Bilgi Güvenliği ve Kriptografi

Kriptoloji-Kriptografi-Kriptoanaliz

- Bilginin değiştirilerek korunması ile uğraşan bilim, **kriptoloji** (kryptos-gizli, logos-bilim) olarak adlandırılır.
- Kriptoloji, *kriptografi* ve *kriptoanaliz* olmak üzere iki kısma ayrılır.
  - **Kriptografi** bilimi, mesajların içeriğini gizleyerek bir şifreleme sisteminin oluşturulmasıyla ilgilenir. Bir kriptografik algoritma, şifreleme ve deşifreleme için kullanılan matematiksel fonksiyonlardan oluşur. Şifreleme ve deşifreleme işlemlerinde ayrıca, bir anahtar değeri kullanılmaktadır.
  - **Kriptoanaliz** ise, şifreleme anahtarı bilinmeden şifreyi çözme yöntemleriyle uğraşmaktadır. Kriptoanalizin başarısı, mesaj yada anahtarın elde edilmesiyle değerlendirilmektedir

Kriptosistemler için Gerekli Koşullar

Bilginin korunması için günümüzdeki kriptosistemler aşağıdaki koşulları gerektirmektedir.

- Şifreli bilgi yalnız anahtar bilindiği durumda okunabilmelidir.
- Şifreli metin parçası ve ona karşılık gelen açık metine göre kullanılan şifreleme anahtarının belirlenmesi için gerekli işlem sayısı, bütün mümkün anahtarlar sayısından daha az olmamalıdır.
- Anahtarların denenerek bulunması için gerekli işlem sayısı, kesin alt sınıra sahip olmalıdır ve bu sınır günümüzdeki bilgisayarların erişebileceği sınırın üzerinde olmalıdır.
- Şifreleme algoritmasının bilinmesi bilgi güvenliğine etki etmemelidir.

Kriptosistemler için Gerekli Koşullar

- Anahtar değerindeki küçük bir değişim şifreli metinde büyük değişimlere neden olmalıdır.
- Şifreleme algoritmasının yapısal bütünlüğü sağlanmalıdır.
- Anahtar kümesi içerisinden ele alınan keyfi bir anahtar bilgi güvenliğini sağlamalıdır.
- Şifreli metnin boyu yaklaşık olarak ana metinle aynı olmalıdır.
- Algoritmalar yazılımsal olduğu kadar donanımsal kullanıma da imkan sağlamalıdır.
- Anahtarın boyunun değiştirilmesi algoritmanın etkinliğini bozmamalıdır.
- Anahtarlar arasında basit ve kolaylıkla oluşturulabilecek ilişkiler bulunmamalıdır.

Kriptosistemlerin Hedefleri

- **Güvenilirlik (Confidentiality):** Bilginin içeriğinin, yetkili kimseler dışındaki herkesten saklı tutulması servisidir. Güvenilirliği sağlama konusunda pek çok yaklaşım vardır. Bunlar, fiziksel korumadan matematiksel algoritmalara kadar sıralanır ve veriyi anlaşılmaz hale getirir.

- **Veri Bütünlüğü (Data Integrity):** Verinin izinsiz olarak değiştirilmesini engellemeye yönelik bir servistir. Verinin bütünlüğünü temin etmek için, yetkisiz kişilerce verinin işlenmesinin tespit edilmesi gerekir. Verinin işlenmesi ekleme, silme, yer değiştirme gibi işlemleri içerir.

- **Belgeleme (Authentication):** Tanıma ve kimlik saptama ile ilişkili bir servistir. Bu fonksiyon hem bilginin kendisine hem de haberleşen kişilere uygulanır. Haberleşmeye başlayan iki taraf birbirini tanımalıdır. Kriptografinin bu konusu, *kişinin belgelenmesi* (entity authentication) ve *veri kaynağının belgelenmesi* (data origin authentication) olmak üzere iki ana sınıfa ayrılır Veri kaynağının belgelenmesi dolaylı olarak veri bütünlüğünü de sağlar. Veride değişiklik olması durumunda kaynak ta değişecektir.

- **İnkarı Önleme (Non-Repudiation):** Bir kişinin önceki sorumluluklarını yada yaptığı şeyleri inkar etmesini önleyen servistir. Bu amaçla sistemde herkesin güvendiği 3. bir kişi bulunabilir.

Kriptoloji Terminolojisinde Kullanılan Kavramlar

- **Alıcı ve Gönderici (Receiver and Sender):** Bir mesajı gönderen kişiye *gönderici*, mesajı alan kişiye ise *alıcı* adı verilir. Gönderici alıcıya bir mesaj gönderirken, başka kişilerin mesajı okumayacağından emin olmak istemekte, dolayısıyla mesajın güvenli ve gizli bir şekilde alıcıya ulaşmasını sağlamaya çalışmaktadır.

- **Mesajlar ve Şifreleme:** Bir mesaj *açık metin* (plaintext) olarak adlandırılır. Mesajın özünü gizlemeye yönelik yapılan değiştirme işlemine *şifreleme* (encryption) adı verilir. Şifrelenmiş mesaj, *şifreli metin* (ciphertext)'dir. Şifreli metni açık metne dönüştürme işlemi ise *deşifreleme* (decryption) olarak adlandırılır.

Kriptoloji Terminolojisinde Kullanılan Kavramlar

- E şifreleme fonksiyonu, M açık metnine uygulanarak C şifreli metni elde edilir. Bu matematiksel olarak aşağıdaki şekilde ifade edilir.

$$E(M) = C$$

- D deşifreleme fonksiyonu ise, C şifreli metninden M açık metninin elde edilmesinde kullanılır. Bunun matematiksel ifadesi ise;

$$D(C) = M$$

Kriptoloji Terminolojisinde Kullanılan Kavramlar

- **Algoritmalar ve Anahtarlar:** Bir kriptografik algoritma, şifreleme ve deşifreleme için kullanılan matematiksel fonksiyonlardan oluşur.

- Kriptografide, *K* ile ifade edilen bir şifreleme anahtarı kullanılır. Anahtar için mümkün değerler kümesine, *anahtar uzayı* (keyspace) adı verilir. Hem şifreleme hem de deşifreleme işlemleri, bu anahtar kullanılarak gerçekleştirilir. Bazı algoritmalar, farklı şifreleme (K_1) ve deşifreleme (K_2) anahtarları kullanırlar

$$E_K(M) = C \qquad E_{K_1}(M) = C$$

$$D_K(C) = M \qquad D_{K_2}(C) = M$$

Kriptoloji Terminolojisinde Kullanılan Kavramlar

- Uygulanan algoritmanın güvenliği seçilen anahtara bağlıdır. Şifreleme algoritması bilindiğinde anahtar değeri elde edilmeden mesajların okunması mümkün değildir. Anahtar tabanlı algoritmaların *simetrik* (symmetric) ve *genel* (*açık*) *anahtar* (public key) olmak üzere iki genel türü vardır

Simetrik Algoritmalar:

- Simetrik algoritmalarda, şifreleme anahtarının deşifreleme anahtarından üretilmesi mümkün ve oldukça kolaydır. Bunun tersi de doğrudur.
- Çoğu simetrik algoritmalarda, şifreleme ve deşifreleme için kullanılan anahtar aynıdır. Anahtar kullanımına bağlı olarak bu algoritmalar
  - *tek anahtarlı* (single key),
  - *gizli anahtarlı* (secret key)

  algoritmalar olarak ta adlandırılmaktadır.
- Alıcı ve göndericinin güvenli bir şekilde haberleşmesi için, öncelikle belirli bir anahtar üzerinde görüş birliğine varmaları gerekir.
- Bu algoritmaların güvenliği anahtara bağımlı olduğu için, anahtarı bilen herkes mesajları şifreleme ve deşifreleme imkanına sahiptir. Haberleşmenin güvenli olması için anahtar gizli tutulmalıdır.

Simetrik Algoritmalar:

- Simetrik algoritmalar iki sınıfa ayrılır.
  - Açık metnin bitler ardışıklığı üzerinde işlem yapan algoritmalar, *akış şifreleyiciler* (stream ciphers) olarak adlandırılır.
  - *Blok şifreleyiciler* (block ciphers) ise, işlemleri bit grupları üzerinde gerçekleştirir. Bu bit grubuna blok adı verilir.

Genel (Açık) Anahtar Algoritmalar:

- Genel anahtar algoritmalar aynı zamanda asimetrik algoritmalar olarak ta bilinmektedir.
- Bu algoritmalarda şifreleme anahtarı, deşifreleme anahtarından farklıdır. Öte yandan, şifreleme anahtarından faydalanılarak deşifreleme anahtarının hesaplanması mümkün değildir.
- Şifreleme anahtarı genel olarak herkesin kullanımına açıktır. Herhangi bir kişi bu anahtarı kullanarak mesajlarını şifreleyebilir, fakat yalnız deşifreleme anahtarına sahip alıcılar mesajları deşifre edip okuyabilir.
- Bu sistemde şifreleme anahtarı *genel anahtar* (public key), deşifreleme anahtarı ise *özel anahtar* (private key) olarak adlandırılır.

Kriptolojinin Matematiksel Temelleri-Asal Sayılar

Asal Sayılar

- Herhangi pozitif bir tam sayı, sadece 1'e ve kendisine bölünebiliyorsa, asal sayı olarak adlandırılır. Asal olmayan sayılar bileşik sayılardır. Bunun sonucu olarak 1'den büyük tüm sayılar asal veya bileşiktir. En büyük ortak böleni 1 olan iki sayı ise *aralarında asal* sayılar olarak adlandırılır.
- Asal sayıların çarpılması ile tüm pozitif tam sayıları oluşturmak mümkündür. Herhangi bir asal olmayan pozitif *n* tam sayısı, asal sayıların çarpımı şeklinde ifade edilebilir.
- $n = p_1 * p_2 * \cdots * p_m$
- 12=2*2*3 11011=7*11*11*13

- **Böyle bir çarpanlara ayırma her zaman mümkündür.**
- **Her bir pozitif tamsayı aşağıdaki formda yazılabilir.**

$$n = \prod_p p^{n_p} \qquad n_p \geq 0$$

Kriptolojinin Matematiksel Temelleri-Asal Sayılar

- Sağ taraf sonsuz sayıdaki asal sayıların çarpımından oluşur. Fakat herhangi bir *n* için, bazı üsler 0 olduğundan çarpanlar 1 olacaktır. Bu nedenle, bu işlem sonlu bir işlemdir.

- Burada $(n_2, n_3, n_5, \ldots)$ dizisi, pozitif tamsayılar için sayı sistemi olarak düşünülebilir. Örneğin, bu sayı sisteminde, 12'nin asal-üs gösterimi (2,1,0,...), 18'inki ise (1,2,0,...) şeklindedir.

- İki sayıyı çarpmak için bu iki sayının asal-üs gösterimi toplanır (12*18=216->(3,3,0,…)).

$$k = mn \quad \Leftrightarrow \quad k_p = m_p + n_p \quad tüm \quad p'ler \quad için$$

Kriptolojinin Matematiksel Temelleri-Asal Sayılar

- Asal-üs gösterimiyle, sayıların *gcd* (greatest common divisor-ortak bölenlerin en büyüğü) ve *lcm* (least common multiple-ortak katların en küçüğü) ilişkisi de elde edilebilir.

$$k = \gcd(m,n) \quad \Leftrightarrow \quad k_p = \min(m_p, n_p)$$
$$k = lcm(m,n) \quad \Leftrightarrow \quad k_p = \max(m_p, n_p)$$

- Örneğin, 12 ve 18 için, bu sayıların en büyük ortak böleni, ortak üslerin maksimumu ile, ortak katlarının en küçüğü ise ortak üslerin minimumu ile elde edilebilir.

$$gcd(12,18) = 2^{\min(2,1)}.3^{\min(1,2)} = 2.3 = 6$$

$$lcm(12,18) = 2^{\max(2,1)}.3^{\max(1,2)} = 2^2.3^2 = 36$$

Kriptolojinin Matematiksel Temelleri-Asal Sayılar

- *p* asal sayısı, *m***n* çarpımını tam olarak bölüyorsa, *p*, *m*'yi, *n*'yi yada her ikisini tam olarak böler. Fakat bileşik sayılar bu özelliğe sahip değildir.

- Örneğin; 4, 60=6.10'u kalansız böler. Fakat 6 yada 10'u tam olarak bölmez. Bunun nedeni 60'ın çarpanlarına ayrılmasında 60=(2*3)(2*5) eşitliğinin mevcut olmasıdır. Burada 4'ün iki asal çarpanı, 4=2.2, iki parçaya bölünmüştür. Asal sayı bu şekilde parçalanamayacağı için, orijinal çarpanlardan birini mutlaka bölmelidir.

- Genel anahtar kriptosistemlerde asal sayılara dayalı çarpanlara ayırma problemine ayrıca değinilecektir.

Kriptolojinin Matematiksel Temelleri-MOD İşlemi

Modüler aritmetik, sayı teorisi ile sağlanan ana araçlardan birisidir.

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \bmod m = b \bmod m$$

$a \equiv b \pmod{m}$ denklemi, "a, mod m'ye göre b'ye denktir" şeklinde okunur. Örneğin 9≡-16 (mod 5)'tir. Çünkü 9=4(mod 5) ve –16=4(mod 5)'tir. Mod işlemini aşağıdaki şekilde de ifade etmek mümkündür.

$a \equiv b \pmod{m} \quad \Leftrightarrow \quad (a-b)$, m'nin katı ise

Kriptolojinin Matematiksel Temelleri-MOD İşlemi

Denklik işareti '≡' , eşitlik işaretine '=' eşdeğer görünür. Bir denklik ilişkisinde; '$a \equiv a$' yansıma özelliğini, '$a \equiv b \Rightarrow b \equiv a$' simetri özelliğini ve '$a \equiv b \equiv c \Rightarrow a \equiv c$' geçişli olma özelliğini sağlar. Çünkü herhangi bir $a \equiv b \Leftrightarrow f(a)=f(b)$'yi sağlayan ilişki, denklik ilişkisidir. Bundan başka denkliği kaybetmeden elemanları toplamak ve çıkarmak mümkündür.

$$a \equiv b \text{ ve } c \equiv d \quad \Rightarrow \quad a+c \equiv b+d \pmod{m}$$

$$a \equiv b \text{ ve } c \equiv d \quad \Rightarrow \quad a-c \equiv b-d \pmod{m}$$

Kriptolojinin Matematiksel Temelleri-MOD İşlemi

Tam sayılarla işlem yapıldığında çarpma işlemi de aynı özelliğe sahiptir.

$$a \equiv b \text{ ve } c \equiv d \quad \Rightarrow \quad ac \equiv bd \pmod{m} \qquad b, c \text{ tamsayı}$$

$ac-bd=c(a-b)+b(c-d)$ olduğundan, bu çarpım özelliğinin tekrarlanması ile, üs alma işlemi gerçekleştirilebilir.

$$a \equiv b \quad \Rightarrow \quad a^n \equiv b^n \pmod{m} \qquad a, b, n \text{ tamsayı}, n \geq 0$$

Örneğin $2 \equiv (-1) \pmod 3$ olduğundan, $2^n \equiv (-1)^n \pmod 3$ olur. Bu 2^n-1'in n çift olduğunda, 3'ün katı olduğu anlamına gelir.

Kriptolojinin Matematiksel Temelleri-MOD İşlemi

Bu sayede, alışılmış denklemlerle yapılan çoğu cebirsel işlem, denkliklerle de yapılabilir. Bölme işlemi, dikkat çekici bir şekilde mevcut değildir. $ad \equiv bd \pmod{m}$ ise, her zaman, $a \equiv b$ sonucuna varılamaz. Örneğin, $3*2 \equiv 5*2 \pmod{4}$ olduğu halde 3, 5'e denk değildir. Fakat d ve m aralarında asal ise denklik sağlanır.

$$ad \equiv bd \quad \Leftrightarrow \quad a \equiv b \pmod{m} \qquad a,b,d,m \text{ tamsayı, } d \perp m$$

Örneğin, $15 \equiv 35 \pmod{m}$'den, $3 \equiv 7 \pmod{m}$'yi çıkarmak, m, 5'in katı olmadığı sürece mümkündür.

Kriptolojinin Matematiksel Temelleri-MOD İşlemi

Denkliğe bölmeyi uygulamanın başka bir yolu, modun da diğer sayılar gibi bölünmesidir.

$ad \equiv bd \pmod{md} \quad \Leftrightarrow \quad a \equiv b \pmod{m}, \; d \neq 0$

Dağılma kurallarına dayanan bu kural, tüm a,b,d,m sayıları için doğrudur.

$(a \bmod m)\, d = (ad \bmod md)$

$a \bmod m = b \bmod m \Leftrightarrow (a \bmod m)d = (b \bmod m)d \Leftrightarrow ad \bmod md = bd \bmod md$ elde edilir. Böylece $3*2=5*2 \pmod 4$ den $3 \equiv 5 \pmod 2$ sonucuna varılır.

Yukarıdaki özellikler genel bir kural oluşturmak için aşağıdaki şekilde birleştirilebilir.

$$ad \equiv bd \pmod{m} \quad \Leftrightarrow \quad a \equiv b \left(\bmod \frac{m}{\gcd(d,m)} \right) \quad a, b, d, m \text{ tamsayı}$$