

II. Kriptografiye Giriş

II.III Basit Şifrelerin Tarihi Örnekleri

Öteleme Şifresi

En eski şifrelerden biri Caesar şifresidir, Julius Caesar'a aittir. Bu methodda 'a' 'D', 'b' 'E', 'c' 'F' olur. . . , ve 'z' 'C' olur. Bu fikirin genel uygulaması şifreletiminin her zaman '3' yerine 'k' harf ötelenmesine dayanır. Bu durumda, 'k' ikame şifresi olarak bilinen şifrenin anahtarı olur. Bu süreç sağdaki animasyonda gösterilmektedir. (Genel olarak, kriptoloji topluluğunda A ve B harfleri için Alice ve Bob kullanılır).

Daha teknik terimler ile, ikame şifresinin işlevi şu formüller ile açıklanabilir:

$$C = EK(P) = P + K \text{ mod } n$$

$$P = DK(C) = C - K \text{ mod } n$$

Burada 'n' dildeki harflerin sayısını gösterir. Mesela bu İngilizce için '26'dır. Düzmetin (P), Şifreletimin (C) ve Anahtar (K) 0 ile 25 arasında bir sayı değeri alır. Bu kısaca şöyle gösterilebilir

$$P = C = K = \mathbb{Z}_{26}$$

Toplama ve çıkarma işlemleri n modunda yapılır.

$$\text{Örnek: } 15+21 = 10 \text{ mod } 26.$$

İkame Şifresi

$P=C=\mathbb{Z}_{26}$ olsun. K 26 sembol $0,1,\dots,25$ 'in tüm permütasyonları olsun. Tüm permütasyonlar için $? \in K$,

$$C = E_{?}(P) = ?(C)$$

$$P = D_{?}(C) = ?^{-1}(C)$$

olarak tanımlansın,

ve $?^{-1}$, $?$ 'nin ters permütasyonu olsun.

Özellikler:

- İkame Şifresi için olan bir anahtar basitçe 26 alfabetik karakterin bir permütasyonundan oluşur.
- Bu permütasyonların sayısı $26!$ dir, ve 4.0×10^{26} 'dan bile büyük bir sayıdır.
- Bu yüzden, tüm anahtarları aramak bir bilgisayar için bile mümkün değildir.

- Fakat, bir İkame Şifresi başka metodlar ile kriptanalizden geçirilebilir. Nasıl?

Vigenere Şifresi

m sabit bir pozitif tam sayı olsun. $P=C=K=(Z_{26})^m$ olsun. $K = (k_1, k_2, \dots, k_m)$, gibi bir anahtar için,

$$E_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

$$D_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

olarak tanımlansın. tüm işlemler ise Z_{26} 'da yapılsın.

Özellikler:

- Öteleme Şifresi ve İkame Şifresi monoalfabetiktir (düzmetindeki tüm harfler şifremetin olarak sabit bir harfe dönüştürülür). Vigenere Şifresi polialfabetiktir (dönüşüm metnin yerine göre değişir).
- Polialfabetik özellik Vigenere Şifresini frekans analizine karşı daha güçlü kılar. Ve fakat, Kasiski tarafından 1863'te kırılmıştır.