



RSA ALGORİTMASI

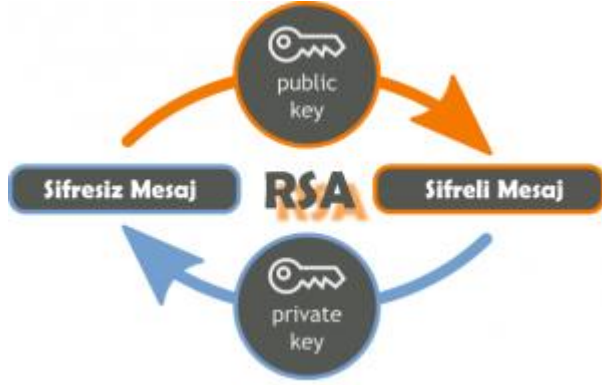
KRİPTOLOJİ PROJE ÖDEVİ



ZEYNEP TORUN – G151210307
MUHAMMET RAŞİT TOSUN - B171210372

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.

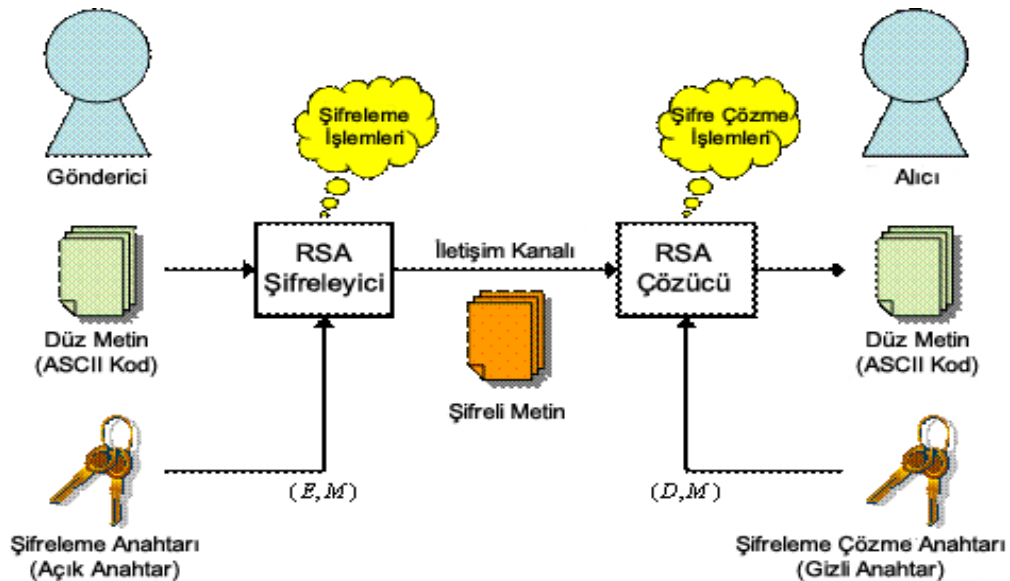
Bu algoritma için iki anahtara ihtiyaç vardır. Şifreli mesaj gönderebilmek için kullanılan açık anahtar ve mesajı alan tarafın şifreli metni açabilmesi için gönderilen şifreli metnin açılabilmesi için ise gizli anahtara sahip olması gerekir.

DEZAVANTAJLARI

- Her kullanıcı kendine ait bir şifre tutmasıyla bütün gizlenmiş metinleri tek anahtarla çözme imkânına sahiptir. Bu da anahtarın kaybolması durumunda veya başka birinin ele geçmesi durumunda büyük sıkıntılara yol açmaktadır.
- Anahtarların değiş tokuş edilmesi gerektiğinden dolayı anahtarı karşı tarafa iletmek için bir ağ kullanma zorunluluğu vardır. Bu da ağda ekstra güvenlik önlemi almayı gerektirmektedir.

Örneğin n tane kullanıcı olması durumunda n-1 adet şifre oluşturmak gerekli ve bu sistemde tutulmalıdır. Bu da ekstra bellek alanı tutacağından bu da bir dezavantaj olarak görülebilir.

ÇALIŞMA PRENSİBİ



Yeterince büyük iki adet asal sayı seçilir. (Seçili sayıların büyük olmasıyla asal olup olmadığının kontrolünü yapmak zor olacağından bu kısımda Fermat Teoremi kullanılabilir.)

Örneğin; p ve q olsun.

Bu iki asal sayının çarpımı hem açık hem de kapalı şifreler için taban olarak(mod) seçilir.

$$n = p * q$$

Yine bu iki asal sayı için Totient Fonksiyonu(T(n)) hesaplanır.

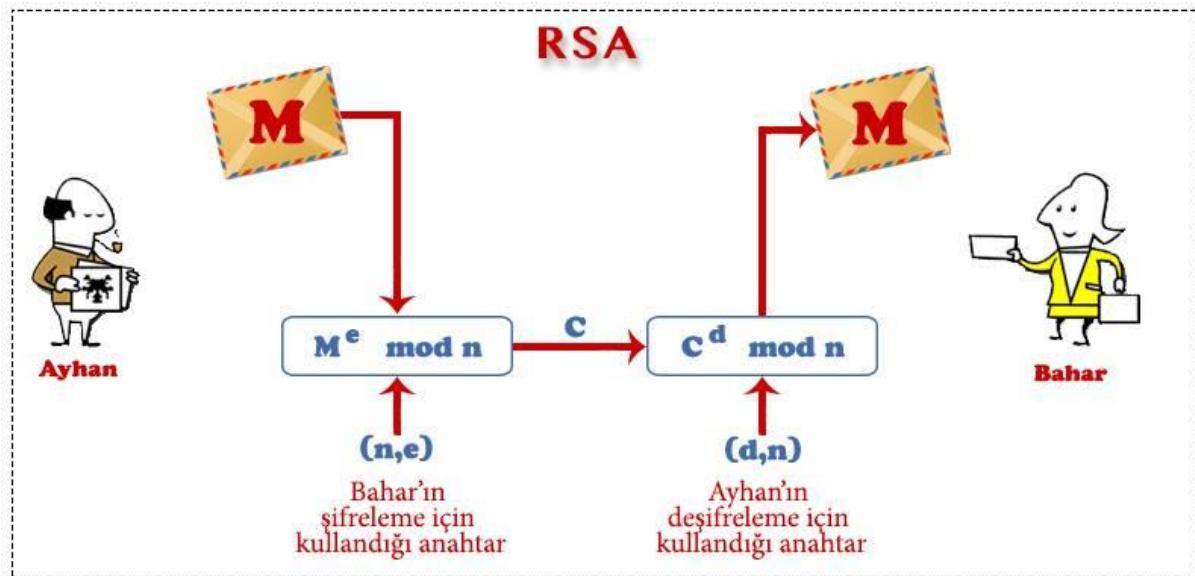
$$T(n) = (p-1)(q-1)$$

Hesaplanan T(n) değeri ile aralarında asal olan bir açık anahtar(e) belirlenir.

$$1 < e < T(n) \text{ olmalıdır.}$$

Aşağıdaki denklığe sahip kapalı anahtar(d) seçilir. Bu anahtar öyle bir sayı olmalıdır ki e sayısı ile çarpımının T(n) değerine göre mod alındığında 1 çıkmalı yani genişletilmiş öklit algoritmasından yararlanılarak T(n) mod değerine göre e anahtarının tersi d anahtarı olarak belirlenmelidir.

$$de \equiv 1 \pmod{T(n)}$$



Tüm bu işlemlerden sonra şifrelenecek metnin her bir karakterinin ASCII kod değerlerine göre

$$c = m^e \bmod(n)$$

Şifrelenmiş metnin çözülmesi için, yine her bir karakterin ASCII değerine göre;

$$m = c^d \bmod(n)$$

PROGRAM ÖRNEK EKRAN ÇIKTILARI

İlk grupta iki asal sayı girilmesi istenmektedir. Eğer kullanıcı sayı girmek istemezse butona basıp sayı üretmesi beklenmektedir. Bu iki durumun ortak sonucunda T(n) değeri hesaplanmış olacaktır. Hemen

altındaki ikinci bölümde ise açık anahtar olan e değerinin girilmesi veya Generate butonu ile rastgele üretilmesi beklenmektedir. En son şifrelenecek metin girilip Encrypted butonuna basıldığında, şifreleme ve gizli anahtar(d) ile doğrulama amaçlı şifreli metni çözme işlemleri yapılacaktır.

The screenshot shows the 'RSA Algorithm' application window. It has two main sections for input. The first section, 'Enter Numbers or Random Generate', contains 'Prime Numbers' (97 and 47), 'T(n)' (4416), and a 'Random Generate' button. The second section, 'Enter Key Number or Random Generate', contains 'Public Key (e)' (1097), a 'Generate' button, and 'Private Key (d)' (4271). Below these is a 'Text to be encrypted' field containing 'Türkiye Sakarya'. A large 'Encryption' button is on the left. To the right, the 'Encrypted' field shows a string of characters, and the 'Decrypted' field shows 'Türkiye Sakarya'.

Eğer asal sayı girilmesi gereken yerler veya şifrelenecek metin girilmezse aşağıdaki uyarıları verir.

The screenshot shows the 'RSA Algorithm' application window with an error message dialog box overlaid. The dialog box has a title bar with a close button (X) and contains the text 'Please enter Prime numbers or Generate'. There is a 'Tamam' (OK) button at the bottom of the dialog. The background application window shows the same input fields as the previous screenshot, but they are partially obscured by the dialog box.

The RSA Algorithm window displays the following fields and controls:

- Enter Numbers or Random Generate:**
 - Prime Numbers: 11, 47
 - T(n): 460
 - Random Generate button
- Enter Key Number or Random Generate:**
 - Public Key (e): 53
 - Generate button
- Private Key (d):** (Empty field)
- Text to be encrypted:** (Empty text box)
- Encryption** button
- Encrypted:** (Empty text box)
- Decrypted:** (Empty text box)

A modal dialog box is open with the text "Please enter the Text" and a "Tamam" button.

Diğer hatalar;

Eğer asal sayılar yokken e anahtarı üretilmek için Generate butonuna basılırsa, T(n) değeri ile aralarında asal kontrolü yapamayacağı için önce T(n) değerinin hesaplanmış olması beklenir. Bu değer olmadığı için hata verilmesi gerekir.

The RSA Algorithm window displays the following fields and controls:

- Enter Numbers or Random Generate:**
 - Prime Numbers: (Empty fields)
 - T(n): (Empty field)
 - Random Generate button
- Enter Key Number or Random Generate:**
 - Public Key (e): (Empty field)
 - Generate button
- Private Key (d):** (Empty field)
- Text to be encrypted:** (Empty text box)
- Encryption** button

A modal dialog box is open with the text "Please enter the Prime numbers or Generate One." and a "Tamam" button.

Açık anahtar(e) olmadan şifrele butonuna basılırsa yine hata verilir.

The image shows a window titled "RSA Algorithm" with the following fields and buttons:

- Enter Numbers or Random Generate**
 - Prime Numbers: 2017, 1453
 - T(n): 2927232
 - Random Generate button
- Enter Key Number or Random Generate**
 - Public Key (e):
 - Private Key (d):
 - Generate button
- Text to be encrypted:
- Encryption button
- Encrypted:
- Decrypted:

An error dialog box is displayed in the center with the text: "Please enter Enc. Key or Generate One" and a "Tamam" button.

Eğer T(n) değeri ve açık anahtar varken, aralarında asal olup olmadığının kontrolü de yapılır. Değilse hata verilir.

The image shows the same "RSA Algorithm" window with the following fields and buttons:

- Enter Numbers or Random Generate**
 - Prime Numbers: 13, 71
 - T(n): 840
 - Random Generate button
- Enter Key Number or Random Generate**
 - Public Key (e): 5
 - Generate button
- Private Key (d):
- Text to be encrypted:
- Encryption button

An error dialog box is displayed in the center with the text: "The E Number must be coprime with the T(n) number." and a "Tamam" button.