ASAL SAYILAR VE ŞİFRELEME

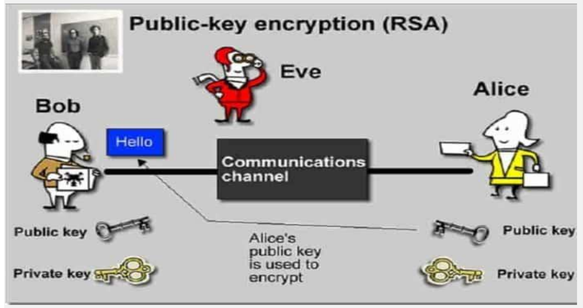
DANIŞMAN: Doç. Dr. Canan AKIN

Samet NALBANT

GİRİŞ

Tanım
Bir doğal sayı $p > 1$, yalnızca 1 ve kendisine tam bölünebiliyorsa asal sayı olarak adlandırılır.

Asal sayılar, hem matematiksel yapıları hem de teknolojik uygulamalardaki işlevleri nedeniyle modern bilim dünyasında merkezi bir konuma sahiptir. Asal sayılar, aritmetiğin temel taşlarından biridir. Günümüzde asal sayıların en kritik kullanım alanlarından biri şifreleme bilimidir. Veri güvenliği, gizlilik ve kimlik doğrulama gibi temel bilişim süreçleri, büyük asal sayılar üzerine kurulu matematiksel algoritmaların sağladığı dayanıklılık sayesinde işletilmektedir. Özellikle RSA gibi asimetrik şifreleme yöntemleri, asal sayıların bölünemezlik özelliklerinden yararlanarak güçlü ve pratik güvenlik mekanizmaları oluşturur. Şifreleme, bilginin yetkisiz erişime kapalı hâle getirilmesi amacıyla yapılan matematiksel dönüşüm işlemlerini kapsar. Bu dönüşümler çoğunlukla modüler aritmetik gibi sayılar teorisine dayalı yapılara başvurur. Şifreleme, genel olarak iki ana kategoriye ayrılır: simetrik ve asimetrik şifreleme. Simetrik şifrelemede aynı anahtar hem şifreleme hem de çözme işlemi için kullanılırken, asimetrik şifrelemede biri açık (public key), diğeri gizli (private key) olmak üzere iki farklı anahtar bulunur. Asimetrik sistemlerin güvenliği, büyük asal sayıların çarpanlara ayrılmasının hesaplama açısından son derece zor olmasına dayanır.



ARİTMETİĞİN TEMEL TEOREMİ

Her pozitif tam sayı $n > 1$, tekil (benzersiz) biçimde asal çarpanlarına ayrılır:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Burada p_i asal sayılardır ve α_i pozitif tam sayılardır.

FERMAT TEOREMİ

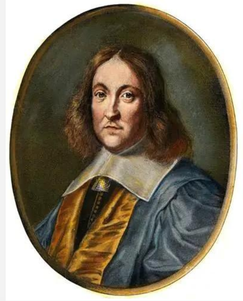
Eğer p asal ve a tam sayı olup gcd(a, p) = 1 ise, o zaman

$a^{p-1} \equiv 1 \pmod{p}$

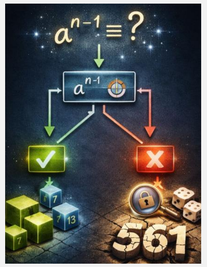
FERMAT ASALLIK TESTİ

Verilen bir $n > 2$ tamsayısı için:

1. $1 < a < n-1$ **olacak şekilde rastgele bir** a **seç.**
2. $\gcd(a, n)$ **hesapla.**
$\gcd(a, n) > 1 \Rightarrow n$ bileiktir.
3. **Eğer** $\gcd(a, n) = 1$ **ise,** $a^{n-1} \bmod n$**'i hesapla.**
$a^{n-1} \bmod n = 1$ ise n olası asaldır,
$a^{n-1} \bmod n \neq 1$ ise n kesin bileşiktir.



ÖRNEK



$n = 15$ **olsun.**
$\gcd(2, 15) = 1$.

Hesaplayalım:
$2^{14} = 16384$
$16384 \bmod 15 = 4 \neq 1$

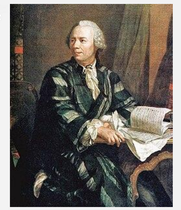
Yani:
$2^{15-1} \not\equiv 1 \pmod{15} \Rightarrow 15$ bileşiktir.

Test bileşiği doğru tespit etti.

İSTİSNALAR:CARMICHAEL SAYILARI

Bazı özel bileşik sayılar n için:
$a^{n-1} \equiv 1 \pmod{n} \quad \forall a$ ile $\gcd(a, n) = 1$
koşulu geçerlidir.
Bu sayılara Carmichael sayıları denir.
Örneğin:
$561 = 3 \times 11 \times 17$
ve:
$a^{560} \equiv 1 \pmod{561}$
her a için geçerlidir.
Dolayısıyla Fermat testi, bu tür sayılarda yanılabilir.

EULER TOTİENT FONKSİYONU



Euler'in totient fonksiyonu, φ(n) ile gösterilir ve 1 ile n arasındaki, n ile aralarında asal (ortak böleni 1 olan) pozitif tam sayıların sayısını verir.

Yani:

$\phi(n) = |\{k \in \mathbb{N} \mid 1 \le k \le n, \gcd(k, n) = 1\}|$

Örnek:
n = 9 için:
1'den 9'a kadar sayılar: 1, 2, 3, 4, 5, 6, 7, 8, 9
9 ile aralarında asal olanlar: 1, 2, 4, 5, 7, 8
→ 6 tane sayı vardır.

Dolayısıyla: φ(9) = 6

Eğer a ve b aralarında asal ise:

$\phi(ab) = \phi(a) \cdot \phi(b)$

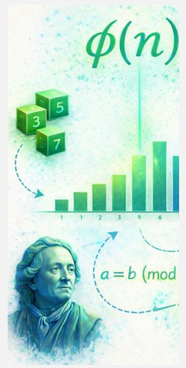
Bu özellik çok önemlidir — çünkü RSA'da n = p · q iki asalin çarpımıdır.
Bu durumda:

$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

TOTİENT FONKSİYONUNUN ÖZELLİKLERİ

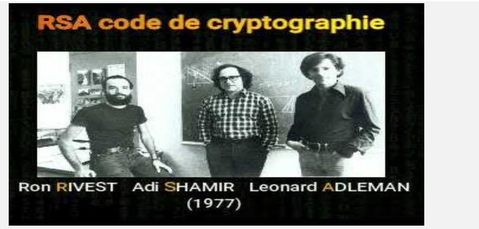
1. **Bir sayı $n > 2$ verilsin.**
2. **$1 < a < n-1$ olacak şekilde rastgele bir a seç.**
3. **$a^{n-1} \bmod n$ değerini hesapla.**
4. **Eğer sonuç 1'den farklıysa → n bileşiktir. Eğer sonuç 1 ise → n "muhtemelen asal" dır.**

Eğer n asal bir sayıysa, p'ye kadar olan bütün sayılar p ile aralarında asaldır (sadece kendisi hariç).
$\Rightarrow \varphi(p) = p - 1$
Örnek:
$p = 7$ **için**
$\varphi(7) = 7 - 1 = 6$
(1, 2, 3, 4, 5, 6 — hepsi 7 ile aralarında asaldır)



RSA ALGORİTMASI

RSA Algoritması ve Asal Sayıların Rolü En yaygın kullanılan açık anahtar şifreleme yöntemi RSA algoritmasıdır. 1977 yılında Rivest, Shamir ve Adleman tarafından geliştirilmiştir. RSA algoritması şu şekilde çalışır: 1. İki büyük asal sayı seçilir: ppp ve qqq. 2. Bu iki sayı çarpılır: 3. Euler Totient fonksiyonu hesaplanır: Şifreleme: Şifre çözme: RSA'nın güvenliği, büyük sayıların asal çarpanlarına ayrılmasının zorluğuna dayanır. Örneğin, 300 basamaklı bir sayının asal çarpanlarını bulmak, günümüz bilgisayarları için bile oldukça zordur.



RSA (Rivest–Shamir–Adleman), 1977'de geliştirilmiştir.
Güvenliği, büyük bir sayının asal çarpanlarına ayrılmasının zorluğuna dayanır.

Adımlar:

1. **İki büyük asal sayı seçilir:**
   p, q asal
2. **Modül hesaplanır:**
   n = p × q
3. **Euler'in totient fonksiyonu:**
   φ(n) = (p − 1)(q − 1)
4. **Bir şifreleme anahtarı e seçilir:**
   1 < e < φ(n) ve gcd(e, φ(n)) = 1
5. **Açma anahtarı d hesaplanır:**
   1 < d < φ(n) ve e·d ≡ 1 (mod φ(n))

Anahtar çiftleri:
Açık anahtar: (e, n)
Gizli anahtar: (d, n)

6. **Şifreleme:**
   $c = m^e \pmod{n}$
7. **Şifre çözme:**
   $m = c^d \pmod{n}$

RSA algoritmasında:
$n = p \cdot q$
$\varphi(n) = (p-1)(q-1)$

Şifre çözme işleminin doğru çalışmasının nedeni, Euler'in teoremidir.

Çünkü e ve d öyle seçilir ki:
$e \cdot d \equiv 1 \pmod{\varphi(n)}$

Dolayısıyla:
$m^{ed} = m^{1+k\varphi(n)} \equiv m \pmod{n}$

Durum	Formül	Örnek
p asal	$\varphi(p) = p - 1$	$\varphi(7) = 6$
p^k	$\varphi(p^k) = p^k - p^{k-1}$	$\varphi(8) = 4$
$n = p \cdot q$, p, q asallar	$\varphi(n) = (p-1)(q-1)$	$\varphi(15) = 8$

KAYNAKÇA

https://evrimagaci.org/
https://tr.wikipedia.org/
https://erkanliman.com/genel/rsa-sifreleme-algoritmasi.html
https://di-mgt.com.au/rsa_alg.html#note6
https://www.matematikciler.com/
https://bilimgenc.tubitak.gov.tr/
Chatgpt
https://planetcalc.com/8983/?utm_source