1. GİRİŞ

Bilgi insanlar için her zaman kıymetli olmuştur. Tarih boyunca, Bilgi savaşları kazanmak, para kazanmak ve tarihi şekillendirmek için bir araç olmuştur. Geçmişte, kriptoloji bilgiyi yalnızca düşmandan gizlemek amacıyla kullanılmıştır. Günümüzde ise teknolojinin hayatımıza girmesiyle birlikte bilginin güvenliği çok daha önemli hale gelmiştir. Mesela; "para" ile aynı özellikleri taşıyan bit'ler nasıl oluşturulabilir?

Bu derste,

- Kriptografi, kriptoloji ve kripto sistem nedir?
- Geçmişte bilgiyi düşmandan gizlemek için kullanılan metotlar nelerdir? (Klasik kripto sistemler)
- Günümüzde modern kriptografi hangi konularla ilgilenir?
- Günümüzde bilgiyi gizlemek için kullanılan metotlar nelerdir? (Modern kripto sistemler)
- Matematiğin kriptografideki önemi nedir?

gibi sorulara cevap verilerek Kriptolojiye bir giriş yapılacaktır.

1.1. Kriptografi ve Kriptoloji nedir ?

Tarih boyunca insanlar birbirleriyle gizli haberleşme ihtiyacı duymuşlar ve bunun güvenilir yollarını aramışlardır. Yunancada gizli anlamına gelen *kripto*

ve yazılmış bir şey anlamına gelen *grafi* kelimelerinden oluşan **kriptografi** gizli yazışma sanatı anlamına gelmektedir.

Kriptografi bilimin çalışma disiplinine **Kriptoloji** denir. Kriptoloji konusunda çalışan kişiler bir yandan bilgiyi gizlemenin daha etkili yöntemlerini geliştirirken bir yandan da bu sistemlerin nasıl kırılabileceğini (**Kriptoanaliz**) düşünmek zorundadırlar. Dolayısıyla kriptoloji iki yönlü bir çalışma sahasıdır. Bu derste daha çok kripto sistemler tanıtılacaktır. Yani, kriptoanaliz sahasına detaylı olarak girilmeyecektir. Kriptografinin temel amacı telefon hattı veya bilgisayar ağı gibi güvenli olmayan bir kanal üzerinden iki kişinin (gönderici ve alıcı) bir başka şahsın söylenenleri anlayamayacağı şekilde iletişim kurmalarını sağlamaktır. Gönderici ileteceği anlaşılabilir mesaja bir kapama kuralı uygular ve anlaşılamayan bir mesaj elde eder. Gönderici kanal üzerinden bu anlaşılamayan mesajı alıcıya gönderir. Bir başka şahıs, kanal üzerinden elde edebileceği bu anlaşılamayan mesajdan orjinal mesajı (anlaşılabilir mesaj) elde edememelidir. Alıcı kendisine gelen anlaşılamayan mesaja bir açma kuralı uygulayarak orjinal mesajı elde eder.

İletişim teknolojisindeki gelişmeler günümüzde kriptografinin önemini daha da artırmıştır. Modern kriptografi mesajın istenmeyen kişiler tarafından **anlaşılamaması**, mesajın iletilmesi sırasında **değiştirilememesi**, mesajı gönderenin daha sonra mesajı kendisinin gönderdiğini **yalanlayamaması** ve mesajın **kimin tarafından** gönderildiğinin anlaşılabilmesi gibi konularla ilgilenir.

Günümüzde etkili kripto sistemler geliştirmek için matematiksel teknikler kullanılmaktadır. Sayılar teorisinin en önemli uygulama alanlarından biri kriptografi

alanıdır. Bu derste sayılar teorisinin yanı sıra eliptik eğri teorisine dayanan kripto sistemler tanıtılacak ve böylece modern kriptografide matematiğin önemi vurgulanarak kriptolojiye bir giriş yapılacaktır.

Kripto sistemlere geçmeden önce kullanacağımız bazı terimlerin tanımlarını verelim.

- Şifrelenmemiş (anlaşılabilir) mesaja **açık yazı** denir.
- Şifrelenmiş mesaja **kapalı yazı** denir.
- Açık yazı ve kapalı yazıyı oluşturmak için bir **alfabe** tanımlanması gerekir.

Alfabeyi $\sum$ sembolü ile göstereceğiz. Alfabe, doğal veya yapay bir dil olabilir. Mesela, eğer 26 harflik ingilizce alfabesini kullanacaksak $\sum$={A,B,C,...,Z} olur. Alfabenin eleman sayısınıda $|\sum|$ sembolü ile göstereceğiz. Örneğimizde $|\sum| = 26$ dır. Bu alfabede büyük harf küçük harf ayrımı olmamasına rağmen gösterim olarak açık yazı için küçük harfler, kapalı yazı için büyük harfler kullanacağız. Kullanacağımız alfabenin eleman sayısı sonlu olmalıdır. Açık yazı ile kapalı yazı için kullanılan alfabe aynı olmak zorunda değildir. Fakat genellikle aynı alfabe kullanılır. Alfabe büyük harf, küçük harf, boşluk, sayı, sembol vb. içerebilir.

- Açık yazıdan kapalı yazıyı elde etme kuralına **kapama fonksiyonu** denir.

Bu kuralın tersi, yani

- Kapalı yazıdan açık yazıyı elde etme kuralına **açma fonksiyonu** denir.

Kripto sistemler (şifreleme sistemleri) açık anahtarlı ve klasik (gizli) kripto sistemler olmak üzere ikiye ayrılır. Klasik kripto sistemlerde iletişim kuracak kişiler

önceden aralarında bir gizli anahtar üzerinde uzlaşırlar.Açık anahtarlı sistemlerde ise herkes, açık (herkesin bildiği) ve gizli (yalnızca kendisi bilir) olmak üzere iki anahtara sahiptir.

1.2. Klasik Kripto Sistem nedir ?

Klasik (Gizli anahtar) kripto sistem kavramını matematiksel notasyon kullanarak tanımlayalım.

Tanım 1.2.1 (Klasik kripto sistem)

$\mathcal{P}$, açık yazıların sonlu bir kümesi,

$\mathcal{C}$, kapalı yazıların sonlu bir kümesi,

$\mathcal{K}$ (Anahtar uzayı), olası anahtarların sonlu bir kümesi,

$\mathcal{E}$, kapama fonksiyonlarının sonlu bir kümesi,

$\mathcal{D}$, açma fonksiyonlarının sonlu bir kümesi olsun.

Eğer,

$\forall k \in \mathcal{K}$ için bir kapama fonksiyonu $e_k \in \mathcal{E}$ ve buna karşılık gelen açma fonksiyonu $d_k \in \mathcal{D}$ olmalıdır; öyleki,

$e_k : \mathcal{P} \longrightarrow \mathcal{C}$ ve $d_k : \mathcal{C} \longrightarrow \mathcal{P}$ fonksiyonları

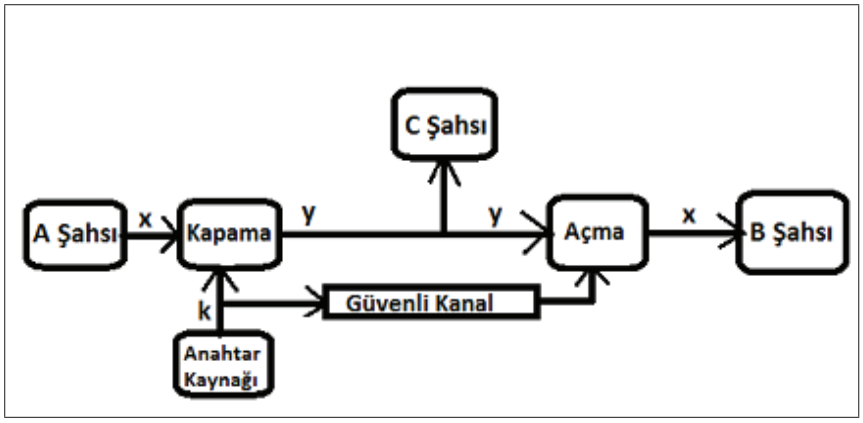
$$\forall x \in \mathcal{P} \quad \text{için} \quad d_k(e_k(x)) = x \tag{1.2.1}$$

özelliğini gerçekliyorsa $\left(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D} \right)$ beşlisine bir kripto sistem denir.

Not : $\forall x \in \mathcal{P}$ için $d_k(e_k(x)) = x$ özelliğinin sağlanması için e_k bire-bir fonksiyon olmalıdır.

Bir klasik kripto sistemin nasıl çalıştığını Şekil 1.2.1 den yararlanarak anlatalım :

İletişim kuracak olan A ve B şahısları belirli bir kripto sistemi kullanmak için aşağıdaki protokole uyarlar. İlk olarak güvenli bir kanal üzerinden rasgele bir $k \in \mathcal{K}$ belirlerler. Basit kripto sistemlerde güvenlik için kullanılan anahtarın sık sık değiştirilmesi gerekir.Bundan dolayı klasik kripto sistemlerde *anahtar yönetimi* sorunu vardır. Klasik kripto sistemlerde kapama ve açma fonksiyonları için aynı gizli anahtar, k, kullanılır. Bu yüzden gizli anahtar kripto sistem *simetrik kripto sistem* olarak da adlandırılır.



Şekil 1.2.1

Kabul edelim ki açık yazı, $n \geq 1, n \in \mathbb{Z}, x_i \in \mathcal{P}$ olmak üzere $x = x_1x_2x_3...x_n$ olsun. Önceden belirlenmiş $k \in \mathcal{K}$ anahtarı ile tanımlanan e_k kapama fonksiyonunu kullanarak herbir x_i şifrelenir. A şahsı $1 \leq i \leq n$ için $y_i = e_k(x_i)$ leri hesaplayarak $y = y_1y_2...y_n$ kapalı yazısını kanal üzerinden B şahsına gönderir. B şahsı d_k açma fonksiyonunu kullanarak y kapalı yazısından $x = x_1x_2...x_n$ açık yazısını elde eder.