4. AÇIK ANAHTAR KRİPTOGRAFYA

4.1. Açık Anahtar Kripto Sistemlere Giriş

Şimdiye kadar gördüğümüz kripto sistemlerde gönderici ve alıcı tarafından e_k kapama fonksiyonu için bir k anahtarı seçilerek buna karşılık bir d_k kapama fonksiyonu belirleniyordu. İki işlem içinde aynı anahtar kullanıldığından gönderici ve alıcının anahtar alışverişinde bir başka şahsın anahtarı elde etmemesi için büyük özen göstermeleri gerekir. Klasik kripto sistemlerde anahtar yönetimi en önemli sorunlardan biridir. Örneğin, telefon hattı veya e-mektup gibi güvenli olmayan kanallardan anahtar alışverişi yapmak mümkün değildir. Kurye ile anahtar alışverişi güvenli bir yoldur fakat zaman alabilir. Askeri ve diplomatik iletişimlerde kuryelerin kullanılması mümkündür, fakat bu yol hem çok pahalı hemde pratik değildir. Günümüzde bilgisayarların bir çok alanda olduğu gibi iletişim alanında da etkili bir şekilde kullanılması askeri ve diplomatik haberleşmenin yanı sıra bankacılık, ticari vb. gibi iletişimler için de güvenli haberleşme ihtiyacı doğurmuştur ve buralarda kurye sisteminin kullanılma olasılığı yoktur. Klasik kripto sistemlerde buna ek anahtar yönetimi sorunları da vardır. Network üzerinden bir grup insanın birbiriyle güvenli bir iletişim yapmak istediklerini düşünelim. Gruptaki her insan çifti için farklı bir anahtar belirlenmelidir. Örnek olarak, grupta 10 kullanıcının olduğunu düşünürsek, $\binom{10}{2} = 45$ farklı anahtara ihtiyacımız var. Eğer grupta 100 kullanıcı varsa, $\binom{100}{2} = 4950$ anahtara ihtiyacımız var. Anahtarların büyük sayıda olması ayrı bir güvenlik sorunu daha oluşturur.

Klasik kripto sistemlerde bir başka sorun karşılıklı güvendir. İki kullanıcı da aynı anahtarı kullandığından bir güven sorunu olur. Kabul edelim ki A ve B şahısları aynı gizli anahtarı paylaşsınlar. Eğer C şahsı gizli anahtarı elde ederse, B şahsıymış gibi A şahsına mesaj gönderebilir. A şahsının bu mesajın B şahsından gelmediğini bilme şansı yoktur. Üstelik C şahsı , A şahsından B şahsına giden bir mesajı yakalayıp değiştirme imkanına da sahiptir. Bu durumda B şahsı mesajın değiştirildiğinin farkına varamaz. Klasik kripto sistemlerde B şahsının gönderdiği bir mesajı anahtarın çalındığını öne sürerek yalanlama imkanıda vardır. Ticari durumlarda bunlar çok önemlidir. Bir banka müşterisi yaptığı bir işlemi yalanlayamazken, müşteri de bankanın kendisi yerine bir işlem yapmadığından emin olabilmelidir.

Sonuç olarak, bir kripto sistemin kripto analiz olarak güvenli olmasının yanında aşağıdaki hususları da dikkate almamız gerekir.

(1) *Anahtar yönetimi* : Haberleşecek taraflar arasında anahtar alışverişi

(2) *Kimlik Doğrulama* : Mesajı alan kişinin mesajın kimden geldiğini belirleyebilmesi

(3) *Bütünlük* : Mesajı alan kişi mesajın kanal üzerinde değiştirilip değişti-rilmediğini belirlemesi

(4) *Reddetme* : Mesajı gönderen kişinin gönderdiği mesajı kendisinin göndermediğini iddia etmesi

Bu ihtiyaçları klasik kripto sistemlerle karşılamanın imkanı yoktur. Diffie ve Hellman (1976) tarafından bulunan anahtar alış-verişi anahtar sevkiyatı sorununu çözmüştür. Bu yöntem açık anahtar kripto sistemlerin doğmasına neden olmuştur. Anahtar alış verişine gerek duymaksızın oluşturulan kapama fonksiyonu (E) tek yönlü ve açma fonksiyonu (D) trapdoor fonksiyonu olan kripto sistemlere açık anahtar kripto sistem diyebiliriz. Bunu biraz daha açıklayalım :

İletişim kuracak kişiler kapama (E) fonksiyonlarını ilan ederken, açma (D) fonksiyonlarını gizli tutarlar. Dolayısıyla her kişi, E kapama fonksiyonunu belirleyen ve herkes tarafından bilinen bir kapama anahtarı ile birlikte D açma fonksiyonunu belirleyen gizli bir açma anahtarı olmak üzere iki anahtara sahiptir. Bu da network iletişiminde anahtar sayısını büyük ölçüde azaltır. Örneğin, klasik kripto sistemi kullanarak 10 kişilik bir network iletişiminde $\binom{10}{2} = 45$ anahtar kullanılırken, açık anahtar kriptosistemde $10 \times 2 = 20$ tane anahtar kullanılmış olur.

A şahsına açık yazı göndermek isteyen herhangi biri, bu şahsın ilan ettiği kapama anahtarını kullanarak açık yazıyıdan kapalı yazıyı elde edip kanal üzerinden gönderir. A şahsı gizli tuttuğu açma anahtarını kullanarak kendisine gelen kapalı yazıdan açık yazıyı elde eder.

Açık anahtar kripto sistemlerde kapama anahtarı dolayısıyla kapama metodunun bilinmesi açmaya imkan sağlamamalıdır.

Not : Kapama ve açmanın doğru çalışması için herhangi bir x açık yazısı için $D(E(x)) = x$ şartı sağlanmalıdır.

Kapama fonksiyonu herkes tarafından bilineceğinden herhangi biri istediği kadar kapalı yazı elde edebilir. Yani, böyle bir sistem kapalı yazı ve karşılık gelen açık yazı bilinerek yapılan ataklara karşı dayanıklı olmalıdır. Aynı zamanda pratik kullanım için kapama ve açma fonksiyonları hızlı bir şekilde hesaplanabilmelidir. Güvenlik açısından, herhangi birisi için E kapama fonksiyonundan D açma fonksi-yonunu hesaplaması mümkün olmamalıdır.

Teorik olarak, bir açık anahtar kripto sistem tek yönlü fonksiyonunun özel bir durumu olan trapdoor tek yönlü fonksiyonu kullanılarak oluşturulabilir.

Tanım 4.1.1. (Tek yönlü fonksiyon)

$f : X \to Y$ bire-bir fonksiyon olsun. Eğer, f fonksiyonu aşağıdaki özellikleri gerçekliyorsa f ye tek yönlü (one way) fonksiyon denir.

(1) $\forall x \in X$ için $f(x)$ i hesaplamak kolay (Bilgisayar kullanarak bir algoritma ile makul bir zamanda hesaplanabilir)

(2) $y = f(x)$ olmak üzere, y verildiğinde x i hesaplamak zor (Bilgisayar kullanarak bilinen algoritmalarla makul bir zamanda hesaplamak imkansız).

Tanım 4.1.2. (Trapdoor tek yönlü fonksiyon)

$f : X \to Y$ bir tek yönlü fonksiyon olsun.

Ek bir bilgi (trapdoor) kullanılarak, $y = f(x)$ olmak üzere y verildiğinde x i hesaplamak kolay oluyorsa f fonksiyonuna trapdoor tek yönlü fonksiyon denir.

Tanım 4.1.1. de geçen kolay ve zor kavramlarının aksiyomatik tanımı olmadığından herhangi bir fonksiyonun tek yönlü bir fonksiyon olduğunun ispatlanması mümkün değildir.

Örnek 4.1.1.

p ve q asal sayılar olmak üzere $f(p, q) = pq = N$ fonksiyonunu düşünelim. p ve q verildiğinde $N = f(p, q)$ değerini hesaplamak kolaydır. Fakat eğer p ve q asallarını yeterince büyük seçersek bilinen metodlarla N bilinirken p ve q yu makul bir sürede hesaplanamaz. Yani, p ve q asalları uygun seçilirse f^{-1} i hesaplamak oldukça zor bir problemdir. Bu fonksiyonun tek yönlü fonksiyon olduğu düşünülmektedir.

Kapama ve açma fonksiyonları için tek yönlü fonksiyonların doğrudan doğruya kullanılması uygun değildir. Kapama ve açma fonksiyonlarını tanımlamak için tek yönlü fonksiyonların özel durumu olan trapdoor tek yönlü fonksiyonları kullanacağız. Mesela $N = pq$ bilinirken, ek bilgi olarak $\phi(N)$ de biliniyorsa p ve q asalları bulunabilir. Bu ek bilgiye trapdoor denir. Eğer Kriptografide tek yönlü trapdoor fonksiyonları kullanılırsa; E kapama fonksiyonundan D açma fonksiyonunu elde etmek için trapdoor'a ihtiyacımız vardır.

Tanım 4.1.3. p asal sayı olmak üzere, $(\mathbb{Z}_p^*, *)$ devirli çarpımsal bir gruptur. a, $\mathbb{Z}_p$ nin bir primitif elemanı olsun (Bölüm 3).

$$a^x \equiv b \,(\mathrm{mod}\, p)$$

kongürüansında a , b ve p bilinirken $0 \leqslant x \leqslant p-2$ olacak şekildeki x tamsayısını bulma problemine $\mathbb{Z}_p$ deki diskrete logaritma problemi denir ve DLP ile gösterilir.

DLP yi çözmenin bir yolu $0 \leqslant x \leqslant p-2$ olacak şekilde $\forall x$ için $a^x \,(\mathrm{mod}\, p)$ değerlerini hesaplayıp tablo haline getirmektir. Fakat, eğer p asalı büyük seçilirse (Bölüm 3) bu yolla DLP yi makul zamanda çözmek mümkün değildir. DLP yi çözmek için başka algoritmalarda mevcuttur. PSH (Pohlip-Silver-Hellman) algoritması eğer $p-1$ küçük asal bölenlere sahipse DLP problemini makul bir zamanda çözebilmektedir.

Genel olarak, eğer p asalı dikkatli seçilirse DLP nin zor olduğu kabul edilir. DLP için polinom zamanlı genel bir algoritma mevcut değildir. Bilinen atakları engellemek için p asalı en az 150 basamaklı olmalıdır ve $p-1$ büyük bir asal bölene sahip olmalıdır. DLP nin zor olmasına karşılık, a, x ve p bilinirken b tamsayısı makul bir zamanda mod m de üs alma (Bölüm 3) algoritması ile hesaplanabilir. Yani, uygun asallar için $\mathrm{mod}\, p$ de üs alma tek yönlü bir fonksiyon olduğundan kriptografik amaçla kullanılabilir.

4.2. Anahtar Alış-Verişi (Key-Exchange)

Klasik kripto sistemlerdeki anahtar alış verişi sorunundan bahsetmiştik. Bu sorunun üstesinden gelmek için Diffie ve Hellman aşağıdaki anahtar alış-verişi protokolünü önermişlerdir:

A ve B şahıslarının gizli bir anahtar belirlemek istediklerini düşünelim. A ve B şahısları bir p asalı ve $\mathbb{Z}_p$ de bir g primitif elemanı belirlesinler. $\mathbb{Z}_p^*$ devirli çarpımsal bir grup olduğundan $g \in \mathbb{Z}_p^*$ vardır (Bölüm 3). $\mathbb{Z}_p$ ve g herkes tarafından bilinebilir. Anahtar alış-verişi protokolü aşağıdaki gibidir.

(1) A şahsı, $0 < a < p-2$ olacak şekilde rasgele bir a sayısı seçer, sonra $u = g^a \pmod p$ ifadesini hesaplar ve B şahsına gönderir.

(2) B şahsı, $0 < b < p-2$ rasgele bir b sayısı seçer, sonra $v = g^b \pmod p$ ifadesini hesaplar ve A şahsına gönderir.

(3) B şahsı $u^b \pmod p$ ifadesini hesaplar.

(4) A şahsı $v^a \pmod p$ ifadesini hesaplar.

$$u^b \equiv (g^a)^b \equiv g^{ab} \pmod p$$
$$v^a \equiv (g^b)^a \equiv g^{ab} \pmod p$$

k sayısını $k := g^{ab} \pmod p$ olarak tanımlayalım.

Dolayısıyla, $u^b \pmod p = k = v^a \pmod p$ olduğundan A ve B şahsı aynı k anahtarını seçmiş oldular. a veya b sayıları hesaplanabilirse k anahtarı bulunabilir. Fakat, u, v, p ve g sayıları bilinirken a veya b sayılarını hesaplamaya çalışma bir DLP dir. a ve b sayılarını bilmeden, makul bir zamanda k anahtarını hesaplayabilen bir algoritma mevcut değildir.