4.3. RSA Kripto Sistemi

RSA en eski ve en ünlü açık anahtar kripto sistemlerinden biridir. Rivest, Shamir ve Adleman tarafından 1978 yılında bulunmuştur. Kapama fonksiyonu olarak trapdoor tek yönlü fonksiyonu kullanılır. RSA kripto sisteminin güvenliği "Asal çarpanlara ayırma" problemine dayanır. Bu problem modern bilgisayar teknolojisine rağmen bilinen algoritmalarla makul bir zamanda çözülememektedir.

Anahtar alış verişine gerek duymaksızın A şahsının B şahsına açık yazısını göndermek istediğini düşünelim. Bunun için B şahsı sırasıyla aşağıdaki işlemleri yapar.

1. Herhangi iki tane büyük ve farklı p ve q asallarını seçerek $N := pq$ sayısını hesaplar (p ve q asalları Ek-1 de verilen asallık testi kullanılarak üretilebilir).

2. $Ebob(e, \phi(N)) = 1$ ve $1 < e < \phi(N)$ olacak şekilde bir e sayısı seçer.

3. $de \equiv 1 \pmod{\phi(N)}$ şartını sağlayan d sayısını belirler.

4. p, q ve d sayılarını gizli tutarken N ve e sayılarının herkes tarafından bilinmesine müsade eder.

Bu durumda, A şahsı göndermek istediği x ($0 < x < N$) açık yazısından

$$y := x^e \pmod{N} \tag{4.3.1.}$$

ifadesini kullanarak y kapalı yazısını hesaplar ve B şahsına gönderir.

y kapalı yazısını alan B şahsı

(4.3.2.) $$x = y^d \pmod N$$

ifadesinden x açık yazısını elde etmiş olur.

4.3.1. numaralı eşitlikte y, e ve N bilinirken x in bulunmasının diskrete logaritma problemi olduğuna dikkat edelim.

Şimdi 4.3.2. eşitliğinin sağlandığını gösterelim :

$$ed \equiv 1 \pmod{\phi(N)}$$

olduğundan

(4.3.3.) $ed = t\phi(N) + 1$ ve $t \geqslant 1$olacak şekilde $t \in \mathbb{Z}$ vardır.

1. Durum : $ebob(x, N) = 1$ olsun.

Euler teoreminden (Bölüm 3)

$$x^{\phi(N)} \equiv 1 \pmod N \quad \text{dir.}$$

Euler teoremini kullanarak

$$\begin{aligned} y^d \equiv (x^e)^d &\equiv x^{t\phi(N)+1} \pmod N \\ &\equiv (x^{\phi(N)})^t x \pmod N \\ &\equiv 1^t x \pmod N \\ &\equiv x \pmod N \qquad \text{dir.} \end{aligned}$$

2. Durum : $ebob(x, N) \neq 1$ olsun.

$ebob(x, N) \neq 1$ ve $x < N$ olduğundan x, p ve q asallarından sadece biri ile bölünür. Kabul edelim ki $p \mid x$ olsun (Diğer durumda da tamamen aynıdır). Bu durumda $x \equiv 0 \pmod{p}$ olduğundan

(4.3.4.) $$x^{ed} \equiv x \pmod{p}$$

4.3.3 eşitliğini kulanırsak

$$ed - 1 = t\phi(n) = t(p-1)(q-1) \Longrightarrow q - 1 \mid ed - 1 \quad \text{dir.}$$

Euler teoreminden $x^{q-1} \equiv 1 \pmod{q}$ ve $q - 1 \mid ed - 1$ olduğundan

(4.3.5.) $$x^{ed} \equiv x \pmod{q}$$

dir.

4.3.4 ve 4.3.5 den dolayı $x^{ed} \equiv x \pmod{N}$dir. Böylece istenen sonucu bulmuş oluruz.

Şimdi, RSA kripto sisteminin matematiksel tanımını yapalım.

RSA Kripto sistem :

p ve q farklı iki asal olmak üzere $N := pq$ olsun. $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$,

$\mathcal{K} : \{(N, p, q, e, d) : \ p$ ve q farklı asallar , $N = \ pq$ ve $ed \equiv 1 \pmod{\phi(N)}\}$.

$k = (N, p, q, e, d)$ için kapama ve açma fonksiyonlarını tanımlayalım:

$$E_k(x) := x^e \pmod{N} \quad \text{ve} \quad D_k(y) := y^d \pmod{N} \quad (x, y \in \mathbb{Z}_N).$$

N ve e ilan edilirken; p,q ve d gizli tutulur.

Not: Kapama ve açma fonksiyonları Mod m de üs alma kullanılarak makul bir sürede hesaplanabilir (Bölüm 3).

Örnek 4.3.1.

Kabul edelim ki B şahsı $p = 101$ ve $q = 113$ asallarını seçmiş olsun. $N = pq = 11413$ ve $\phi(N) = (p-1)(q-1) = 100 * 112 = 11200$ olur. $11200 = 2^6 5^2 7$ olduğundan e sayısı 2,5 ve 7 ile bölünmeyen bir sayı olabilir (Pratikte B şahsı $\phi(N)$ i çarpanlarına ayıramamalı, $ebob(\phi(N), e) = 1$ olduğunu bölme algoritmasını kullanarak doğrulamalıdır). Kabul edelim ki B şahsı e sayısını $e = 3533$ olarak seçsin. Bölme algoritmasını kullanarak (Bölüm 3) :

$$d \equiv e^{-1} \equiv 6597 \pmod{11200}.$$

Yani, B şahsının açma anahtarı $d = 6597$ dir.

B şahsı $N = 11413$ ve $e = 3533$ sayılarını ilan eder. A şahsı $x = 9726$ açık yazısını B şahsına göndermek istesin. A şahsı

$$9726^{3533} \pmod{11413} \equiv 5761$$

ifadesini hesaplar ve $y = 5761$ kapalı yazısını kanal üzerinden B şahsına gönderir.

B şahsı $y = 5761$ kapalı yazısını alınca açık yazıyı elde etmek için kendi açma anahtarı d yi kullanır:

$$5761^{6597} \pmod{11413} \equiv 9726.$$

Böylece açık yazıyı elde etmiş olur.

RSA kripto sisteminin güvenliği $E_k(x) = x^e \pmod N$ kapama fonksiyonunun tek yönlü fonksiyon olmasına dayanır. Yani kapalı yazıyıdan açık yazı bilinen algoritmalarla makul bir zamanda elde edilemez. B şahsı $N = pq$ olacak şekilde p ve q asallarını bildiğinden (trapdoor), $\phi(N) = (p-1)(q-1)$ ifadesini hesaplayabilir ve sonra bölme algoritmasını (Bölüm 3) kullanarak d açma anahtarını bulabilir; böylece kapalı yazıdan açık yazıyı elde eder.

RSA kripto sisteminde p ve q asalları seçilirken birbirlerine çok yakın seçilmemelidir. Örnek olarak, 179 ve 181 asalları için $N = 32399$ olur. Böylece p ve q asalları $\sqrt{N}$ ye çok yakın sayılardır ve kolaylıkla bulunabilirler. Ayrıca; Mersenne asalları 2^{n-1}, Fermat asalları 2^{n+1}, seçilmemelidir. Çünkü bu tip asallar açık formülü olduğundan kolayca denenebilir.

4.4. ElGamal Kripto Sistemi

$\mathbb{Z}_p$ deki ElGamal kripto sistemi (ElGamal 1985).

$\mathbb{Z}_p$ deki DLP zor olacak şekilde bir p asalı seçilir. α, $(\mathbb{Z}_p^*, *)$ devirli çarpımsal grubun primitif elemanı olsun.

$\mathcal{P} := \mathbb{Z}_p^*$, $\mathcal{C} := \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, $\mathcal{K} := \{(p, \alpha, a, \beta) : \beta = \alpha^a \pmod p\}$

öyle ki p, α ve β herkes tarafından bilinirken a gizli tutuluyor.

$K = (p, \alpha, a, \beta)$ ve rasgele seçilen $k \in \mathbb{Z}_{p-1}$ sayısı için kapama fonksiyonu (k gizli),

$$y_1 := \alpha^k \pmod p \qquad \text{ve} \qquad y_2 := x\beta^k \pmod p \quad \text{olmak üzere}$$

$$e_K(x, k) := (y_1, y_2) \qquad \text{dir.}$$

$y_1, y_2 \in \mathbb{Z}_p^*$ için açma fonksiyonu,

$$d_K(y_1, y_2) := y_2(y_1^a)^{-1} \pmod p \quad \text{dir.}$$

B şahsının bir a sayısı seçip, gizli tuttuğunu düşünelim.

A şahsı, B şahsına bir x açık yazısını göndermek istesin,

A şahsı, rasgele bir k sayısı seçer ve $e_K(x, k) = (y_1, y_2)$ ifadesini hesaplayıp, B şahsına gönderir. Kapalı yazı x açık yazısına ve rasgele seçilen k sayısına bağlı olduğundan, aynı açık yazı k sayısına bağlı olarak bir çok sayıda kapalı yazı olarak kapatılabilir.

B şahsı kendisine gelen kapalı yazıyı açmak için açma fonksiyonunu kullanarak

,

$$\begin{aligned} d_K(y_1, y_2) &= y_2(y_1^a)^{-1} \pmod p \\ &= x\beta^k((\alpha^k)^a)^{-1} \pmod p \\ &= x\alpha^{ak}\alpha^{-ak} \pmod p \\ &= x \pmod p \end{aligned}$$

x açık yazısını elde eder. B şahsı, a sayısını gizli tuttuğundan x açık yazısını sadece kendisi hesaplayabilir. $\beta \equiv \alpha^a \pmod p$ kongürüansından a sayısını hesaplamak bir diskret logaritma problemidir. Yani, ElGamal kripto sistemin güvenliği DLP ye dayanır. a sayısını hesaplamadan $y_1^a \equiv \alpha^{ka} \pmod p$ hesaplanabilirse ElGamal kripto sistemi kırılabilir fakat $\alpha^k \pmod p$ ve $\alpha^a \pmod p$ bilinirken $\alpha^{ka} \pmod p$ ifadesini makul bir zamanda hesaplayan bir yöntem bilinmemektedir.

Örnek 4.4.1.

$p = 2579$, $\alpha = 2$ olsun. B şahsı, $a = 765$ sayısını seçmiş ise

$$\begin{aligned} \beta &\equiv 2^{765} \pmod{2579} \\ &= 949 \end{aligned}$$

dir.

p, α ve β sayıları herkes tarafından bilinirken, a sayısı yalnızca B tarafından bilinir.

A şahsı, $x = 1299$ açık yazısını B şahsına göndermek için

(1) Rasgele bir k sayısı seçer. $k = 853$ sayısını seçmiş olsun.

(2) Kapama fonksiyonunu kullanarak,

$$\begin{aligned} y_1 &\equiv 2^{853} \pmod{2579} \\ &= 435 \\ y_2 &\equiv 1299 \times 949^{853} \pmod{2579} \\ &= 2396 \end{aligned}$$

$y = (y_1, y_2) = (435, 2396)$ kapalı yazısını hesaplar ve B şahsına gönderir.

B şahsı, kendisine gelen y kapalı yazısına açma fonksiyonunu uygular,

$$\begin{aligned} x &\equiv 2396 \times (435^{765})^{-1} \pmod{2579} \\ &= 1299 \end{aligned}$$

açık yazısını elde eder.

Şimdiye kadar gördüğümüz örneklerde mesajı alan kişi mesajın kimden geldiğini belirleyemez. Şimdi, bu sorunun üstesinden gelen dijital imzayı inceleyelim.