**Kriptografinin Tarihçesi, Türleri ve Siber Güvenlikteki Yeri**

**1. Kriptografinin Tarihçesi**

Kriptografi, bilgilerin gizliliğini ve bütünlüğünü korumak amacıyla şifreleme tekniklerinin kullanıldığı bir bilim dalıdır. Kriptografinin tarihi, eski uygarlıklara kadar uzanır. İşte bu tarihin bazı önemli aşamaları:

* **Antik Dönemler (MÖ 1900 - MÖ 400):** İlk kriptografik teknikler, Mezopotamya’da yazılı metinlerde gizli mesajlar oluşturmak amacıyla kullanılmıştır. Antik Mısır'da, hiyerogliflerin kullanımı da gizlilik için bir yöntem olarak görülmüştür.
* **Roma İmparatorluğu (MÖ 1. Yüzyıl):** Roma İmparatoru Jül Sezar, **Sezar Şifresi** olarak bilinen teknikle bilinir. Bu şifreleme yöntemi, harflerin yerine alfabetik olarak belirli bir sayı kadar kaydırma yapılmasını içeriyordu. Bu, basit bir simetrik şifreleme tekniğiydi.
* **Orta Çağ ve Arap Bilim İnsanları:** Orta Çağ’da Arap bilim insanları, şifre çözme ve şifreleme üzerine önemli çalışmalar yapmışlardır. Bu dönemde, kriptografi daha çok askeri ve diplomatik amaçlarla kullanıldı.
* **17. - 19. Yüzyıl:** Modern kriptografinin temelleri atıldı. Özellikle Fransız matematikçi Blaise de Vigenère’in **Vigenère Şifresi**, o dönemin en karmaşık şifreleme yöntemlerinden biriydi.
* **20. Yüzyıl (İkinci Dünya Savaşı):** En bilinen kriptografik gelişme, Almanların **Enigma makinesi**ni kullanmasıdır. Enigma, çok karmaşık bir şifreleme cihazıydı ve İngiliz matematikçi Alan Turing, Enigma şifrelerini kırarak savaşın seyrini değiştiren büyük bir başarıya imza atmıştır.
* **Bilgisayar Çağı (1970’ler ve Sonrası):** Bilgisayarların gelişmesiyle birlikte kriptografi, dijital çağda çok daha büyük bir rol oynamaya başladı. **RSA algoritması**, **AES (Advanced Encryption Standard)** ve **SHA (Secure Hash Algorithm)** gibi modern kriptografik algoritmalar geliştirilmiştir.

**1. Antik Dönemler (MÖ 1900 - MÖ 400)**

**Mezopotamya ve Antik Mısır:**

* **Mezopotamya:** İlk kriptografik tekniklerin kullanımı, özellikle gizli mesajlar oluşturmak amacıyla Mezopotamya'da yazılı metinlerde görülmüştür. Bu dönemde, yazılı metinler ve semboller üzerinden gizli anlamlar yaratmak için bazı basit kodlama yöntemleri uygulanmıştır. Ancak bu teknikler daha çok sembolik ve dini anlam taşıyan mesajlar içermekteydi.
* **Antik Mısır:** Antik Mısır'da, **hiyeroglif** yazısı ve semboller kullanılarak gizli anlamlar taşınan mesajlar yazılmıştır. Hiyeroglifler, aynı zamanda bir tür "şifreleme" olarak da kabul edilebilir çünkü bu semboller her zaman belirli bir anlam taşımaz, bazen şifreli bir mesajı ifade etmek için kullanılmıştır. Ancak bu, günümüz kriptografisiyle karşılaştırıldığında çok daha basit bir şifreleme yöntemidir.

**2. Roma İmparatorluğu (MÖ 1. Yüzyıl)**

**Sezar Şifresi:**

* Roma İmparatoru **Jül Sezar**, en ünlü ve erken döneme ait şifreleme tekniğini geliştirmiştir: **Sezar Şifresi**. Bu yöntem, harflerin yerine alfabetik olarak belirli bir sayı kadar kaydırma yapılmasını içerir. Örneğin, bir harf üç basamak kaydırılıyorsa, **A** harfi **D**'ye dönüşür, **B** harfi ise **E**'ye dönüşür.
* **Örnek:** "HELLO" kelimesi Sezar şifresiyle 3 harf kaydırılarak "KHOOR" olur.

**3. Orta Çağ ve Arap Bilim İnsanları**

* **Arap Kriptografisi ve El-Kindi:** Orta Çağ'da Arap bilim insanları, özellikle **El-Kindi** (9. yüzyıl) ve **Alfarabi**, kriptografi üzerinde önemli çalışmalar yapmışlardır. **El-Kindi**, şifre çözme üzerine yazdığı kitapta **frekans analizi** yöntemini kullanarak, şifreli metinleri çözme yöntemini açıklamıştır. Bu, günümüzün kriptanaliz tekniklerinin temellerini atmıştır.
* **Şifreleme Uygulamaları:** Orta Çağ'da kriptografi genellikle askeri ve diplomatik amaçlar için kullanılmıştır. Arap dünyasında bu dönemdeki şifreleme, esasen **alfabetik şifreleme** ve **sembol kullanımı** gibi basit tekniklerden ibaretti. Ancak bu dönemde, bilginin güvenliğini sağlamak için daha sofistike yöntemler geliştirilmiştir.

**4. 17. - 19. Yüzyıl**

**Vigenère Şifresi:**

* **Blaise de Vigenère** (16. yüzyıl sonunda), çok daha karmaşık bir şifreleme yöntemi olan **Vigenère Şifresi**'ni geliştirdi. Bu şifreleme, her harfi başka bir harf ile şifrelemek için bir anahtar kelime kullanır. Her harf, bir anahtar harfiyle kaydırılır ve kaydırmalar her harf için farklıdır, bu da şifreyi çok daha zor hale getirir.
* **Örnek:** Anahtar kelime "KEY" ve şifreleme yapmak için "HELLO" kelimesini kullanırsak, her harf farklı kaydırmalarla şifrelenir:
  + **H** + **K** (10) = **R**
  + **E** + **E** (4) = **I**
  + **L** + **Y** (24) = **J**
  + **L** + **K** (10) = **V**
  + **O** + **E** (4) = **S**

Sonuçta, "HELLO" kelimesi "RIJVS" olarak şifrelenmiş olur.

**Vigenère Şifresindeki Mod 26 Kullanımı**

Vigenère şifresinde, **mod 26** kullanarak harfleri kaydırıyoruz çünkü İngiliz alfabesinde **26 harf** vardır. Yani, harflerin sayısal değerini bulduktan sonra, kaydırmalar sonucu elde edilen değeri **26 ile böleriz** ve kalan değeri alırız. Bu, şifremizin tekrar başa dönmemesini sağlar.

Mesela, eğer **Z** harfini kaydırmak istiyorsak (yani, Z'yi 1 harf ileri kaydırmak gibi), alfabedeki son harfe (Z'ye) geldik ve tekrar başa dönmek istiyoruz. Bu durumda, **Z + 1** işlemi **mod 26** ile yapılır.

**Adım Adım Örnek**

Örnek olarak, **"HELLO"** metnini **"KEY"** anahtar kelimesiyle şifrelemek istiyoruz.

Şifreleme için kullandığımız işlem şu:

**(Harf değeri + Anahtar harfi değeri) mod 26**

**1. H + K:**

* "H" harfi, **alfabedeki 8. harf** olduğundan değeri **7** (A=0, B=1, C=2, ..., H=7).
* "K" harfi, **alfabedeki 11. harf** olduğundan değeri **10**.

Şimdi şifrelememiz şöyle olacak:

**(7 + 10) mod 26**  
**17 mod 26 = 17 (Kural)**

Yani **17** numaralı harf **R**'dir (alfabedeki 18. harf).

**2. E + E:**

* "E" harfi, **alfabedeki 5. harf** olduğundan değeri **4**.
* "E" harfi, yine **4**.

Şifreleme işlemi şu olacak:

**(4 + 4) mod 26**  
**8 mod 26 = 8**

Yani **8** numaralı harf **I**'dir (alfabedeki 9. harf).

**3. L + Y:**

* "L" harfi, **alfabedeki 12. harf** olduğundan değeri **11**.
* "Y" harfi, **alfabedeki 25. harf** olduğundan değeri **24**.

Şifreleme işlemi şöyle olacak:

**(11 + 24) mod 26**  
**35 mod 26 = 9**

Yani **9** numaralı harf **J**'dir (alfabedeki 10. harf).

**4. L + K:**

* "L" harfi, **alfabedeki 12. harf** olduğundan değeri **11**.
* "K" harfi, **alfabedeki 11. harf** olduğundan değeri **10**.

Şifreleme işlemi şöyle olacak:

**(11 + 10) mod 26**  
**21 mod 26 = 21**

Yani **21** numaralı harf **V**'dir (alfabedeki 22. harf).

**5. O + E:**

* "O" harfi, **alfabedeki 15. harf** olduğundan değeri **14**.
* "E" harfi, **alfabedeki 5. harf** olduğundan değeri **4**.

Şifreleme işlemi şu şekilde yapılacak:

**(14 + 4) mod 26**  
**18 mod 26 = 18**

Yani **18** numaralı harf **S**'dir (alfabedeki 19. harf).

**Sonuç:**

Bütün bu işlemleri gerçekleştirdiğimizde, **"HELLO"** kelimesi **"RIJVS"** olarak şifrelenmiş olur.

**5. 20. Yüzyıl (İkinci Dünya Savaşı)**

**Enigma Makinesi:**

* **Enigma Makinesi**, II. Dünya Savaşı sırasında **Almanya** tarafından kullanılan bir şifreleme cihazıdır. Enigma, 26 harflik bir alfabe kullanarak her harf için farklı bir şifreleme üretmek için dönen makineler ve rotorlar kullanıyordu. Bu makinelerin şifreleri son derece karmaşıktı ve çözülmesi çok zor oluyordu.
* **Alan Turing**, İngiliz matematikçi, Enigma şifrelerini çözmeyi başarmış ve bu başarısı savaşın seyrini değiştiren bir dönüm noktası olmuştur. Bu şifrelerin kırılması, müttefiklerin savaşın ilerleyişini tahmin etmelerini sağlamış ve Almanya'nın kodlarının kırılması, savaşın sonucunu etkileyen önemli bir faktör olmuştur.

**6. Bilgisayar Çağı (1970’ler ve Sonrası)**

**RSA ve Modern Kriptografi:**

* **RSA Algoritması**, 1977 yılında **Ron Rivest**, **Adi Shamir** ve **Leonard Adleman** tarafından geliştirilen bir asimetrik şifreleme algoritmasıdır. Bu algoritma, iki büyük asal sayının çarpımıyla oluşturulan bir anahtar kullanarak şifreleme işlemi yapar. RSA, günümüzde internet üzerindeki güvenli iletişim için temel bir teknoloji olarak kullanılmaktadır.

RSA algoritması, **asimetrik şifreleme** yöntemlerinden biridir. Hem şifreleme hem de dijital imza için kullanılabilir. Bu algoritma, **iki anahtar** kullanır: **Genel Anahtar (public key)** ve **Özel Anahtar (private key)**. Bu iki anahtar birbirine matematiksel olarak bağlıdır, ancak bir anahtarın bilinmesi, diğerinin bulunmasına imkan vermez.

**RSA Algoritmasının Temel Adımları**

RSA algoritmasıyla şifreleme yaparken şu adımları izleriz:

1. **İki büyük asal sayı seçilir.**
2. **Bu sayılar kullanılarak açık anahtar ve gizli anahtar (private key) hesaplanır.**
3. **Mesaj şifrelenir** ve **açık anahtar** ile çözülür.

Şimdi adım adım bir örnek çözerek RSA algoritmasını daha iyi anlayalım.

**RSA Algoritması Örneği**

Diyelim ki **p = 61** ve **q = 53** olsun. Bu iki asal sayıyı seçelim ve RSA algoritmasını uygulayalım.

**Adım 1: Modül N ve Phi (Φ(n)) Hesaplama**

Öncelikle modül **n** hesaplanır:

n=p×q

Burada:

* **p = 61** ve **q = 53**

n=61×53=3233

**n**, **açık anahtarın** bir parçası olacak.

Sonra, **Phi(n)** (Euler's Totient Function) hesaplanır:

**Φ(n)=(p−1) ×(q−1)**

Burada:

* p−1=61−1=60
* q−1=53−1=52

Φ(n)=60×52=3120

**Adım 2: Açık Anahtar (e) Seçimi**

Şimdi **açık anahtar** (**e**) seçmemiz gerekiyor. **e**, **1 < e < Φ(n)** olmalı ve **e** ile **Φ(n)**'nin **en büyük ortak böleni (gcd)** 1 olmalıdır (yani, **e** ve **Φ(n)** birbirine asal olmalı).

Rastgele bir **e** seçelim ve bunun **Φ(n)** ile asal olup olmadığını kontrol edelim. Diyelim ki **e = 17**.

Şimdi, **gcd(17, 3120)**'yi kontrol edelim. Eğer **gcd(17, 3120) = 1** ise, bu **e** geçerli bir seçimdir.

Hesaplama yapalım:

* **gcd(17, 3120) = 1**

Çünkü 17 ve 3120'nin ortak böleni 1'dir. O zaman **e = 17** doğru bir seçimdir.

**Adım 3: Özel Anahtar (d) Hesaplama**

**d**'yi, aşağıdaki eşitliği sağlayan sayıyı bularak hesaplarız:

d×e≡1(modΦ(n))

Yani, **d** sayısı, **d \*17 ≡ 1 (mod 3120)** olmalı.

Bunu çözmek için, **e = 17** ve **Φ(n) = 3120**'yi kullanarak **d**'yi bulmalıyız. **d**, **e**'nin modüler tersi olarak hesaplanır.

Burada, **e = 17** için **d** hesaplamak amacıyla, **modüler tersini** bulmalıyız:

17×d≡1(mod3120)17

Bir modüler ters hesaplama yöntemi kullanarak, **d = 2753** bulunur.

**Adım 4: Açık Anahtar (Public Key) ve Özel Anahtar (Private Key)**

Şimdi, **açık anahtar** (public key) ve **özel anahtar** (private key) belirlenmiştir:

* **Açık Anahtar (Public Key)**: (e=17, n=3233)
* **Özel Anahtar (Private Key)**: (d=2753, n=3233)

**Adım 5: Mesajın Şifrelenmesi**

Diyelim ki şifrelemek istediğimiz mesaj **M = 65**.

Mesajı şifrelemek için **açık anahtar** kullanırız. Şifreleme işlemi şu formülle yapılır:

C=M^e(mod n)

Burada:

* **M = 65**
* **e = 17**
* **n = 3233**

Hesaplama:

C=6517(mod 3233)

Bu hesaplama sonucunda:

C=2790C =2790

**Adım 6: Mesajın Çözülmesi**

Şimdi, şifreli mesajı çözmek için **özel anahtar** kullanılır. Şifreli mesajı çözmek için şu formülü kullanırız:

**M=C^d (mod n)**

Burada:

* **C = 2790**
* **d = 2753**
* **n = 3233**

Hesaplama:

M=2790 ^2753 (mod 3233)

Bu hesaplama sonucunda:

M=65

Yani şifrelendiğimiz mesajın orijinal hali olan **M = 65**'i geri alıyoruz!

* **AES (Advanced Encryption Standard):** AES, simetrik şifreleme için kullanılan en popüler algoritmalardan biridir ve günümüzde verilerin güvenliğini sağlamak için yaygın olarak kullanılır. Bu algoritma, 128, 192 ve 256-bit uzunluğunda anahtarlar kullanarak yüksek güvenlik sağlar.
* **SHA (Secure Hash Algorithm):** SHA, verilerin bütünlüğünü sağlamak için kullanılan bir hash fonksiyonudur. Verilerin doğru şekilde iletilip iletilmediğini kontrol etmek için sıkça kullanılır. Özellikle dijital imzalar ve şifreleme protokollerinde yer alır.

**2. Kriptografi Türleri**

Kriptografi, farklı şifreleme ve güvenlik ihtiyaçlarına göre çeşitli teknikler sunar. Başlıca kriptografi türleri:

**2.1. Simetrik Kriptografi**

* **Tanım:** Aynı anahtar hem şifreleme hem de şifre çözme işlemlerinde kullanılır.
* **Örnekler:** **AES (Advanced Encryption Standard)**, **DES (Data Encryption Standard)**
* **Avantajları:** Hızlı ve verimlidir.
* **Dezavantajları:** Anahtar güvenliği kritik, çünkü anahtarın güvenli bir şekilde iletilmesi zor olabilir.

**2.2. Asimetrik Kriptografi**

* **Tanım:** İki anahtar kullanılır: bir açık anahtar (public key) ve bir özel anahtar (private key). Açık anahtar mesajları şifrelerken, özel anahtar yalnızca şifreyi çözer.
* **Örnekler:** **RSA**, **ECC (Elliptic Curve Cryptography)**
* **Avantajları:** Anahtar paylaşımı güvenlidir, çünkü sadece alıcı özel anahtarına sahiptir.
* **Dezavantajları:** Genellikle simetrik kriptografiye göre daha yavaştır.

**2.3. Hash Fonksiyonları**

* **Tanım:** Verinin sabit uzunlukta bir özetini oluşturur. Verinin bütünlüğünü kontrol etmek için kullanılır.
* **Örnekler:** **SHA-256**, **MD5**
* **Avantajları:** Hızlıdır ve verinin bütünlüğünü hızlıca kontrol etmek için kullanılır.
* **Dezavantajları:** Şifreleme sağlamaz, yalnızca verinin doğruluğunu doğrular.

**2.4. Dijital İmzalar**

* **Tanım:** Asimetrik kriptografi kullanılarak verinin kaynağı ve bütünlüğü doğrulanır.
* **Örnekler:** **RSA Dijital İmza**, **DSA (Digital Signature Algorithm)**
* **Avantajları:** Veri doğruluğunu sağlar ve göndericinin kimliğini doğrular.
* **Dezavantajları:** Dijital imzaların doğrulanması zaman alabilir.

**3. Kriptografinin Siber Güvenlikteki Yeri**

Kriptografi, günümüzde siber güvenliğin temel yapı taşlarından biridir. Hem bireysel kullanıcılar hem de kurumlar, verilerini korumak için kriptografiyi aktif olarak kullanmaktadır. Kriptografinin siber güvenlikteki başlıca rolleri şunlardır:

**3.1. Veri Şifreleme**

* **Açıklama:** Kişisel, finansal ve diğer hassas bilgilerin korunması için verilerin şifrelenmesi gerekmektedir. Bu şifreleme, veri iletimi sırasında bilgilerin çalınmasını engeller.
* **Örnek:** HTTPS protokolü, internet üzerinde güvenli iletişim sağlamak için **SSL/TLS** şifreleme kullanır.

**3.2. Kimlik Doğrulama**

* **Açıklama:** Kullanıcıların kimliklerinin doğrulanması için dijital imzalar ve şifreleme teknikleri kullanılır. Bu, çevrimiçi bankacılık ve diğer hassas işlemler için büyük önem taşır.
* **Örnek:** **İki faktörlü kimlik doğrulama (2FA)**, şifreleme kullanılarak güvenli bir kullanıcı doğrulama yöntemidir.

**3.3. Veri Bütünlüğü**

* **Açıklama:** Hash fonksiyonları kullanılarak, veri iletimi sırasında verilerin değiştirilmediğinden veya bozulmadığından emin olunur. Bu, özellikle dosya transferlerinde kritik öneme sahiptir.
* **Örnek:** **SHA-256**, veri bütünlüğünü kontrol etmek için yaygın olarak kullanılır.

**3.4. VPN ve SSL/TLS Protokolleri**

* **Açıklama:** **VPN (Virtual Private Network)** ve **SSL/TLS** protokolleri, internet üzerinden güvenli iletişim sağlar. Kriptografi, bu protokollerin temelini oluşturur ve verilerin şifreli bir şekilde iletilmesini sağlar.

**3.5. Blokzincir ve Kripto Paralar**

* **Açıklama:** Blokzincir, dijital para birimlerinin güvenliğini sağlamak için kriptografik teknikler kullanır. Özellikle **Bitcoin** ve diğer kripto paralar, işlemlerini güvenli bir şekilde gerçekleştirmek için kriptografi kullanır.