KRİPTOGRAFİ

Bilgiyi Değil, Anlamını Saklama Sanatı

ZERO TRUST

Bünyamin Erol TÜRKKAN
Huzeyfe KUL
İrem Hatun TEK
Nail Erkılıçoğlu

MERHABA

Bugün, bilgiyi korumanın en eski ama hâlâ en güçlü yolunu, yani kriptografiyi konuşacağız.

Kriptografi, bilgiyi yetkisiz kişilerin anlayamayacağı bir forma dönüştürme sanatıdır; amacı bilginin anlamını gizlemektir.

Kriptografi

kryptos (gizli)

+

graphein (yazmak)

Kriptografi, bilginin anlamını gizleyerek onu yetkisiz kişilerden koruma sanatıdır.

Yunanca kelimelerinden gelir.

GİZLEMEK

Gizlilik aslında insanlık tarihi kadar eski bir kavram.

Tarihte insanlar mesajlarını korumak için gerçekten ilginç yöntemler kullanmışlar.

Sizce gizliliğe neden ihtiyaç duyarız?

Bir arkadaşınıza bir sır iletmek isteseniz bunu nasıl yaparsınız?

Steganografi: Mesajın Varlığını Gizleme

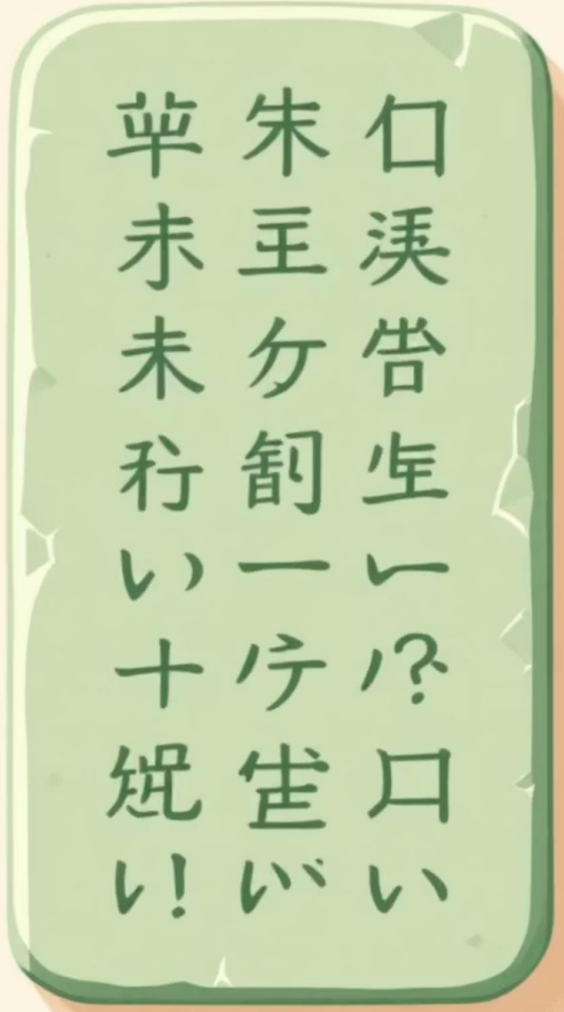
Antik Yunanlıların Yaklaşımı

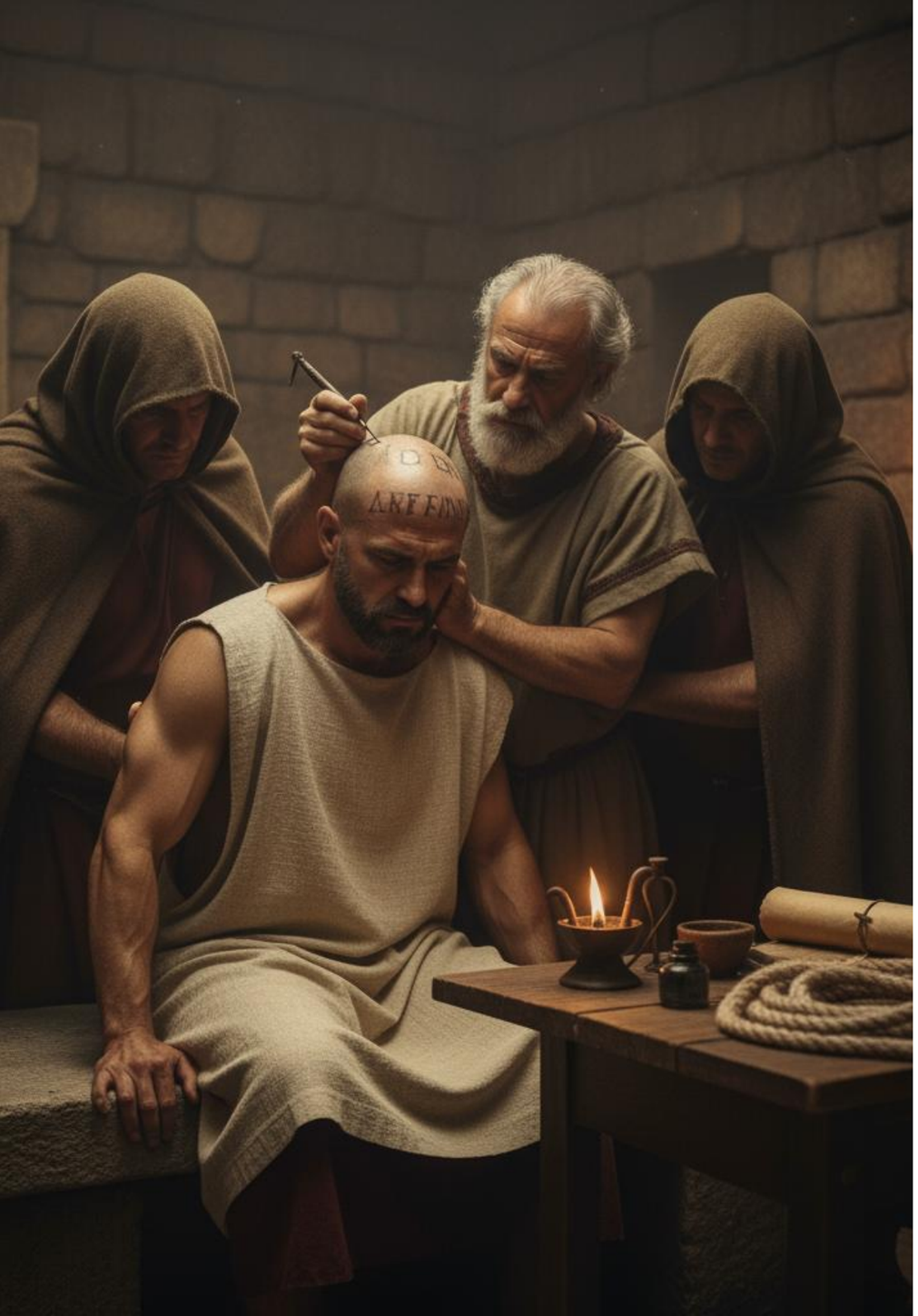
MÖ 600'lü yıllarda Antik Yunanlılar, düşmanın mesajları ele geçirmesini önlemek için yaratıcı yöntemler geliştirdi. Mesajları mürekkepli ahşap tabletlere yazıp, üzerine balmumu ile kaplayarak gizlediler.

- Balmumun üzerine zararsız mesajlar yazma
- Yara bandajı şeklinde gizleme
- Küpe içine saklama
- Dövme olarak yazma
- Sandal ya da katır tırnağına gizleme

Steganografi Tanımı

Steganografi (Yunanca'da "örtülü yazı"), mesajın veya bilginin **varlığını** gizlemeyi amaçlar. Modern uygulamalarda, veriler genellikle resim, ses veya video dosyaları içinde saklanır.





Düşünün ki, bir mesajı yazmak yerine bir insanın kafasına dövme yapıyorsunuz!

Kölenin başı kazınıyor, mesaj kafa derisine işleniyor.

01

Sonra saçları uzayana kadar bekleniyor, böylece mesaj tamamen gizleniyor.

02

Köle hedefe ulaştığında, saçlar tekrar kazınıyor ve gizli mesaj ortaya çıkıyor.

03

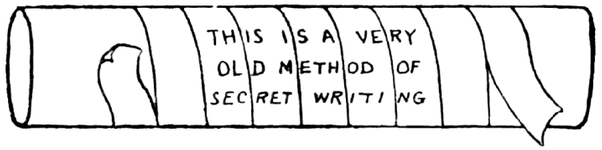
Bu hikâye bize şunu gösteriyor:

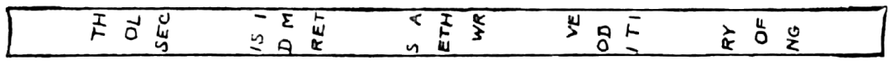
İnsanlık binlerce yıldır bilgiyi saklamanın yollarını arıyor.

Antik Yunan'da
scytale

Bu yöntem, askerî haberleşmede kullanılırdı. Mesaj, bir uzun ve ince parşömen şeridine yazılır ve tahta çubuğun etrafına sarılırdı.

Yalnızca aynı çapta başka bir çubuğa sarıldığında harfler düzgün bir şekilde okunabilir hale gelirdi.





Böylece mesaj, yolculuk sırasında ele geçirilse bile hiçbir anlam ifade etmezdi, çünkü parşömen düz bir şekilde açıldığında harfler karışık görünürdü.

Scytale, böylece kriptografinin ilk mekanik uygulamalarından biri olarak tarihe geçmiştir.

Kriptografinin Temelleri

Alice ve Bob: Kriptografinin İkonik Karakterleri

Kriptografik Ailenin Doğuşu

1978 yılında MIT araştırmacıları, karmaşık güvenli iletişim senaryolarını açıklamak için iki karakter yarattı: **Alice** ve **Bob**. Bu basit isimlendirme, "A" ve "B" yerine kullanılarak, akademik makalelerdeki karmaşık mantığın takip edilmesini kolaylaştırdı.

Araştırmacılar, sürekli kendi adlarını tekrarlamak yerine geleneksel kadın ve erkek isimleri seçtiler. Böylece "o" (dişil) ve "o" (eril) zamirlerini kullanarak açıklamalarını daha anlaşılır hale getirdiler.

Kriptografik Ailenin Genişlemesi

Alice & Bob

İletişim kuran temel taraflar. Güvenli mesajlaşma senaryolarının merkezinde yer alırlar.

Eve

Kulak misafiri (eavesdropper). İletişimi gizlice dinlemeye çalışan pasif saldırgan.

Mallory

Kötü niyetli saldırgan (malicious). Aktif olarak iletişimi manipüle eden ve değiştiren tehdit aktörü.

Trudy

Davetsiz misafir (intruder). Sisteme yetkisiz erişim sağlamaya çalışan saldırgan.

Wendy

İfşacı (whistleblower). Gizli bilgileri açığa çıkaran karakter.

Carol

Üçüncü taraf. Genel iletişim senaryolarında yer alan ek karakter.

Bugüne kadar, kriptografik ailenin adı geçen **26 üyesi** bulunmaktadır. Bu karakterler, karmaşık güvenlik protokollerini açıklamak için evrensel bir dil haline gelmiştir.

Modern Steganografi ve Obfuscation

1 Steganografi

Veriyi zararsız görünen dosyaların (resim, ses, video) görünmez bölümlerine gizler. Dosya başlık alanları (header) veya metadata bölümlerine veri yerleştirir.

2 Veri Maskeleme

Orijinal verinin bir kopyasını oluşturarak onu anlaşılmaz hale getirir. Hassas bilgilerin test ortamlarında kullanılmasını sağlar.

3 Tokenizasyon

Hassas veri öğelerini rastgele bir karakter dizisine (token) dönüştürür. Kredi kartı bilgileri gibi kritik verileri korur.

Obfuscation (karartma), bir şeyi belirsiz hale getirme eylemidir ve siber güvenlikte çeşitli biçimlerde kullanılır.

Kriptografi: Anlamı Gizleme

Steganografinin aksine, kriptografi mesajın **varlığını** değil, **anlamını** gizler. Antik Yunanlılar, mesajı ele geçiren düşmanın içeriği anlayamaması için iki temel yöntem geliştirdi:

1

Yer Değiştirme (Transposition)

Mesajdaki her harfin yerinin yeniden düzenlenmesi. Örnek: "run" → "nru"

Avantaj: Uzun mesajlarda etkili

Dezavantaj: Kısa mesajlar kolayca kırılabilir

2

İkame (Substitution)

Bir harfin yerine başka bir harfin konulması. ROT13 örneği: "security" → "frpheugl"

Avantaj: Basit uygulanabilir

Dezavantaj: Frekans analizi ile kırılabilir

Kriptografinin Temel Kavramları

Şifreleme ve Şifre Çözme

Kriptografi, bilginin yetkisiz kişilerce anlaşılamayacak şekilde dönüştürülmesi uygulamasıdır. Bu süreç iki temel aşamadan oluşur:

Şifreleme (Encryption)

Orijinal metni karıştırılmış bir mesaja dönüştürme süreci

Şifre Çözme (Decryption)

Mesajı orijinal biçimine geri döndürme işlemi

Kriptografi Terminolojisi

Plaintext (Düz Metin)

Şifreleme için girdi olan şifrelenmemiş veri veya şifre çözmenin çıktısı olan metin. Okunabilir ve anlaşılır biçimdedir.

Ciphertext (Şifreli Metin)

Şifrelemenin karıştırılmış ve okunamayan çıktısı. Yetkisiz kişiler tarafından anlaşılamaz durumdadır.

Cleartext (Açık Metin)

Şifrelenmesi amaçlanmayan şifrelenmemiş veri. Kasıtlı olarak "açık" bırakılan bilgidir.

Bu terminoloji, kriptografik işlemlerin her aşamasında standart bir dil sağlayarak, güvenlik protokollerinin net bir şekilde tanımlanmasını mümkün kılar.

Kriptografik Algoritma ve Anahtar

1 Kriptografik Algoritma

Matematiksel bir formüle dayanan prosedürler dizisi. Aynı zamanda **şifreleme** olarak da adlandırılır. Algoritmalar herkese açık ve iyi bilinecek şekilde tasarlanır.

2 Anahtar (Key)

Şifreli Metin üretmek için algoritmaya girilen matematiksel değer. Tıpkı fiziksel bir kilit gibi, veriyi "kilitlemek" için kullanılır.

3 Şifreleme Süreci

Düz Metin + Algoritma + Anahtar = Şifreli Metin. Bu süreç tersine çevrilerek şifre çözme gerçekleştirilir.

Kritik Güvenlik İlkesi: Kriptografik algoritmalar herkese açık olabilir, ancak anahtar her zaman gizli tutulmalıdır. Güvenlik, algoritmanın gizliliğine değil, anahtarın gizliliğine dayanır.

Kriptografinin Güvenlik Felsefesi

Kerckhoffs İlkesi

Modern kriptografinin temel prensibi: Bir kriptografik sistemin güvenliği, **yalnızca anahtarın gizliliğine** dayanmalıdır. Algoritmanın nasıl çalıştığı bilinse bile, anahtar olmadan sistem güvenli kalmalıdır.

> "Güvenlik, gizlilik yoluyla değil, matematiksel sağlamlık yoluyla sağlanır."

Açıklık İlkesi

Kriptografik algoritmalar kamuya açık olmalı ve akademik incelemeye tabi tutulmalıdır. Bu, güvenlik açıklarının tespit edilmesini ve düzeltilmesini sağlar.

Anahtar Yönetimi

Anahtarların güvenli üretimi, dağıtımı, saklanması ve imhası kritik öneme sahiptir. Zayıf anahtar yönetimi, en güçlü algoritmayı bile işe yaramaz hale getirir.

Hesaplama Karmaşıklığı

Modern kriptografi, saldırganın anahtarı kaba kuvvet ile bulmasının hesaplama açısından imkansız olmasına dayanır. Matematiksel zorluk, güvenliğin temelidir.

Kriptografi ve Bilgi Güvenliği

Modern dijital çağda bilgi güvenliğinin temel taşlarından biri olan kriptografinin inceliklerini keşfetmeye hoş geldiniz. Bu sunumda, şifreleme tekniklerinin nasıl çalıştığını, neden bu kadar önemli olduğunu ve günlük hayatımızda nasıl kullanıldığını öğreneceksiniz.

Kriptografi Neden Bu Kadar Önemli?

Kriptografi, bilgiyi şifreleme yoluyla gizleme sanatıdır. Tehdit aktörlerinin hassas verilere erişmesini engelleyerek, kuruluşların en değerli varlıklarını korumalarına yardımcı olur. Bu, risk azaltma stratejilerinin (mitigation) merkezinde yer alır ve sistemleri saldırılara karşı daha dirençli hale getiren bir sertleştirme (hardening) tekniğidir.

Kriptografinin benzersiz özelliği, verinin üç farklı durumunda da koruma sağlayabilmesidir: bekleyen veri (data at rest), kullanılan veri (data in use) ve aktarılan veri (data in transit). Bu çok yönlü koruma, onu günümüz dijital güvenlik stratejilerinin vazgeçilmez bir parçası yapar.

Kriptografinin Beş Temel Kullanım Alanı

Gizlilik (Confidentiality)

Yalnızca yetkili tarafların bilgiyi görebilmesini sağlar. Şifrelenmiş veriler, anahtara sahip olmayan kişiler için anlamsız görünür.

Bütünlük (Integrity)

Bilginin doğru olmasını ve yetkisiz değişikliklerden korunmasını sağlar. Verinin bozulmamış olduğunu garanti eder.

Kimlik Doğrulama (Authentication)

Gönderenin kimliğini doğrular. Sahtekarların sisteme girmesini ve hileli mesajlar göndermesini önler.

İnkâr Edilemezlik (Nonrepudiation)

Bir eylemi gerçekleştiren kişinin bunu reddedemeyeceğini kanıtlar. Dijital imzalar bu prensibi kullanır.

Gizleme (Obfuscation)

Veriyi anlaşılmaz hale getirir. Yetkisiz kullanıcılar şifrelenmiş içeriği okuyamaz.

Gizleme: Yaygın Bir Yanlış Anlama

❌ Gizlilik Yoluyla Güvenlik (Hatalı Yaklaşım)

Bazı kuruluşlar "kötü adamlar bunu bilmiyorsa, güvenlidir« mantığıyla hareket eder. Bu yaklaşım **tehlikelidir** çünkü güvenlik yalnızca bir şeyin bilinmemesine dayanır.

- Sırların tamamen gizli kalması neredeyse imkansızdır
- Er ya da geç keşfedilecek ve güvenlik çökecektir
- Tek başına bir koruma mekanizması olamaz

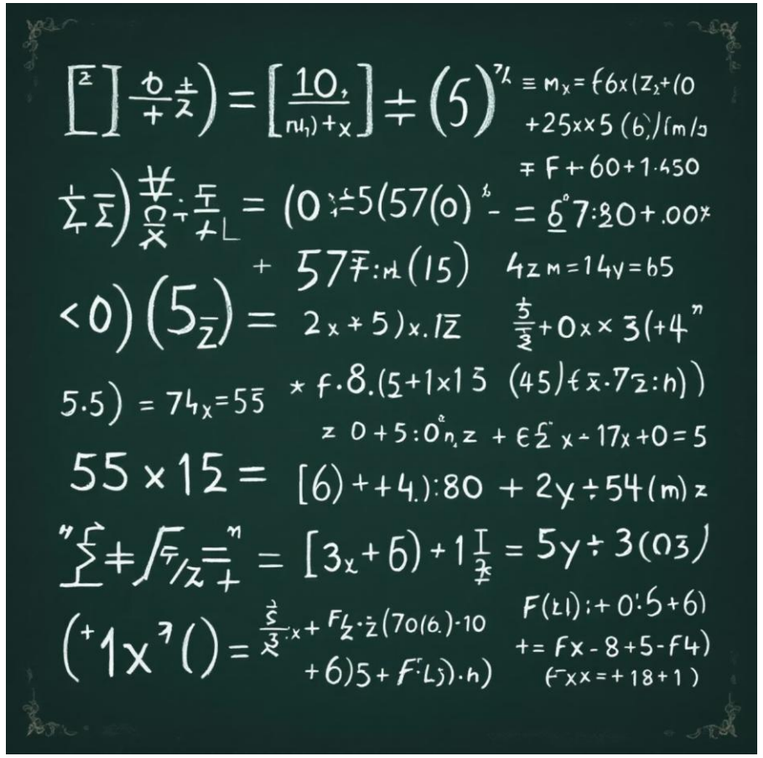
✅ Modern Kriptografi (Doğru Yaklaşım)

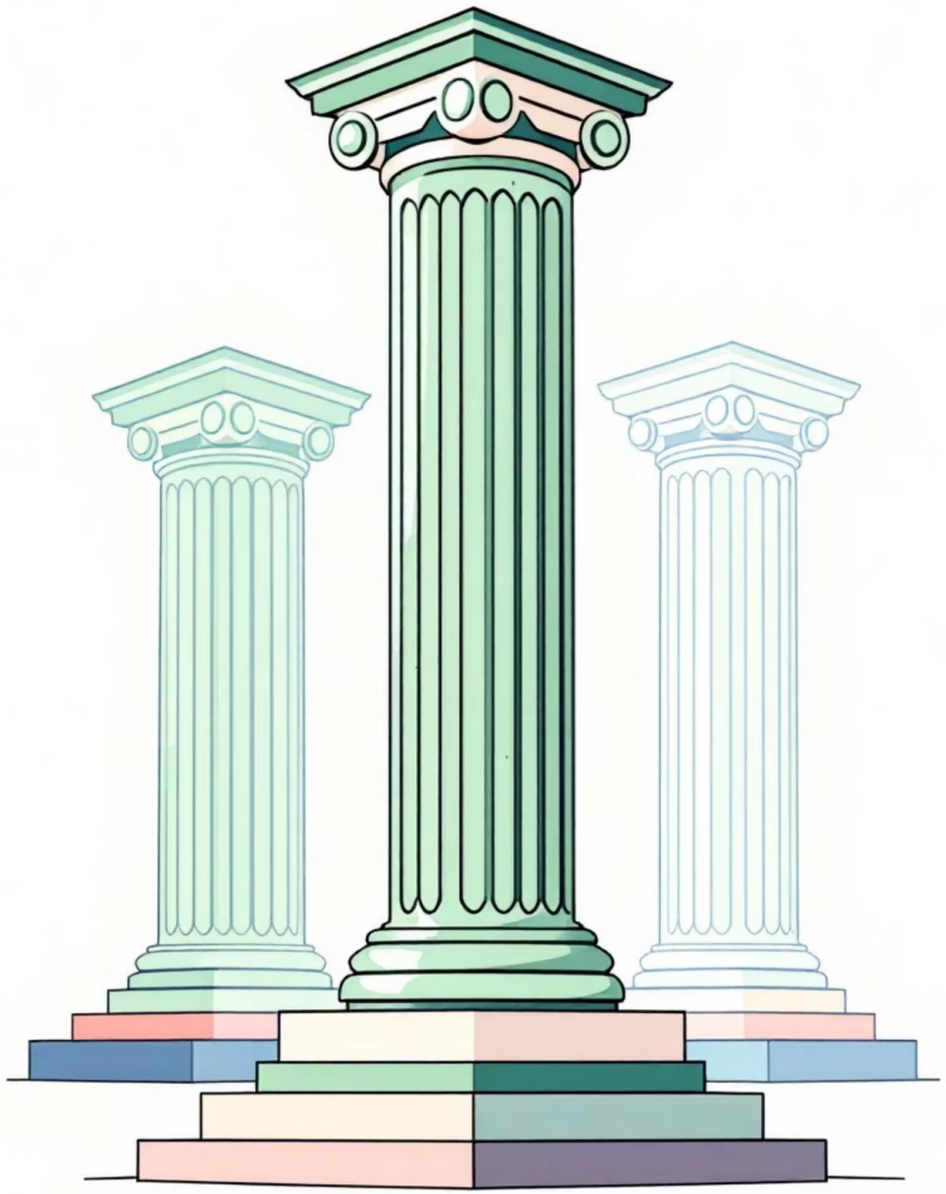
Güvenlik, **kanıtlanmış matematiksel ilkelere** dayanmalıdır. Algoritmaların kendisi herkese açık olabilir, güvenlik anahtarların gizliliğinden gelir.

- Açık algoritmalar topluluk tarafından incelenir
- Zaman içinde güvenirlikleri kanıtlanmıştır
- Tescilli "gizli" algoritmalardan kaçının

⚠️ Önemli Uyarı

Bazı yazılım geliştiricileri "askeri düzeyde" diye lanse ettikleri tescilli kriptografik algoritmalar yaratır. Bu algoritmalar zayıftır ve düzgün analiz edilmemiştir. **Asla kullanılmamalıdır!**





Kriptografik Algoritmaların Üç Ana Kategorisi

Hash Algoritmaları

Tek yönlü şifreleme yapan algoritmalar. Verinin benzersiz bir "dijital parmak izi"ni oluşturur. Bu parmak izi ile orijinal veriye geri dönemezsiniz.

- Veri bütünlüğünü korur
- Karşılaştırma için kullanılır
- Geri döndürülemez

Simetrik Algoritmalar

Şifreleme ve çözme için aynı anahtarı kullanan algoritmalar. "Özel anahtarlı kriptografi" olarak da bilinir.

- Hızlı ve verimli
- Anahtar dağıtımı zor olabilir
- Anahtar gizli kalmalıdır

Asimetrik Algoritmalar

Bir genel ve bir özel olmak üzere iki anahtar kullanan algoritmalar. "Genel anahtarlı kriptografi" olarak da bilinir.

- Anahtar dağıtımı kolaydır
- Daha yavaş işlemler
- Modern internetin temelidir

Hash Algoritmaları: Dijital Parmak İzleri

Hash algoritmaları, herhangi bir boyuttaki veriyi sabit uzunlukta bir "özet" (digest) haline dönüştürür. Bu özet, verinin benzersiz bir dijital parmak izi gibidir ve orijinal veriye geri döndürülemez.

Sabit Boyut

İster 1 sayfalık bir belge, ister 1000 sayfalık bir kitap olsun, hash çıktısı **her zaman aynı boyuttadır**. Bu tutarlılık, karşılaştırmaları kolaylaştırır.

Benzersizlik

İki farklı veri kümesi **aynı hash'i üretemez**. Her verinin kendi benzersiz parmak izi vardır. Bu özellik, veri bütünlüğünü garanti eder.

Orijinallik

İstediğiniz bir hash değerini üreten bir veri kümesi oluşturmak **hesaplama açısından imkansızdır**. Bu, saldırganların sahte veri oluşturmasını önler.

Geri Döndürülemezlik

Hash'ten orijinal veriyi elde etmek **matematiksel olarak mümkün değildir**. Bu tek yönlü fonksiyon, parolaların güvenli saklanmasını sağlar.

Hash algoritmaları günlük hayatta yaygın olarak kullanılır: şifre doğrulama, dosya bütünlüğü kontrolü, dijital imzalar ve blockchain teknolojisi. Örneğin, bir web sitesine girdiğiniz şifre hiçbir zaman olduğu gibi saklanmaz - onun hash'i saklanır ve her girişte karşılaştırılır.

Simetrik vs. Asimetrik Kriptografi

🔑 Simetrik Kriptografi

Şifreleme ve çözme için **tek bir anahtar** kullanır. Bu anahtarın gizli kalması kritik öneme sahiptir.

Avantajlar:

- Çok hızlı ve verimlidir
- Büyük veri miktarları için idealdir
- Hesaplama maliyeti düşüktür

Dezavantajlar:

- Anahtar dağıtımı zorludur
- Çok kullanıcılı sistemlerde karmaşıklaşır
- Anahtar güvenliği kritiktir

Örnek: AES (Advanced Encryption Standard), en yaygın simetrik algoritmadır ve WiFi şifrelemeden disk şifrelemeye kadar her yerde kullanılır.

🔐 Asimetrik Kriptografi

İki farklı ancak matematiksel olarak bağlı anahtar kullanır: **genel anahtar** ve **özel anahtar**.

Avantajlar:

- Anahtar dağıtımı kolaydır
- Genel anahtar herkesle paylaşılabilir
- Dijital imza desteği vardır

Dezavantajlar:

- Simetrik şifrelemeden yavaştır
- Daha fazla hesaplama gücü gerektirir
- Büyük dosyalar için pratik değildir

Örnek: RSA ve ECC (Elliptic Curve Cryptography), HTTPS bağlantılarının ve e-posta şifrelemenin temelini oluşturur.