

I. Kriptografiye Giriş

I.I Kriptografi ve Uygulamaları

Kriptografi

Kriptografi şifreleme bilimi ve sanattır, bilgileri normal formlarından anlaşılabilir formlara dönüştürür. En azından, başlangıcı böyledir. Şimdilerde, kimlik doğrulama, dijital imzalar, ve başka pek çok temel güvenlik fonksiyonunu da içerecek şekilde genişlemiştir.

Kriptografi aşırı miktarda çeşitlilik gösteren bir alandır. Kuantum fiziğinden DNA incelemelerine, kriptografi ile alakalı olan pek çok bilimsel disiplin vardır. Bu yüzden dünyada kriptografi ile ilgili her şeyi bilen hiç kimse yoktur. Hatta çoğunluğunu bilen biri dahi yoktur.

Kriptografi tek başına bir hayli gereksizdir. Daha büyük bir sistemin bir parçası olmalıdır. Kriptografi gerçek dünyadaki "kilit" benzeri bir şeydir. Kilit kendi başına son derece anlamsızdır. Kriptografi güvenlik sisteminin ufak bir parçası olsa da, son derece kritik bir parçasıdır. Kriptografi kilidin görevini üstlenir: "iyi" ulaşım ve "kötü" ulaşımı ayırt edebilmelidir. Bu herkesi dışarda tutmaktan çok daha zordur.

Kriptanaliz

Kriptanaliz çözüme kriptografinin tersidir, şifrelenmiş mesajların anlamını bulmak için çalışır.

Kriptografi ve kriptanaliz bazı zamanlar Kriptoloji çatısı altında toplanırlar (Kriptoloji = Kriptografi + Kriptanaliz). Pratikte, kriptografi bu alanın tamamını ifade etmekte de kullanılır.

Kriptografi Tarihi

Kriptografi 4000 yıl öncesine dayanan inanılmaz bir geçmişe sahiptir. Bir yazıtın anlamını karmaşıklaştırma çabasının ilk örneği Mısır'da görülmüştür. Kriptografi tarihindeki ilk kayda değer isim muhtemelen Julius Caesar'dır (100-44BC), kendisi resmi işler için "İkame Şifresi"ni kullanmıştır. O zamanlarda, şifreleme genel olarak "kağıt kalem" ile yapılmaktaydı, bu yüzden metodlar geçici, basit ve verimsizdi. 1900'lü yıllarda, "rotor" adı verilen mekanik aletlerin bulunması daha sofistike ve sistematik kriptografi tekniklerine imkan sağladı.

Whitfield Diffie tarafından "Uygulamalı Kriptografi" (Bruce Schneier tarafından yazılmıştır) kitabının önsözünde yazıldığı üzere, Birinci Dünya Savaşına kadar, önemli gelişmeler zamanında ortaya çıkmamıştır ve kriptografi bilimi de diğer pek çok özelleşmiş disiplin gibi geride kalmıştır. 1918'de başlamak üzere, kriptografinin kilometre taşları aşağıdaki gibidir (David Kahn'ın kitabından daha detaylı bir tarihi edinilebilir):

1918: William F. Friedman'ın monografı "The Index of Coincidence and Its Applications in Cryptography" bir araştırma raporu olarak çıktı.

1918: Edward H. Hebern ilk rotor makinesinin patentini aldı.

1933: Almanlar tarafından İkinci Dünya Savaşında kullanılan **Enigma** makinesi, Marian Rejewski tarafından kırıldı.

1949: Claude Shannon'un "The Communication Theory of Secrecy Systems" araştırması Bell Systems teknik dergisinde yayınlandı.

1967: David Kahn'ın kriptografi tarihi kitabı, "Codebreakers" yayınlandı.

1970: IBM'de Horst Feistel ileride ABD **DES** (Data Encryption Standard) olarak anılacak çalışmalarına başladı.

1976: Whitfield Diffie ve Martin Hellman "New Directions in Cryptography" açık anahtarlı kriptografi fikrini üretti.

1978: Açık anahtarlı kriptografinin ilk kullanımı, **RSA** algoritması "Communications of ACM" dergisinde yayınlandı.

1991: Phil Zimmermann açık anahtarlı şifreleme programı PGP'yi kaynak kodu ile birlikte Internet'te yayınladı. Zimmermann PGP'yi yayınladığı için senelerce soruşturmadan geçti.

2001: Bir yarışmadan sonra, Rijndael algoritması **AES** (Advanced Encryption Standard) seçildi.

2005: **FIPS** (Federal Information Processing Standards) hash fonksiyonlarından biri olan SHA-1 kırıldı.

Kriptografi Uygulamaları

Tarihsel olarak, kriptografinin ana amacı gizliliği sağlamaktır. E-banka ve e-ticaret uygulamalarının artışı ile, kriptografinin bütünlük korumada kullanımı gizlilik korumadaki kullanımını geçmiş durumdadır. Mesela, elektronik fon transferlerinde, uygun kriptografik karşı tedbirler olmadan, tek bir bitteki bir hata bile milyonlarca doların yanlış olarak çekilmesine veya yatırılmasına sebep olabilir.

Pek çoğunuz zaten kriptografinin Internet'te ne kadar yaygın kullanıldığını en azından SSL, SSH, S/MIME vb. kısaltmalar sayesinde biliyorsunuz. Belki daha az bilinen kriptografinin şu anda kullandığımız neredeyse her elektronik alette olduğu gerçeğidir (mobil telefonlar, ödemeli TV dekodeerleri, oyun konsolları, araba anahtarları, kapı ulaşım kartları, hırsız alarmları vb.)

Kriptografi ayrıca kimlik doğrulama problemi ile de yakından alakalıdır. Örneğin, mevcut doğrulama sistemlerinde şifre güvenliğini güçlendirmek için kullanılması neredeyse bir standart olmuş durumdadır.

Dijital imzalar, dijital para ve bazı diğer uygulamalar iste Internet kullanıcılarına adapte olma sürecindedir. Başka daha egzotik kriptografi uygulamaları e-müzayede, e-oy verme, e-pasaportlar ve başka bazı e'leri içerir.

Soru: Sizce kriptografi ileride çamaşır makinelerinde bile kullanılacak mıdır?

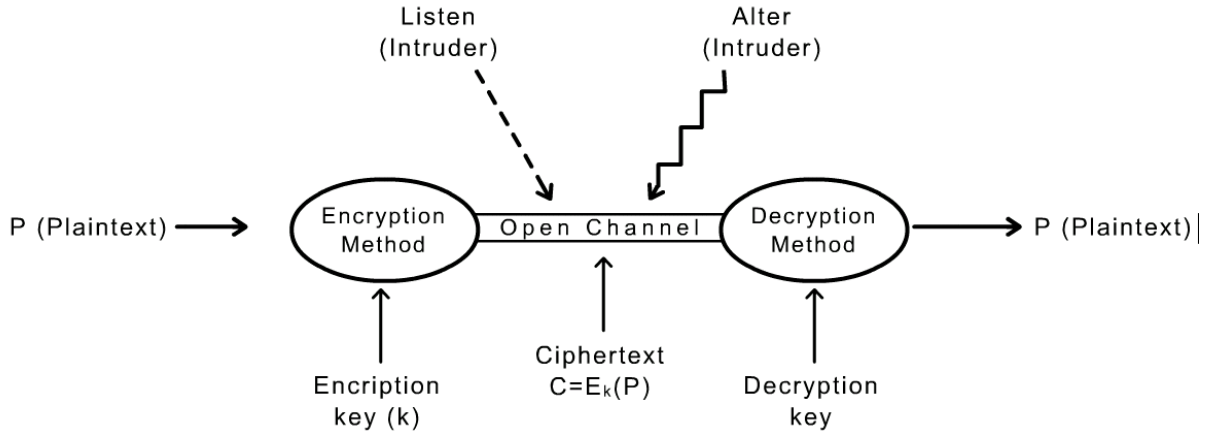
Genel Düzen

AşağıdakiThe animation on the right shows the general setting of (secret-key) cryptography for secrecy (confidentiality). şekil kriptografinin gizlilik için genel düzenini göstermektedir.

Şifreleme mesajın çıkış formatının üçüncü kişilere bir anahtar olmadan anlam ifade etmeyecek şekilde bir işlemden algoritmik olarak geçirilmesidir. Şifre Çözme şifrelenmiş bir mesajı aynı anahtarı kullanarak orijinal formuna döndürme işlemidir. Şifreleme rastgele yapılan bir işlem değildir, tam aksine orijinal mesajın geri getirilebilmesi için alakalı bir geri getirme işlemine sahip olmalıdır. Kriptografi terminolojide mesajın kendisine düz metin (plaintext), şifreleme sürecinin çıktısına şifre metin (ciphertext) ve değişimde kullanılan kriptografik metoda (veya donanıma da) şifre (cipher) denir. Burada kriptografik algoritma veya metod gizli tutulmaz, halka açılır. Diğer taraftan anahtar sadece iki taraf tarafından bilinir.

Düzmetin, şifre metin ve anahtarları ilişkilendirmek genelde faydalı bir yoldur. $C = EK(P)$ formülünün düzmetin P'nin anahtar K ile şifre metin C'yi verdiğini varsayalım. Benzer bir şekilde, $P = DK(C)$ C'nin şifresinin çözülmesinin düzmetini vereceğini gösterir. Bu da demektir ki

$$DK(EK(P)) = P$$



Kerckhoff Prensipleri

1883'te Kerckhoff askeri şifrelemenin standartlarını belirledi. Şifreleme tekniğinin güvenliğinin algoritmanın değil anahtarın gizliliğinden kaynaklanması gerektiğini söyledi. Sebepleri ise şöyleydi:

- Algoritmaları değiştirmek ve gizli tutmak zordur.
- Ufak bir hata ile kriptografik bir algoritmayı güçsüz kılmak son derece olasıdır, bu yüzden standartlaşma ve kamusal algoritmaların açıklığı daha iyi bir süreçtir.