ÇİN KALAN TEOREMİ (CRT)

PARÇALARDAN BÜTÜNE, GİZLİLİKTEN GÜVENE!

Ordumu nasıl gizlerim?

Yaklaşık **2000 yıl önce** Sun Zi tarafından ortaya atılan bu fikir, bugün kredi kartı işlemlerinizden mesajlaşma şifrelemelerine kadar **her yerde** çalışıyor!

Alışverişim güvenli mi?

1 MANTIK: PARÇALARDAN BÜTÜNE GİTMEK

Bir sayının kendisini bilmeseniz bile, o sayının farklı sayılara bölümünden kalanlarını biliyorsanız, orijinal sayıyı tek bir şekilde bulabilirsiniz.

KLASİK ÖRNEK:

Bir grup askeriniz var.
Sayılarını tam bilmiyorsunuz ama...

- **3**'erli dizildiklerinde **2** kişi artıyor.
- **5**'erli dizildiklerinde **3** kişi artıyor.
- **7**'şerli dizildiklerinde **2** kişi artıyor.

Bu veriler birleştiğinde, matematik bize bu grubun en az **23** kişi olduğunu söyler!

Matematiksel Gösterim:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \rightarrow x = 23$$

(en küçük pozitif çözüm)

Bütün koşulları sağlayan en küçük sayı: 23!

2 ANTİK STRATEJİ: ORDUYU GİZLEMEK

1. GİZLİLİK

Askerleri farklı gruplara ayırıp sadece artanları not ederlerdi.

2. CASUSLARIN ELİNDE SADECE PARÇALAR VAR

Casuslar bu bilgileri ele geçirirse bile...

3. SADECE GENERAL BİRLEŞTİRİR

Tüm kalanları birleştiren tek kişi generaldir ve gerçek sayıyı bulur.

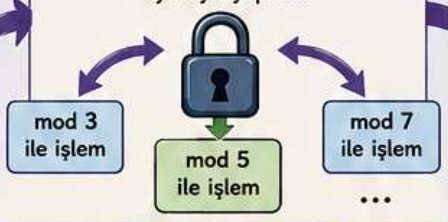
3 MODERN KRİPTOGRAFİ: RSA VE HIZ

BÜYÜK VERİ SORUNU

Dijital şifrelemede kullanılan sayılar çok büyüktür (yüzlerce basamak!). Bilgisayarlar bu sayılarla işlem yaparken yorulur.

CRT ÇÖZÜMÜ

CRT, bu devasa sayıları daha küçük parçalara (modüllere) böler. İşlemler bu küçük parçalar üzerinde ayrı ayrı yapılır...



SONUÇ: HIZ KAZANIMI!

Sonuçlar tekrar birleştirilir ve şifre çözme işlemi yaklaşık 3–4 kat daha hızlı gerçekleşir!

~2000 YIL ÖNCE

Bir generalin "Kaç askerim var?" sorusuna cevap ararken bulduğu yöntem...

ÇİN KALAN TEOREMİ

GÜNÜMÜZDE

Sizin "Bu alışveriş güvenli mi?" sorunuza saniyeler içinde cevap veren dijital anahtarın dişlilerini oluşturuyor!

Matematik, **zamanın ötesinde bir dildir!**