BÖLÜM 7

AÇIK ANAHTARLI SİSTEMLER

Farzedin ki siz e-mail yoluyla başka bir kişiyle haberleşmek istiyorsunuz ve mesajlarınızın şifreli olmasını istiyorsunuz. Örnek vermek gerekirse, düşünün ki şifreleme metodunuz üç harf anahtarlı Vigenere olsun. 26 sayı sistemi taban alındığında, bu anahtar 0 ile $26^2 = 676$; 2 lik sistemde 0 ile 1010100100 arasındadır. Sizinle haberleştiğiniz kişi arasındaki bilgisayar ağı, internet ve fiber optik kanallar güvenli olmadığı için, siz anahtarlarınızı e-mail yoluyla değiştirmek istemezsiniz. 2 lik anahtarlarınızı açık kanal üzerinden güvenli bir şekilde değiştirme yolları vardır. Algoritma ve karmaşıklık teorisinde uzmanlar belirli matematik problemlerin çözümü için aşırı zaman gerektiğine inanıyorlar. Açık anahtarlı kriptosistemler de bu mantığa göre geliştirilmiştir ; öyle ki bu kriptosistemlerin birini kırmak bu zor matematik problemleri çözmekle eşdeğerdir.Çok hızlı bilgisayarlar da programlanmış olan çözüm metodları bile haftalar, aylar, yüzyıllar hatta evrenin sonuna kadar olan hayatı bile kapsayabilir.

7.1 MERKLE-HELLMAN KNAPSACK KRİPTOSİSTEM

Knapsack açık anahtarlı şifreleme sistemleri alt küme toplama problemleri temeline dayanır. Buradaki temel düşünce, çözümü kolay olan bir alt küme toplam problemi örneğini seçip, onu çözümü zor olan bir alt küme toplama problemi örneğine çevirerek

gizlemektir. İlk(orjinal) knapsack kümesi gizli anahtarı, dönüştürülmüş(gizlenmiş) knapsack kümesi de kapalı anahtarı oluşturur.

Merkle-Helman açık anahtarlı şifreleme şeması, süperartan alt küme toplama problemi olarak da adlandırılan kolayca çözülebilen bir alt küme toplama problemi örneğini modüler çarpım ve permütasyon yoluyla gizleme girişimidir.

7.1.1 Süperartan dizi (Superincreasing sequence)

$B = (b_1, b_2, \cdots, b_n)$ dizisinde eğer her sayı kendisinden önce gelen sayıların toplamından büyük ise ,yani

$$b_i = \sum_{j=1}^{i-1} b_j \text{ öyleki } 2 \leq i \leq n,$$

bu diziye süperartan dizi denir.

7.1.2 Süperartan Altküme Toplama Problemini çözme Algoritması

GİRDİ: $(b_1, b_2, \cdots, b_n)$ şeklinde olan süperartan bir dizi ve $b_i$lerin altkümesinin toplamını ifade eden s tamsayısı algoritmamızın girdileri olsun.

ÇIKTI: Elemanları $x_i \in \{0, 1\}$ olan ve $\sum_{i=n}^{n} x_i b_i = s$ koşulunu sağlayan $(x_1, x_2, \cdots, x_n)$ dizi aşağıdaki şekilde hesaplanır:

1. $i \leftarrow n$.
2. $i \geq 1$ ise aşağıdakiler yapılır:

- Eğer $s \geq b_i$, $x_i = 1$ yazılır ve $s \leftarrow s - b_i$ uygulanır. Aksi taktirde $x_i = 0$ yazılır.
- $i \leftarrow i - 1$ işlemi $i = 1$ olana kadar sürer.

3. Bulunan x_i ler $(x_1, x_2, \cdots, x_n)$ dizisini oluşturur.

7.1.3 Merkle-HellmanKnapsack Şifrelemesinde Anahtar Oluşturma Algoritması

Bu kriptosistemde her kişi kendi açık anahtarını ve buna bağlı gizli anahtarını şu şekilde oluşturur:

1. Sistem parametresi olarak sabit bir n tamsayısı alınır.
2. Her A kişisi aşağıdaki $3 - 7$. adımları uygular.
3. Bir tane süperartan $(b_1, b_2, \cdots, b_n)$ dizisi ve $M > b_1 + b_2 + \cdots + b_n$ şartını sağlayan bir M mod sayısı seçer.
4. $1 \leq W \leq M - 1$ ve $gcd(W, M) = 1$ koşullarını sağlayan rastgele bir W tamsayısı seçer.
5. $\{1, 2, \cdots, n\}$ tamsayılarıyla ifade edilen rastgele bir π permütasyonu seçer.
6. $i = 1, 2, \cdots, n$ değerleri için $a_i = W b_{\pi i} \, mod \, M$ ifadelerini hesaplar.
7. A'nın açık anahtarı $(a_1, a_2, \cdots, a_n)$; A'nın kapalı anahtarı ise $(\pi, M, W, (b_1, b_2, \cdots, b_n))$ olur.

7.1.4 Basit Merkle-Hellman Knapsack Açık Anahtar Şifreleme Algoritması

B şahsı A için m mesajını şifreliyor olsun.

1. **Şifreleme**: B, şunları yapar:
   - A'nın açık anahtarı $(a_1, a_2, \cdots, a_n)$ i alır.
   - m mesajını n uzunluğundaki 2 lik dizi,$m = m_1 m_2 \cdots m_n$, olarak ifade eder
   - Daha sonra $c = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n$ değerini hesaplar.
   - Oluşan kapalı metni A'ya gönderir.
2. **Deşifreleme**: c kapalı metnine karşılık gelen m açık metnini çözmek için A şunları yapar:
   - Öncelikle $d = W^{-1} c \, mod \, M$ değerini hesaplar.
   - Süperartan altküme toplam problemini çözerek, $d = r_1 b_1 + r_2 b_2 + \cdots + r_n b_n$ eşitliğini sağlayan $r_1, r_2, \cdots, r_n$ $r_i \in \{0, 1\}$ tamsayılarını bulur.
   - Mesaj bitleri $m_i = r_{\pi(i)}$, $i = 1, 2, \cdots, n$ dir.

Örnek 7.1.1 ***Anahtar Oluşturma:*** *$n = 6$ olsun. A şahsı $(12, 17, 33, 74, 157, 316)$ süperartan bir dizi ve $M = 737 > 12 + 17 + 33 + 74 + 157 + 316 = 609$ tamsayısı seçer. Daha sonra $gcd(W = 635, M = 737) = 1$ koşulunu sağlayan bir $W = 635$ sayısını seçer. Son olarakta $\{1, 2, \cdots, 6\}$ sayılarından oluşup $\pi(1) = 3$, $\pi(2) = 6$, $\pi(3) = 1$, $\pi(4) = 2$, $\pi(5) = 5$, $\pi(6) = 4$ leri sağlayan bir π permütasyonunu alır. A açık anahtarını*

$a_i = Wb_{\pi i} \, mod \, M$ *eşitliğini kullanarak şu şekilde oluşturur:*

$$\begin{aligned}
a_1 &= Wb_{\pi(1)} = Wb_3 = 635 \cdot 33 \, mod \, 737 &&\equiv 319 \\
a_2 &= Wb_{\pi(2)} = Wb_6 = 635 \cdot 316 \, mod \, 737 &&\equiv 196 \\
a_3 &= Wb_{\pi(3)} = Wb_1 = 635 \cdot 12 \, mod \, 737 &&\equiv 250 \\
a_4 &= Wb_{\pi(4)} = Wb_2 = 635 \cdot 17 \, mod \, 737 &&\equiv 477 \\
a_5 &= Wb_{\pi(5)} = Wb_5 = 635 \cdot 157 \, mod \, 737 &&\equiv 200 \\
a_6 &= Wb_{\pi(6)} = Wb_4 = 635 \cdot 74 \, mod \, 737 &&\equiv 559
\end{aligned}$$

Böylece A'nın açık anahtarı $(319, 196, 250, 477, 200, 559)$ *knapsack dizisidir. A'nın gizli anahtarı ise* $(\pi, M, W, (12, 17, 33, 74, 157, 316))$ *dır.*

Şifreleme: *B,* $m = 101101$ *mesajını şöyle şifreler:*

$$\begin{aligned}
c &= 1 \cdot 319 + 0 \cdot 196 + 1 \cdot 250 + 1 \cdot 477 + 0 \cdot 200 + 1 \cdot 559 \\
&= 319 + 250 + 477 + 559 = 1605
\end{aligned}$$

ve bunu A'ya gönderir.

Deşifreleme: *Mesajı çözmek için A,* $d = W^{-1}c \, mod \, M$ *değerini hesaplar ve süperartan altküme toplama problemini çözer. Öncelikle* $W^{-1} = 635^{-1} \equiv 513 \, mod \, 737$*, ikinci olarak* $d = W^{-1}c = 513 \cdot 1605 \equiv 136 \, mod \, 737$ *değerlerini bulur.*

$$\begin{aligned}
136 &= 12 \cdot r_1 + 17 \cdot r_2 + 33 \cdot r_3 + 74 \cdot r_4 + 157 \cdot r_5 + 316 \cdot r_6 \\
&= 12 + 17 + 33 + 74
\end{aligned}$$

Böylelikle $r_1 = 1$*,* $r_2 = 1$*,* $r_3 = 1$*,* $r_4 = 1$*,* $r_5 = 0$*,* $r_6 = 0$ *ve* π *nin permütasyonunun uygulanmasıyla mesaj bitleri* $m_1 = r_3 = 1$*,* $m_2 = r_6 = 0$*,* $m_3 = r_1 = 1$*,* $m_4 = r_2 = 1$*,* $m_5 = r_5 = 0$*,* $m_6 = r_4 = 1$ *bulunur.*

7.2 RSA Kriptosistem

RSA kriptosistem, 1978 yılında " Dijital imza elde etme metodu ve açık anahtarlı kriptosistemler" adlı bir makale ile yayınlandı. Adını yaratıcılarının (Ronald Rivest,Adi Shamir, Leonard Adleman) soyadlarının başharflerinden alan RSA kriptosistem, göndericinin bir metodla ve herkesçe bilinen açık bir anahtarla mesajlarını şifrelediği bir şifre sistemi olarak tanımlanır. Daha önceki gizli(simetrik) anahtarlı sistemlerin tersine anahtarı bilmek deşifre anahtarını ortaya çıkarmaz. Bu sistem hem gizlilik hem de dijital imza sağlamak amaçlı kullanılabilir. Bu sistemin güvenliği tamsayılarda çarpanlara ayırma probleminin kolaylıkla olmaması temeline dayanır.

RSA kriptosisteminde kişilere şifreli mesaj gönderilebilmesi için o kişilerin açık anahtarlarına ihtiyaç vardır. Mesajı alan kişinin de mesajı okuyabilmesi için gizli bir anahtarının olması gerekir.Anahtar oluşturma aşğıdaki algoritmada ifade edilmiştir.

Anahtar Oluşturma algoritması: Her A kişisi anahtarını şu şekilde oluşturur:

- İki tane farklı,rasgele ve yaklaşık aynı uzunlukta olan p ve q asal sayıları seçer.
- $n = pq$ ve $\phi = (p-1)(q-1)$ değerlerini hesaplar.
- $1 < e < \phi$ ve $gcd\,(e, \phi) = 1$ olacak şekilde rastgele bir e sayısı seçer.
- Öklid algoritmasını kullanarak, $1 < d < \phi$ ve $ed \equiv 1\,(mod\,\phi)$ koşulunu sağlayan d sayısını hesaplar.
- A'nın açık anahtarı (n, e); A'nın gizli anahtarı ise d olur.

RSA anahtar oluşumunda e ve d tamsayıları sırasıyla şifreleme üssünü ve deşifreleme üssünü ve n ise mod sayısını gösterir. p ve q sayılarının onluk sistemde uzunluklarının 100 ve dolayısıyla da n nin uzunluğunun 200 olması beklenir. Fakat verilecek örneklerde kolaylık olması açısından küçük sayılar seçilecektir.

Şifreleme Algoritması:

1. B şahsı, A'ya bir m mesajı göndermek istiyor. B, m mesajını şifrelemek için aşağıdakileri yapar:
   - Öncelikle A'nın açık anahtarını (n,e) alır.
   - m mesajını $[0, n-1]$ aralığında yazar.
   - Sonra $c \equiv m^e \,(mod\, n)$ değerini hesaplar.
   - Oluşan c şifresini A'ya gönderir.
2. Şifreli c metninden açık metni bulabilmek için A aşağıdaki işlemi uygular:
   - d gizli anahtarını kullanarak ve $m \equiv c^d \,(mod\, n)$ işlemini uygulayarak m açık metine ulaşır.

NOT: Deşifre sisteminin çalışmasına

$ed \equiv 1 \,(mod\, \phi)$ olduğu içini $ed = 1 + k\phi$ eşitliğini sağlayan mutlaka bir k tamsayısı bulunur. Eğer $gcd\,(m, p) = 1$ ise Fermat teoreminden dolayı

$$m^{p-1} \equiv 1 \,(mod\, p).$$

Eğere bu denkliğin her iki tarafının da $k(q-1)$'inci kuvvetlerini alırsak

$$m^{k(p-1)(q-1)} \equiv 1 \,(\, mod\, p).$$

olur ve her iki tarafı da m ile çarptığımızda

$$m^{1+k(p-1)(q-1)} \equiv m \,(\, mod\, p).$$

sonucuna ulaşırız.

Diğer tarfatan, eğer $gcd\,(m,p) = p$ olursa yukarıdaki denklik yine geçerli olur; çünkü farzedelim belli bir k tamsayısı için $m = kp$ olsun

$$m^{p-1} = (kp)^{(p-1)} = k^{(p-1)}p^{(p-1)} \equiv p \,(\, mod\, p).$$

Eğer bu denkliğin her iki tarafının da $k(q-1)$'inci kuvvetlerini alırsak

$$m^{k(p-1)(q-1)} \equiv p^{k(p-1)(q-1)} \equiv p \,(\, mod\, p).$$

olur ve her iki tarafı da m ile çarptığımızda

$$m^{1+k(p-1)(q-1)} \equiv mp = kp^2 \equiv kp = m \,(\, mod\, p).$$

İki durumda da

$$m^{ed} \equiv m \,(\, mod\, p)$$

olduğu görülür. Aynı şekilde,

$$m^{ed} \equiv m \,(\, mod\, q)$$

olur.

Sonuçta p ve q farklı asal sayılar olğu için,

$$m^{ed} \equiv m \,(\, mod\, n)$$

dir.Böylelikle,

$$c^d = m^{e^d} \equiv m \,(\, mod\, n)$$

Örnek 7.2.1 *1.* ***Anahtar oluşturma****: A şahsı* $p = 2357$ *ve* $q = 2551$ *olan iki tane asal sayı seçmiş olsun. Öncelikle A,*

$$n = pq = 6012707$$

ve

$$\phi = (p-1)(q-1) = 6007800$$

değerlerini hesaplar. A bir tane $e = 3674911$ *değeri seçer.Bu e değeri,* $gcd(e = 3674911, \phi = 6007800) = 1$ *ve* $1 < e = 3674911 < \phi = 6007800$ *koşullarını sağlar. Daha sonra Öklid algoritmasını kullanarak*

$$e \cdot d \equiv 1 \,(mod\, \phi)$$

$$3674911 \cdot d \equiv 1 \,(mod\, 6007800)$$

$d = 422191$ *değerini hesaplar. A' nın açık anahtarı* $(n = 6012707, e = 3674911)$; *gizli anahtarı da* $d = 422191$ *olur.*

2. ***Şifreleme****: B,* $m = 5234673$ *mesajını şifrelemek için A'nın açık anahtarını,yani* $(n = 6012707, e = 3674911)$*, alır ve aşağıdaki şekilde olduğu gibi kapalı metin c 'yi*

hesaplar:

$$c \equiv m^e \,(mod\, n) = 5234673^{3674911} \,(mod\, 6012707) \equiv 3650502$$

ve bu değeri A'ya gönderir.

3. ***Deşifreleme**: A, gelen c kapalı metninden m açık metni aşağıdaki gibi hesaplar:*

$$m \equiv c^d \,(mod\, n) = 3650502^{422191} \,(mod\, 6012707) \equiv 5234673$$

7.3 RSA İmza Şeması

RSA kriptosistemi dijital imzalar için de kullanılabilir. (n, e) A şahsının açık anahtarı, d sayısı da A'nın gizli deşifreleme üssü olsun.Öncelikle mesajın imzalanabilmesi için m mesajının $\{0, 1, \cdots, n-1\}$ arasında olması istenir, daha sonra hesaplamalar yapılır.

7.3.1 İmzalama

A B'ye imzalı m mesajını göndermek isterse, mesaja kendisinin kapalı anahtarını uygular,yani

$$\sigma = m^d \, mod\, n.$$

Daha sonra (m, σ) imzalı mesajı B'ye gönderir.

7.3.2 İmzayı Doğrulama

B, A'dan aldığı (m, σ) imzalı mesajı doğrulamak için

$$m = \sigma^e \, mod \, n$$

değerini hesaplar. Çıkan sonuç m ise mesaj doğrulanmış olur.

Örnek 7.3.1 ***Anahtar Oluşturma:*** *A kişisi* $p = 7927$ *ve* $q = 6997$ *asal sayılarını seçer ve,* $n = pq = 55465219$ *ve* $\phi = 7926 \cdot 6996 = 55450296$ *değerlerini hesaplar. Daha sonra A,* $ed = 5d \equiv 1 \, (mod \, 55450296)$ *eşitliğinden* $d = 44360237$ *sayısını bulur. A'nın açık anahtarı* $(n = 55465219, e = 5)$*; gizli anahtarı* $d = 44360237$ *olur.*

İmzalama: $m = 31229978$ *mesajını imzalamak için A şunu hesaplar:*

$$\sigma = m^d \, mod \, n = 31229978^{44360237} \, mod \, 55465219 \equiv 30729435$$

ve $(m = 31229978, \sigma = 30729435)$ *'yi B'ye gönderir.*

İmzayı Doğrulama: $(m = 31229978, \sigma = 30729435)$*'yi alan B mesajı doğrulamak için şunu yapar:*

$$m = \sigma^e \, mod \, n = 30729435^5 \, mod \, 55465219 \equiv 31229978$$

Çıkan sayı m *olduğu için imza doğrulanmış olur.*

7.4 Ayrık Logaritma(Discrete Logarithm)

RSA kriptosisteminde, RSA fonksiyonu m olan bir elemanın e. kuvvetini oluşturur. Bu fonksiyon birebir bir fonksiyondur ve etkili bir şekilde hesaplanır.Eğer n nin çarpanlara ayrımı bilinmiyorsa, e. kökü hesaplamak için etkili bir algoritma yoktur. Sayılar teorisinde hesaplaması kolay fakat tersinin hesaplaması zor olan başka fonksiyonlar da vardır. Bunlardan en önemlilerinden biri de sınırlı alanlar da (finite fields) kuvvet almadır. Basit olarak sadece asal alanlar (prime fields) düşünülecektir.

p bir asal sayı ve g de Z_p^* de bir primitif kök olsun. Ayrık kuvvet fonksiyonu (discrete exponential function)

$$\text{Exp} : Z_{p-1} \to Z_p^*,\ x \mapsto g^x,$$

tekrarlı karesini alma algoritması örneğinde olduğu gibi etkili bir şekilde hesaplanabilir. Kuvvetin logaritması fonksiyonunun tersini hesaplamak için etkili bir algoritma bilinmemektedir. Bu tahmine ayrık logaritma tahmini (discrete logarithm assumption) denir.

7.5 El-Gamal Açık Anahtarlı Kriptosistem

ElGamal açık anahtarlı şifre sistemi,anahtar transferi modunda Diffie-Hellman anahtar anlaşması(Diffie-Hellman Key Agreement) olarak görülebilir. Güvenilirliği ayrık logaritma problemi ve Diffie-Helman probleminin kolay çözülememesi temeline dayanır. Temel ElGamal ve genelleştirilmiş ElGamal şifreleme şeması bu bölümde tanımlanmıştır.

7.6 ElGamal Açık Anahtarlı Şifrelemede Anahtar Oluşturma Algoritması

Her kişi kendi açık anahtarını ve buna bağlı gizli anahtarını oluşturur. Bunu oluşturmak için A şahsı şunları uygular:

1. Çok büyük rastgele bir p asal sayısı ve mod p ye göre tamsayıların oluşturduğu çarpım grubu Z_p^* nin bir jeneratörü α yı oluşturur.
2. $1 \leq a \leq p-2$ şeklinde olan bir a tamsayısı seçer ve $\alpha^a \, mod \, p$ değerini hesaplar.
3. A'nın açık anahtarı (p, α, α^a); A'nın gizli anahtarı ise a olur.

7.6.1 ElGamal Açık Anahtarlı Şifreleme Algoritması

B şahsı A için m mesajını şifrelesin.

1. **Şifreleme:** B mesajı şifreleme için şunları yapar:
   - A'nın açık anahtarını (p, α, α^a) alır.
   - mesajı $\{0, 1, \cdots, p-1\}$ aralığında m tamsayısı olarak ifade eder.
   - $1 \leq k \leq p-2$'yi sağlayan rastgele bir k tamsayısı seçer.
   - $\gamma = \alpha^k \, mod \, p$ ve $\delta = m \cdot (\alpha^a)^k \, mod \, p$ değerlerini hesaplar.
   - Son olarak $c = (\gamma, \delta)$ kapalı metnini A'ya gönderir.
2. **Deşifreleme:** c kapalı metninden m açık metine ulaşmak için A şunları yapar:

- a gizli anahtarını kullanarak $\gamma^{-a} \, mod \, p$ değerini hesaplar ($\gamma^{-a} = \alpha^{-ak} \, mod \, p$).
- $\gamma^{-a} \cdot \delta \, mod \, p$ değerini hesaplayarak m'yi bulur.

$$\gamma^{-a} \cdot \delta \equiv \alpha^{-ak} \cdot m\alpha^{ak} \equiv m \, (mod \, p)$$

Örnek 7.6.1 ***Anahtar Oluşturma:*** *A şahsı bir* $p = 2357$ *asal sayısı ve* $\alpha = 2 \in \mathcal{Z}^*_{\in \ni \bigtriangledown'}$ *bir jeneratör seçer. Buna ilave olarak bir* $a = 1751$ *gizli anahtarı seçer ve*

$$\alpha^a \, mod \, p = 2^{1751} \, mod \, 2357 \equiv 1185$$

değerini hesaplar. A'nın açık anahtarı $(p = 2357, \alpha = 2, \alpha^a = 1185)$ *tir.*

Şifreleme: $m = 2035$ *mesajını şifrelemek için B şahsı rastgele bir* $k = 1820$ *tamsayısı seçer ve*

$$\gamma = 2^{1520} \, mod \, 2357 \equiv 1430$$

ve

$$\delta = 2035 \cdot 1185^{1520} \, mod \, 2357 \equiv 697$$

değerlerini hesaplar. Son olarak B $(\gamma = 1430, \delta = 697)$ *'yi A'ya gönderir.*

Deşifreleme: *A gelen kapalı metni çözmek için*

$$\gamma^{-a} = 1430^{-1750} \equiv 1430^{605} \, mod \, 2357 \equiv 872$$

bulur ve m mesajına da

$$m = 872 \cdot 697 \, mod \, 2357 \equiv 2035$$

böylece ulaşır.

7.6.2 ElGamal İmzası

ElGamal kriptosisteminde imza RSA 'da olduğu gibi mesajın doğru kişiden geldiğini kontrol etmek için kullanılır. Sadece kapalı metin yerine imzalanmış kapalı metin gönderilerek o kapalı metnin istenen kişiden gelip gelmediği de kontrol edilmiş olur. A şahsının açık anahtarı $(p, \alpha, \alpha^a = y)$ ve gizli anahtarının da a olduğu düşünülsün.

7.6.3 İmza Algoritması

m mesajının Z_p nin bir elemanı olduğu düşünülür.Eğer değilse hash fonksiyonu kullanılarak m mesajının Z_p nin elemanı olması sağlanır. A şahsı m mesajını şu şekilde imzalar:

1. Rastgele bir t tamsayısı seçer öyleki $1 \leq t \leq p-2$ ve $gcd(t, p-1) = 1$ koşulunu sağlamalıdır.
2. $r = \alpha^t$ ve $s = t^{-1}(m - ra) \, mod \, (p-1)$ eşitliklerini kurar.
3. (m, r, s) A'nın imzalı mesajıdır.

7.6.4 Doğrulama

(m, r, s) imzalı mesajı alan B şahsı aldığı mesajın A'dan geldiğini şu şekilde doğrular:

1. Öncelikle $1 \leq r \leq p-1$ olduğunu kontrol eder.Eğer değilse imzayı reddeder.
2. Daha sonra $v = \alpha^m$ ve $w = y^r r^s$ değerlerini hesaplar (Buradaki y sayısı A'nın açık anahtarındaki y sayısıdır.)
3. Eğer $v = w$ eşitliği sağlanıyorsa imza kabul edilir, aksi taktirde reddedilir.

Örnek 7.6.2 ***Anahtar Oluşturma:*** *A şahsı bir* $p = 2357$ *asal sayısı ve* $\alpha = 2 \in \mathcal{Z}^*_{\in \ni \bigtriangledown}$ *bir jeneratör seçer. Buna ilave olarak bir* $a = 1751$ *gizli anahtarı seçer ve*

$$\alpha^a \, mod \, p = 2^{1751} \, mod \, 2357 \equiv 1185$$

değerini hesaplar. A'nın açık anahtarı $(p = 2357, \alpha = 2, \alpha^a = 1185)$ *tir.*

İmza Oluşturma: *Basit olması açısından mesaj* $m = 1463$ *olarak seçilsin (Eğer mesaj* p *asal sayısından büyük olsaydı hash fonksiyonundan geçirilirdi).* $m = 1463$ *mesajını imzalamak için A önce rastgele bir* $t = 1529$ *sayısı seçer, daha sonra*

$$r = \alpha^t \, mod \, p = 2^{1529} \, mod \, 2357 \equiv 1490$$

ve

$$t^{-1} \, mod \, (p-1) = 1529^{-1} \, mod \, (2356) \equiv 245$$

$$s = t^{-1}(m - ra) \, mod \, (p-1) = 245(1463 - 1490 \cdot 1751) \, mod \, 2356 \equiv 1777$$

A'nın imzası $(m = 1463, r = 1490, s = 1777)$

İmzayı Doğrulama: *B aldığı imzalı mesajı doğrulamak için önce*

$$v = \alpha^m \, mod \, p = 2^{1463} \, mod \, 2357 \equiv 1072$$

değerini hesaplar. Daha sonra

$$w = y^r r^s \, mod \, p = 1185^{1490} 1490^{1777} \, mod \, 2357 \equiv 1072$$

değerini hesaplar ve $v = w$ *olduğu için imzayı kabul eder.*

7.7 Diffie-Hellman Anahtar Anlşması (Diffie-Hellman Key Agreement)

Diffie-Hellman anahtar anlaşması, anahtar dağıtma problemine ilk pratik çözümdür. Üs olarak anahtar değiştirme olarak da bilinen bu sistem daha önce hiç haberleşme sağlamamış iki tarafın açık kanal üzerinden mesajlarını birbirlerine göndererek ortak bir anahtar yaratma temeline dayanır.

p yeteri kadar büyük bir asal sayı olsun öyleki Z_p^* de discrete logaritma problemini çözmek mümkün olmasın. g'de Z_p^* de primitif bir kök (primitive root) olsun. p ve g herkes tarafından bilinsin. A ve B kişileri aşağıdaki yolu izleyerek ortak bir anahtar yaratabilirler:

7.7.1 Diffie-Hellman Anahtar Anlaşması Algoritması:

- A, $0 \leq a \leq p-2$ eşitsizliğini sağlayan ve tesadüfi olan bir a sayısı seçer. $c = g^a$'yı bulur ve bunu B'ye gönderir.
- A, $0 \leq b \leq p-2$ eşitsizliğini sağlayan ve tesadüfi olan bir b sayısı seçer. $d = g^b$'yi bulur ve bunu A'ya gönderir.

- A, ortak anahtar k'yı şu şekilde hesaplar:

$$k = d^a = (g^b)^a$$

- B, ortak anahtar k'yı şu şekilde hesaplar:

$$k = c^b = (g^a)^b$$

Böylelikle A ve B aralarında ortak bir anahtar olan k için anlaşmış olurlar.