

I. Kriptografiye Giriş

I.II Kriptanaliz Türleri

Önceden de belirttiğimiz gibi, kriptanaliz kriptolojinin başkaları tarafından kullanılan kriptografik sistemleri kırmak üzerine çalışır.

Bilinen en eski kriptanaliz kitabı olan “Treatise on Cryptanalysis” 801 AD ve 873 AD arasında yaşamış Al-Kindi’ye aittir. Al-Kindi’nin kitabındaki ana konular kriptanaliz metodları, kriptanaliz şifreleri ve Arapça frekans analizidir.

Tarihsel olarak, frekans analizi basit şifreleri kırmanın ana tekniği olmuştur. İstatistikleri kullanarak tek harfli kelimelerin ve kombinasyonlarının doğal dillerdeki frekanslarını ölçer. Modern kriptanalizde, şifreler daha kompleks oldukları için, frekans analizi diğer matematiksel teknikler üzerindeki üstünlüğünü kaybetmiştir.

Kriptanaliz kriptanalistin ulaşabileceği bilgi miktarına göre bazı alt gruplarına bölünebilir. Kriptanaliz türleri şöyledir:

- **Surf şifremin saldırısı:** Kriptanalist şifremin örneklerini ve düzmetin ile ilgili bazı istatistiksel özelliklerini bilmektedir.
- **Bilinen düzmetin saldırısı:** Kriptanalist şifremin/düzmetin çiftlerinin örneklerini elde eder.
- **Seçili düzmetin saldırısı:** Kriptanalist bir kaç düzmetin yaratır ve bunların şifreminlerini alır.
- **Uyarlamalı seçili düzmetin saldırısı:** Kriptanalist bir kaç seçili düzmetin saldırısı yapar ve öncekilerden elde ettiği bilgileri yeni düzmetin saldırısı için kullanır.

Unutmayın ki, amaç her zaman anahtarın tamamını bulmak veya tüm şifreminin şifresini çözmek değildir. Daha çok, bu yolda yardımcı olacak bilgileri elde etmektir.

Anahtar Uzayı anahtarın sahip olabileceği tüm muhtemel değerleri ifade eder. Anahtar uzayının boyutu kritiktir, zira eğer yeterince büyük değilse, düzmetin-şifremin çiftleri kullanarak, saldırgan tüm anahtar uzayını deneyerek doğru anahtarı bulabilir. Geniş kapsamlı anahtar arama bazen kaba kuvvet saldırısı (brute-force attack) olarak da nitelenir, zira hiçbir zeka bulundurmamaktadır. Kriptanalistin hedefi kaba kuvvet saldırısından daha etkili bir saldırı bulabilmektir.