Kriptoloji (Cryptology)

Bu yazımızda kriptoloji(cryptology)'nin yani şifre bilimine basit anlamda bir giriş yapacağız. Kriptolojiyi tanımladıktan sonra kriptoloji tarihine geçiş yapacağız. Kriptolojinin temel olarak ayrıldığı iki dalı vardır: Kriptografi(Cryptography) ve Kripto analiz(Cryptanalysis).

Kriptoloji basit anlamda şifreli belgeler, gizli yazılar bilimidir. İki ayrı ana dalı vardır: Kriptografi ve Kripto analiz. **Kriptografi**, metin şifrelemekte kullanılan tekniklerin tümünü inceleyen bilim dalıdır. **Kripto analiz**, ise şifrelenmiş bir metnin şifrelenmemiş düz metin haline getirebilmek için yapılabilecek her türlü saldırıları ve türlerini inceleyen bilim dalıdır. Kaba tabiriyle, kriptografi bilimi ile şifrelenen metinler, kripto analiz bilimi ile kırılmaya çalışılır.

Kriptolojinin tarihçesine baktığımızda uzun yıllar geriye gitmemiz gerekmektedir. M.Ö. 1900'lü yıllarda firavunların mezarlarındaki yazıtlarda kullanılan semboller bilinen ilk kriptografik dönüşümlerdir. Daha çok sıkı askeri disiplinleri ve talimleriyle tanınan Kuzey Yunanistandaki tarihi bir şehir olan Sparta' da M.Ö. 475 yılında bilinen ilk kriptografik iletişim aracı 'skytale' geliştirilmiştir. M.Ö. 60'lı yıllarda ise Julius Ceaser askeri anlamda şifreli metinleri kullanan ilk kişidir. Daha sonraki makalelerimizde daha detaylı olarak anlatacağımız Ceaser şifrelemesi o zamanlara dayanmaktadır. Bilinen en eski bilimsel kripto analiz eseri, ünlü Yunan bilim adamı alKalkashandi tarafından 1412 yazılmıştır. Ardından birinci dünya savaşı yıllarına kadar bu alanda pek bir gelişme kaydedilmemiştir. 1917'de Edward Hugh Hebern tarafından Rotor machine adı verilen bir şifreleme aracı geliştirilmiştir. 1971'de de IBM tarafından Lucifer adı verilen şifreleme şeması oluşturulmuştur. 1975'te DES, 1976'da da Diffie and Hellman şifreleme teknikleri geliştirilmiştir. Burada ismi geçen şifreleme yöntemleri daha sonraki makalelerimizde çok daha detaylı olarak işlenecektir.

Kriptografiyi temel olarak üç ayrı sınıfa ayırmak mümkün. Birincisi düz metni belirli şifreleme algoritmaları çerçevesinde geri dönüşümü olacak şekilde şifrelemektir. Harflerin yerlerinin değiştirilmesi ya da her harfin başka bir harfle değiştirilmesidir. Bir örnek ile açıklamak istersek, DOTNET kelimesini TTEDON ve ya EPUOFU şeklinde şifreleyebiliriz. İkinci yöntem olarak da, gönderen ve/veya alıcı tarafından bilinen anahtarlar kullanılarak metinleri şifreleyebiliriz. DES, IDEA vs.. Üçüncü yöntem olarak da metinleri bloklar halinde ve bir bütün olarak şifreleyebiliriz. Block Cipher ve Stream Cipher.

Kripto analizinde kullanılacak stratejiler kullanılan şifreleme planına ve elimizdeki bilgilere göre değişmektedir. Aşağıdaki tabloda şifrelenmiş metin üzerine yapılabilecek saldırı çeşitleri listelenmiştir:

Saldırı türü	**Kripto analiz için bilinenler**
Sadece Şifrelenmiş Metin	Şifreleme algoritması Deşifre edilecek şifreli metin
Şifrelenmemiş Metin	Şifreleme algoritması Deşifre edilecek şifreli metin Bir ya da daha fazla şifrelenmemiş metin örneği çifti
Belirli Şifrelenmemiş Metin	Şifreleme algoritması Deşifre edilecek şifreli metin Şifreli metin ve bu metne karşılık gelen şifrelenmemiş metin örneği
Belirli Şifrelenmiş Metin	Şifreleme algoritması Deşifre edilecek şifreli metin Şifrelenmiş ve deşifre edilmiş anlamlı metin
Belirli Metin	Şifreleme algoritması Deşifre edilecek şifreli metin Şifrelenmiş ve deşifre edilmiş anlamlı metin Şifreli metin ve bu metne karşılık gelen şifrelenmemiş metin örneği

Kriptolojiden bahesedip de İkinci Dünya Savaşının kaderini değiştiren Enigma' dan bashetmemek olmazdı. Rotor Machine prensibine dayanan Enigma, Alman Arthur Scherbuis tarafından geliştirilmiş bir şifreleme aracıdır. Kauçuk, lastik gibi elektriği iletmeyen bir maddeden yapılan Rotor bir buz hokeyi diski boyutlarındadır. Bu disk veri girişi ve çıkışı için iki ayrı levhadan oluşmuştur. Hem veri girişi levhası hem de veri çıkışı levhasında diski

çevreleyen eşit olarak bağlanmış 26 bağlantısı vardır. Veri girişi levhasındaki 26 bağlantı rotorun veri çıkışı levhasındaki 26 bağlantı noktasına rastgele bağlanmaktadır. Makinenin tüm gizemli kısmını da zaten rastgele oluşturulmuş bu bağlantılar sağlamaktadır. İkinci Dünya Savaşında İngilizler Almanların enigma ile şifrelenmiş belgelerini çözümleyemediler. Bir İngiliz baskıyla bir enigma aracının İngilizlerce bulununcaya kadar enigmanın sırrı çözülemedi. Enigma ile şifrelenmiş bilgileri kırmayı başaran İngilizler Almanların şüphelenmemesi için bir sonraki Alman saldırısına izin verdiler. Almanlar ne olduğunu dahi anlayamadan İngilizler savaşı lehlerine çevirmeyi başardılar. Bu da kriptolojinin ve şifreleme mekanizmalarının önemi üzerine sizlere bir fikir verebilir.

Burada bahsedilmesi gereken önemli bir diğer terim de "Güvenli Sistemler" dir. İki çeşit güvenli sistem vardır: Koşulsuz Güvenli Sistemler(Unconditionally Secure Systems) Matematiksel olarak Güvenli Sistemler(Computationally Secure Systems)

Eğer şifrelenmiş metin, boyutu ne olursa olsun, şifrelenmemiş metni oluşturmak için yeterli bilgiyi içermiyorsa bu tür sistemler Koşulsuz Güvenli Sistemler olarak adlandırılmaktadır. Şifrelenmiş metni kırmanın maliyeti şifrelenmemiş metnin değerinden fazlaysa ve/ve ya şifrelenmiş metni kırmak için gereken zaman bilginin geçerlilik süresinden fazlaysa da, bu tür sistemler Matematiksel olarak Güvenli Sistemler olarak adlandırılır.

Ayrıca şunu da belirtmekte yarar var ki, bu ve bundan sonraki makalelerimizde geçecek olan düz metinden (plain text) kastımız, şifrelenmemiş metindir.

Son Söz

Bu yazımızda kriptolojiye ve alt dalları olan kriptografi ve kripto analize basit anlamda bir giriş yaptık. Sistem güvenliğinin temelini oluşturan kriptolojinin köklü bir geçmişi olduğundan bahsettik. Yüzyıllardan beri süregelen bu alandaki araştırmaların teknoloji ile birlikte daha da gelişeceğini ve gelecekteki bir çok olaya damgasını vuracağını söyleyebiliriz. Burada bahsi geçen şifreleme tekniklerini daha sonraları çokca detaylandıracağız.

suphiucar@yazgelistir.com - yemre@yazgelistir.com
Suphi UÇAR – Yunus Emre ALPÖZEN

Referanslar

Stallings. William. 1995. Network and Internetwork Security Principles and Practice. Prentice Hall. New Jersey.

Yazar : Yunus Emre ALPÖZEN