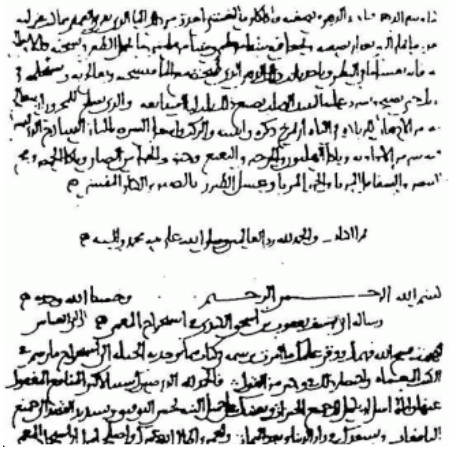
ŞİFRE: HAYATIMIZA NE ZAMAN VE NASIL GİRDİ?

Normal metindeki karakter veya verileri anlaşılamayan karakter veya verilerle değiştirmeye şifreleme denir. İmparator Sezar ve ABD başkanlarından Jefferson, kendi adlarıyla anılan şifreler geliştirmişti.

Yunanlılar'ın Skytale adlı şifre aleti

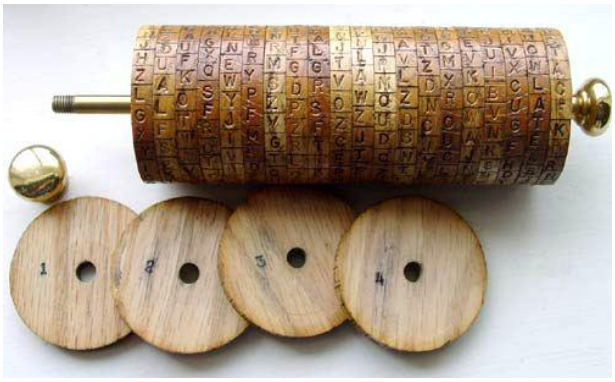
Şifreleme 3500 Yıl Öncesine Uzanır

Şifre kelimesi İngilizce "cipher" olarak yazılır ve Arapça'daki "sifr" yani sıfır kelimesinden gelir. Sümerler'in ustaları, renkli seramik sırlarının reçetesini gizlerdi. Bu nedenle günümüzde bile "sırlı seramik" ifadesi kullanılır. Bir Mezopotamya tabletinde (M.Ö. 1500) şifreli yazı ile seramik sırrının yapımı anlatılır. İbrani peygamber Yeremya, M.Ö. 600-500'lerde ATBASH şifresini kullandı. Şifrede, alfabenin ilk harfi son harfle, ikinci harf sondan ikinci harfle yer değişir. Böylece alfabenin ilk yarısındaki harfler, ikinci yarıdaki uygun harfle yer değiştirmiş olur. AĞAÇ kelimesinin şifrelenmiş hali "ZRZÜ" dür. Her harfe bir sayı belirleyen şifre örneği "Ebced" hesabıdır. Cümledeki harflerin ebced tablosundaki sayısal karşılığı ile bir olayın tarihini belirlemeye tarih düşürme denir (*).



El Kindi'nin şifre kırma eserinin ilk sayfası

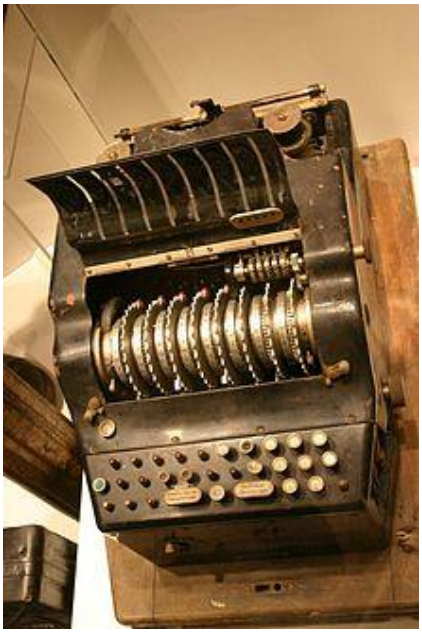
Askeri Amaçlı Gizli Mesaj Örnekleri
Yunanlılar, M.Ö. 5-3. yüzyılda "Skytale" adlı şifreleme aletini savaşta kullandı. Kalın bir sopaya deri şerit sarılırdı. Mesaj şeritin üzerine sopa boyunca yazılır ve şerit açık olarak yollanırdı. Karşı taraf, şeridi aynı kalınlıkta bir sopaya sarıp mesajı okurdu. Roma İmparatoru Sezar'ın şifresi, harfleri alfabede 3 harf sonrasındaki ile değiştirmeye dayanırdı. Sezar Şifresi, Galya Savaşı'nda kullanıldı. Şifrede "A" yerine 3 harf sonra gelen Ç, "S" yerine U ve "Z" yerine C yazılır. Sezar şifresiyle "SEZAR" yazarsak UĞCÇT olur. Bir Yunanlı, M.Ö. 480'de İran'da iken kölesinin saçlarını kazıttı ve başına dövme ile Persler'in saldırı planını yazdı. Saçı uzatılan köle, Yunanistan'a gizli mesajı iletti. Kurtuluş Savaşı sırasında ordumuz, mesajları kağıda limon suyuyla yazdı. Mesajı alan, kağıdı soba üstünde ısıtınca yazı okunur hale gelirdi.



ABD Başkanı Thomas Jefferson'un 1790'da geliştirdiği şifreleme diski

Şifre Kırma Teknikleri
Frekans analiziyle şifre kırma tekniğini, Müslüman matematikçi El Kindi (801-873) buldu. Sezar Şifresi ve benzerlerinin çözümünü anlatan eser, Süleymaniye Osmanlı Arşivi'ndedir. Önce, şifreli mesajın yazıldığı dildeki normal bir metinde her harfin kaç kez kullanıldığı sayılır (frekans). Türkçe metinde "A" harfi binde 121 kez, "B" 25 kez geçer. Sonra şifreli metindeki harflerin de kaç kez kullanıldığı bulunur. Şifreli metin Türkçe ise, en çok kullanılan harfin "A" olduğu anlaşılır. İlgili dilde harflerin kullanım yüzdesinden, şifreli metnin harf karşılığı bulunup şifre kırılır. İtalyan Vigenere'nin, 1553'te geliştirdiği çok alfabeli şifreyi İngilizler kırdı. ABD Başkanı Thomas Jefferson, 1790'da 26 diskten oluşan şifreleme diskini geliştirdi. Jefferson Diski'nde istenilen mesaj, diskleri döndürerek bir satıra yazılır. Diskteki diğer bir sıradaki harf dizisi şifre metni olarak karşı tarafa iletilir. Aynı diske sahip olan alıcı diskte şifre metni yazınca diskin başka bir sırasındaki anlamlı mesajı bulup okur. Mucit olan Başkan Jefferson, ABD kriptolojisinin atası olarak anılır. Yeni şifreler geliştikçe, kriptoanaliz uzmanları da kırmak için çalışır. İtalyan mucit G. Marconi, 1901'de telsiz sinyalini 3500 kilometre uzağa iletti. Askeri

haberleşmede kullanılan telsizin dinlenmemesi için elektronik şifreleme geliştirildi. Birinci Dünya Savaşı'nda Almanlar 1918'deki saldırıdan önce yeni bir şifre geliştirdi. Yeni şifreyi Fransızlar kırınca, Almanlar yenilgiye uğradı. Almanlar 1917'de bir telgrafla, ABD'ye karşı Meksika'ya işbirliği önerdi. Karşılığında Meksika'ya, Arizona ve Teksas verilecekti. İngilizler, telgrafı ele geçirdi ve şifresini kırıp ABD'yi uyardı. Tarafsız ABD savaşa katılınca Almanlar savaşı kaybetti. Şifre, bugün matematikçi ve bilgisayarcıların "Kriptografi" ve "Kriptoanaliz" adlı bilim alanlarıdır. Kriptografi kelimesi, Yunanca "kryptos" (gizli) ve "graphein" (yazı) kelimelerinden türedi. Kriptografi, okunabilir bilgiyi istenmeyen kişilerce okunamaz hale getiren teknoloji ve matematiksel yöntemlere denir. Kriptoanaliz, şifrelenmiş anlamsız görünen metinlerin anlamlı hale getirilmesi bilimidir.



Sekiz diskli bir ENIGMA

Almanlar'ın Şifresi Kırılamayan Makinesi: ENIGMA

Almanlar'ın ENIGMA şifreleme cihazı, 1926'da askeri birliklerde kullanıma girdi. Cihaz elektrikli bir daktiloya benzer ve 3-8 arasında değişen döner diskleri vardır. Örneğin "A" harfi için klavyedeki A'ya basınca ilk disk döner A'yı "K" harfine dönüştürür. Sonra ikinci disk döner ve K'yı "P" harfine dönüştürür. İşlem böyle sürer ve sonunda ışıklı harflerden örneğin "Y" yanardı. Mesajdaki "A" yerine şifreli metine "Y" yazılırdı. Karşı tarafta benzer makine ile Kod Kitabı vardı. Bunlarla şifreli metin orijinal mesaja çevrilirdi. Kod sürekli değiştiği için makineyi ele geçirmek, şifre kırmaya yetmiyordu. Polonyalı bilim adamları ilk ENIGMA'nın şifresini 1938'de kırdı. Almanlar da sisteme elektronik ünite ekleyip disk sayısını artırdı. İngiltere 1939'da, Fransa ve Polonya ile işbirliği yaptı. Bletchley Park adlı yerde yıllarca ENIGMA'nın

şifresi kırmaya çalıştı. Bu olayı anlatan ENIGMA adlı bir sinema filmi vardır. İnsan gücüyle şifre kırılamayınca, Polonya'nın desteğiyle elektronik makineler yapıldı ama yine kırılamadı. Kaçak bir Alman subay, Fransızlara ENIGMA'nın kod kitabını verdi. İngilizler de esir alınan Alman gemisinden ENIGMA makinesini ele geçirdi. Şifre çözülemedi, çünkü ne zaman hangi kodun kullanılacağı bilinmiyordu. Bir Alman gemisinde bir sonraki ayın kod listesi ele geçince şifre çözüldü. Zaten savaş sona ermek üzereydi.

Şifre, günlük hayatta yaptığımız iş ve işlemlerin güvenli ve kolay olmasını sağlıyor. Bu kötü niyetli şifre kırıcılar engellendiği sürece geçerli.

Prof. Dr. Ural Akbulut
ODTÜ Kimya Bölümü

(*) C. Çimen, S. Akleylek ve E. Akyıldız, ***Şifrelerin Matematiği. Kriptografi,*** ODTÜ Yayıncılık, 2008