Şifreleme Teknikleri

Klasik şifremele yöntemleri aşağıdaki gibi özetlenebilir.

Gizli Jargon

Gönderici ve alıcı arasında önceden belirlenmiş bir jargon dizisi ile yapılan gizli haberleşmedir. İzciler tuvalet ihtiyaçlarını "hava almak", "çiçek toplamak" ve "çelenk bırakmak" gibi ifadelerle dile getirirler. Böylece ayıp sayılan sözcükleri kullanmadan, aralarında gizli bir haberleşme mütabakatı sağlamış olurlar. İzcilerin telsizle haberleşmesinde konuların doğrudan söylenmesi yerine ima edilmesi de bu türden bir uygulamadır. Örneğin: "Görev ekibi birinci buluşma noktasına doğru yola çıktılar" ifadesinde kişiler ve mekan açıkça belirtilmemiş, önceden bilinen mütabakat kastedilmiştir. Obalar özellikle rekabet halindeyken yazılı, sözlü ve telsiz haberleşmelerinde kendilerine özgü jargonları kullanabliler.

Steganografi (Saklama)

Mesajın farklı bir metin, görsel veya ses içinde saklanması sıkça kullanılan bir yöntemdir. Bu tekniğe Steganografi adı verilmektedir. Steganografi kendi başına çok kapsamlı bir kriptoloji tekniğidir. Modern kriptolojide dijital resim ve seslerin içinde, sadece uygun yazılımlarla çözülerek ortaya çıkarılabilen gizli mesajların saklanması mümkündür.

Roma döneminde mesajcıların saçları kazıtılıp gizli mesajlar kafa derisi üzerine dövme yapılarak yazılıyordu. Daha sonra saçları uzayan haberci, mesajını güvenle taşıyabiliyor, şüphe çekmiyordu.

İzcilerin tercih ettikleri yaygın uygulamalarda, çoğunlukla gizli mesaj "masum" bir metin içinde, sadece saklama kuralını bilenler tarafından anlaşılacak şekilde saklanır. Bu kitapçıkta "Saklı Mesajımız" bölümündeki uygulama Steganografi tekniğine güzel bir örnek olarak verilebilir.

Anlamsız Şifreleme

Kriptoloji bilminde "Null Cipher" olarak geçen "anlamsız şifreleme" tekniğinde, şifrelenecek mesaj, araya sokulan anlamsız harflerle gizlenir. Bu teknik Steganografi yönteminin en basit şekli olarak da kabul edilebilir. Bu kitapçıkta yer alan "Grilles Şifresi" anlamsız şifreleme tekniğine güzel bir örnek olarak verilebilir.

Yer Değiştirme

Bazı kaynaklarda "Karıştırma Yöntemi" olarak da geçen yer değiştirme tekniği, metinde kelimelerin veya sıklıkla hafrlerin yer değiştirilmesiyle anlamın gizlenmesi prensibine dayanan yöntemdir. Mesajın belirli bir kurala göre karıştırılması; kelime, paragraf veya tüm metin içinde harflerin yer değiştirilmesi prensibine göre yapılan şifreleme yöntemidir. En basit

uygulama kelimelerin veya paragrafların tersten yazılmasıdır. Kelimeleri tersten okuma, hem eğlenceli bir oyun hem de şifreli haberleşme uygulaması olarak kaşiflerin ilgisini çekmektedir.

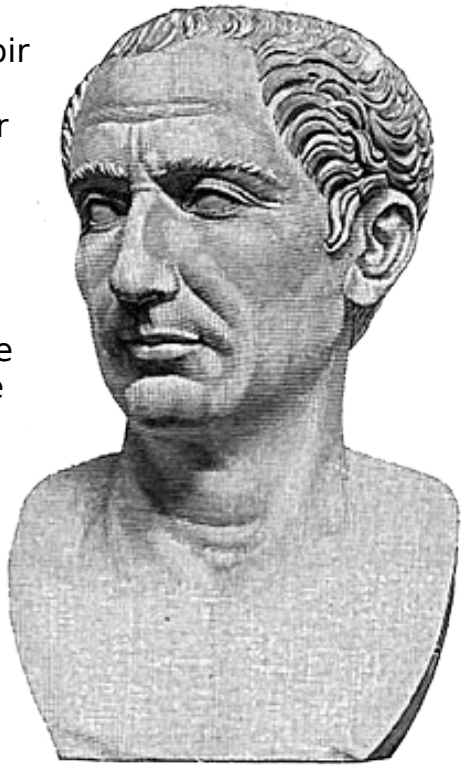
Bu kitapçıkta yer alan “Scytale Şifresi” yer değiştirme tekniğine güzel bir örnek olarak verilebilir.

Yerine Koyma

Doğal alfabenin yerine kullanılabilecek, gizli bir alternatif alfabenin kullanılması prensibidir. Bu yönteme substitution (yerine koyma) metodu da denilmektedir. Obalar, üniteler kendi sembollerinden oluşan gizli alfabelerini oluşturup haberleşme amacıyla kullanılabilirler. Mesajlar gizli alfabeyle yazılır, dönüşüm tablosu kullanılarak deşifre edilir. İzcilikte sıkça kullanılan gizli kodlama yöntemlerinden biri Pinpen şifresidir. Bu kitapcıkta Pinpen Şifresi detaylı bir şekilde anlatılmaktadır.

Kaydırma

Prensip olarak yerine koyma metodunun bir türüdür. Sözcükleri oluşturan harflerin belirli bir düzenle ötelenmesi, kaydırılmasıyla metinler şifrelenir. Genellikle kaydırma miktarı basit bir sayı olarak uygulanır. Örneğin anahtar olarak “3” kullanıldıysa, A harfi yerine alfabedeki üçüncü harf olan C harfi kullanılır. Benzer şekilde B yerine Ç, C yerine D harfleri kullanılır. Bu şifreleme 3 anahtarını bilen alıcı tarafından kolayca çözülebilir. Şifreli mesaj ele geçerse “kaba kuvvet” olarak bilinen deneme yanılma yöntemiyle zor da olsa çözümlenebilir. Bu nedenle anahtar olarak basit bir sayı kullanmak yerine farklı yöntemler kullanılabilir. Örneğin: her kelime için anahtarı bir artırmak gibi.



Bu yönteme, Roma İmparatoru Jul Sezar tarafından icat edildiği için “Sezar Şifresi” adı da verilmektedir.

Anahtarlama

Modern şifreleme yöntemlerinde kullanılan anahtarlama yönteminde alıcıda bulunan bir anahtar kelime veya sayı dizisi temel alınır. Şifreleme bu parolanın kaydırma düzeni kullanılarak yapılır. Kelimeleri oluşturan her bir harf anahtardaki karşılığı kadar kaydırılır. Modern kriptolojide, dijital ortamlarda, bu kaydırma işlemi, harfleri oluşturan ikili (binary) sayıların bitleri boyunca yapılır.

Hibrit Yöntemler

Yukarıda belirtilen yöntemlerin birkaçının beraber kullanılmasıyla gerçekleştirilen şifreleme yöntemleridir. Örneğin: Bir metin önce yer değiştirme (karıştırma), sonra yerine koyma ve nihayet kaydırma yöntemleri ile birkaç kez üstüste şifrelenerek çözülmesi neredeyse imkansız bir hale getirilebilir.