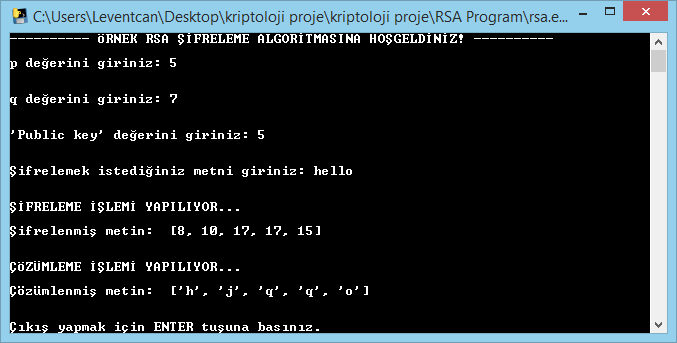
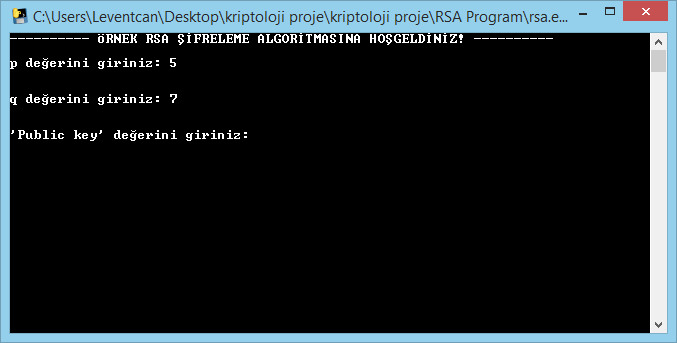
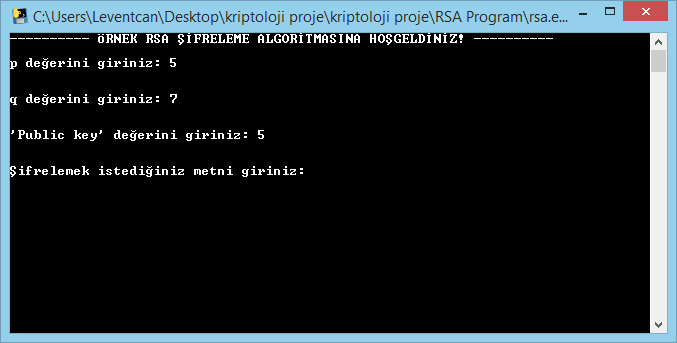
RSA, güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978’de **Ron Rivest**, **Adi Shamir** ve **Leonard Adleman** tarafından bulunmuştur. Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir, ancak şu anki yöntemlerle eğer ortak anahtar yeterince büyükse sadece asal çarpanları bilen kişi bu mesajı çözebilir. RSA şifrelemeyi kırmanın çarpanlara ayırma problemini kırmak kadar zor olup olmadığı hala kesinleşmemiş bir problemdir.

**PROGRAMIN AMACI**

Kullanıcı tarafından girilen p, q ve e (public key) değerlerine göre, gerekli işlemleri yaparak d (private key) üreten ve ürettiği bu key'ler ile kullanıcın şifrelemek istediği metnin, şifrelenmiş ve çözümlenmiş hallerini gösteren, Python dilinde yazılmış bir program

**Uygulamanın örnek çalıştırma ekran çıktıları**

****

****