AĞ GÜVENLİĞİ

2. Öğretim A Şube

Ad-Soyad : wajeeh albasha

Öğrenci numarası : G181210552

Kriptografi Tanımı :

Kriptografik algoritmalar bilgi toplumunda çok önemli bir rol oynamaktadır. Banka kartı veya kredi kartı kullandığımızda, birisini cep telefonundan aradığımızda, sağlık vaka hizmetlerine eriştiğimizde veya web'den bir şey satın aldığımızda, kriptografik algoritmalar bizi korur. Bu algoritmalar, işlemlerimizin ve banka hesaplarımızın güvende olmasını, kimsenin cep telefonu, VoIP veya anlık mesajlaşma iletişimlerimizi dinlememesini ve hassas sağlık verilerinin yetkisiz erişime karşı korunmasını sağlar. Kriptografik protokoller ayrıca dijital imzalar, kullanıcı ve veri kimlik doğrulaması ve elektronik para veya elektronik oylama gibi daha gelişmiş işlevler sağlayabilir. Bilgi teknolojisi daha da genişliyor ve kısa vadede daha fazla e-devlet, eoylama, e-ticaret görmeyi bekliyoruz.

Kriptografinin birbirini tamamlayan iki yönü vardır: açık anahtarlı kriptografi ve özel anahtarlı kriptografi.

AÇIK ANAHTAR :

Açık anahtar (veya Asimetrik) Şifreleme, 1976'da Diffie ve Hellman tarafından icat edilen bir kavramdır. Kullanıcıların, ortak anahtar ve özel anahtar olarak belirlenmiş bir çift şifreleme anahtarı kullanarak, paylaşılan bir gizli anahtara önceden erişime sahip olmadan güvenli bir şekilde iletişim kurmasını sağlar. , matematiksel olarak ilişkilidir. Açık anahtar kriptografisi genellikle, bilinmeyen bir çarpanlara ayırma tamsayısının üslenmesi modulo veya iyi seçilmiş bir eliptik eğrinin noktaları grubundaki hesaplama gibi bazı sayı teorik ilkellerine dayanır.

Açık anahtarlı şifrelemedeki modern yaklaşım, kanıtlanabilir güvenlik yaklaşımıdır. Bir kriptosistemin güvenliğinin kanıtlanması, önce kriptosistem tarafından ulaşılması gereken güvenlik kavramlarının resmileştirilmesinden oluşur ve bu güvenlik kavramları da matematiksel bir kanıtla kurulabilir. Güvenlik kanıtları çoğunlukla görecelidir: Biri, iyi tanımlanmış bir hesaplama probleminin sertliğini varsayarak, belirli bir güvenlik kavramına ulaşıldığını gösterir. Kanıtlanabilir güvenlik, günümüzün kriptografisinde ana akımdır.

KRIPTOGRAFI AMACI :

Kriptografi, bir düşmanın varlığına rağmen bir amacı gerçekleştiren planlar yapmakla ilgilidir. Bu nedenle, bir şifreleme sisteminin güvenliğini resmileştirmek için, saldırganın ne yapmasına izin verildiğini ve saldırının ne zaman başarılı olduğunu belirtmek gerekir. Bazı karmaşıklık varsayımları altında (örneğin, büyük tamsayıları çarpanlara ayırmak zordur) bu tür bir saldırının imkansız olduğu (belki ihmal edilebilir olasılık dışında) gösterilebilirse, bir kriptosistem "güvenli" olarak adlandırılacaktır. Örneğin, bir açık anahtar şifreleme şeması için, saldırganın amacının açık anahtardan özel anahtarı kurtarmak olduğu düşünülebilir. Ama bu aslında çok iddialı bir hedeftir (ki bu da planın tamamen bozulmasına tekabül eder). Uygulamada, saldırgan daha mütevazı bir hedef izliyor olabilir, örneğin karşılık gelen şifreli metin verilen düz metni kurtarmak veya hatta düz metin hakkında sadece bir bit bilgi elde etmek.

Bir kriptografik işlevselliğin güvenliğini doğru bir şekilde formüle etmek kolay bir iş değildir. İmza şemaları için, ilk tatmin edici güvenlik kavramı yalnızca 1988'de elde edildi (bu, S. Goldwasser, S. Micali ve R. Rivest tarafından "A dijital imza şeması -mesaj saldırıları", SIAM J. of computer, 1988).

Açık anahtarlı şifreleme şemaları için, ilk tatmin edici kavram sadece 1991'de elde edildi (bu, Charles Rackoff ve Daniel R. Simon tarafından "İnteraktif Olmayan Sıfır-Bilgi Kanıtı ve Chosen Ciphertext Attack", CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology). Bununla birlikte, bir güvenlik kavramını doğru bir şekilde tanımlamak hayati derecede önemlidir: bir kişi, güvenli bir şemanın hangi özellikleri elde etmesi gerektiğini bilmiyorsa, güvenli bir şema elde etmeyi umamaz!

Güvenlik kavramı doğru bir şekilde resmileştirildikten sonra, ikinci adım, bu tanımı kanıtlanabilir bir şekilde karşılayan bir şema oluşturmaktan oluşur. Güvenlik kanıtı çoğunlukla indirgeme yoluyla bir kanıttır: biri, güvenlik kavramı karşılanmadıysa, yani düzeni bozabilecek bir saldırgan varsa, o zaman bu saldırganı kullanarak birinin, olduğuna inanılan bir matematik problemini verimli bir şekilde çözebileceğini gösterir. çözülmesi zor (örneğin, büyük tamsayıları çarpanlara ayırma). Bu nedenle, bir şifreleme şemasının güvenliği çoğunlukla görecelidir: güvenlik, yaygın olarak inanılan bir karmaşıklık varsayımına dayanır (örneğin, büyük tamsayıları çarpanlara ayırmak zordur). Kanıtlanabilir güvenlik alanı şu üç adımın birleşimidir: tanım, şema ve güvenlik kanıtı. Bu yaklaşım artık kriptografik araştırma topluluğunda ana akımdır.

ÖZEL ANAHTAR :

Özel Anahtar (veya Simetrik) Şifreleme, paylaşılan gizli anahtar ayarında verimli ve güvenli ilkeller oluşturmakla ilgilidir. Blok şifreler, akış şifreleri, kriptografik özet fonksiyonları ve mesaj doğrulama kodları, sundukları yüksek hız ve kullanım kolaylığı nedeniyle günümüzün güvenlik protokollerinin çoğunun inşa edildiği temel ilkellerdir. Son birkaç yılda, yeni şemaların belirli güvenlik özelliklerini kanıtlayan artan sayıda makale gördük. Ancak, bu kanıtların kapsamı hala çok sınırlıdır (genellikle dar bir saldırı sınıfına karşı direnç gösterilir). Güvenlik anlayışımızı geliştirmek ve mevcut ve gelecekteki algoritmalara olan güvenimizi artırmak için, güvenliklerini değerlendirmek için yeni yöntemler geliştirmeye ve yeni saldırılar ve tasarım fikirleri geliştirmeye hala ihtiyaç var.