BİLGİ GÜVENLİĞİNİN TEMEL YAPI TAŞI: KRİPTOLOJİ

Erdinç AVAROĞLU
Doç. Dr.,Mersin Üniversitesi Bilgisayar Mühendisliği
eavaroglu@mersin.edu.tr

Özet

Günümüzde teknolojinin hızlı gelişimiyle birlikte, elektronik ortamlarda bilginin iletimi ve paylaşımı dünyanın bir ucundan diğer ucuna anlık olarak yapılmaya başlamıştır. Bu hızlı gelişmeler sonrasında, bilgiye ulaşmak ve bilgiyi paylaşmak kolay hâle gelmiş, ancak doğru bilgiye güvenilir kaynaktan nasıl ulaşılacağı ve bilginin güvenliği sorunu ortaya çıkmıştır. Bu sorunların ortadan kalkması ise bilgi güvenliğinin temel yapı taşı olan kriptolojiye dayanmaktadır. Bu amaçla çalışmada, bilgi, bilgi güvenliği ve kriptoloji konularına odaklanılmıştır.

Anahtar kelimeler: Bilgi, Bilgi Güvenliği, Kriptoloji

Giriş

Teknolojinin baş döndürücü bir hızda gelişimi ile birlikte, özellikle internet teknolojisinin getirdiği kolaylıklar sayesinde insanların hayatı kolaylaşmakta ve günlük hayatlarında birçok değişiklik meydana gelmektedir. Nesnelerin interneti, yapay zekâ, büyük veri gibi teknolojilerinde hayatımıza girmeye başlaması ile birlikte insanların yaşam tarzının hangi boyutlarda değişeceğini tahmin etmek mümkün olmayacaktır. Bilgi teknolojilerinde meydana gelen bu tarz yenilikler insanlığın bilgi sistemlerine olan bağımlılığı arttırmaktadır.[1,2]

Bilgi teknolojilerine yönelik artan bu bağımlılık, sunulan birçok hizmette güvenlik önlemini ön plana çıkarmıştır. Özellikle, internet üzerinde gerçekleşen internet bankacılığı işlemleri, sosyal medya hesapları, sanal ortamda alışveriş, mesajlaşma gibi uygulamalarda kullanılan bilginin güvenliği en önemli sorun haline gelmiştir. Şunu unutmamak gerekir ki internet üzerinde yüzde yüz güvenlik mümkün değildir. [1,2]

Bilgi güvenliğinin sağlanması için, yazılım, donanım, ağ iletişim, personel eğitimi ve tabii ki en önemlisi kriptoloji gibi unsurların gözönünde tutulması gerekir. Bu unsurlar arasında, bilgi güvenliğinin temeli kriptolojiye dayanmaktadır. Kriptoloji, gizlilik, veri bütünlüğü, kimlik doğrulama ve inkâr edememe gibi güvenlik ilkelerini sağlamak için matematiksel yöntemlerin bir araya getirilmesidir.

Çalışmanın ikinci bölümünde bilgi ve bilgi güvenliği hakkında bilgi verilmiştir. Üçüncü bölümde ise bilgi güvenliğinin temeli olan kriptolojiden bahsedilmiştir. Dördüncü bölümde ise sonuç verilmiştir.

Bilgi ve Bilgi Güvenliği

Bilgi güvenliği, bir bilgiye izinsiz erişilmesi, değiştirilmesi, yok edilmesi ve başka kişilerin eline geçmesini önlemek olarak tanımlanabilir. Bilgi güvenliği kavramının iyi anlaşılabilmesi için

bilgi teknolojilerinin girdisi olan bilginin tanımının yapılması gerekmektedir. Bilginin İngilizcedeki karşılığı data, information ve knowledge olarak geçmektedir. Bu terimler dilimizde veri, bilgi ve malumat olarak kullanılmaktadır. [3]

Veri: Sayısal ve mantıksal her bir değere (rakam, harf, sembol) veri veya data denir. Kısaca, işlenmemiş bilgiye veri denir. Örneğin: Mersin, Üniversite,1992.

Bilgi: Verinin işlenmiş veya anlamlı hale getirilmiş haline bilgi denir. Örneğin: "Mersin Üniversitesi 1992 yılında kuruldu."

Malumat: Tecrübe etme, öğrenme şeklinde veya kendi kendine gözlem ile elde edilen gerçeklerin veya bilgilerin farkında olunması olarak tanımlanabilir.

Bilgi Tablo1'de görüldüğü üzere bilgi; fiziksel ortamda, elektronik ortamda, sosyal ortamda ve tanıtım platformlarında bulunabilir.

Tablo1. Bilginin bulunduğu ortamlar [3]

Fiziksel Ortamlar	**Elektronik Ortamlar**
Kağıt, Tahta Pano, Yazı tahtası Faks kağıdı Çöp/Atık Kağıtlar Dosyalar Dolaplar	Bilgisayarlar, mobil iletişim cihazları, pano, yazı tahtası e-posta, USB, CD, disk disket manyetik ortamlar
Sosyal Ortamlar	**Tanıtım Platformları**
Telefon görüşmeleri Muhabbetler Yemek araları Toplu taşıma araçları Facebook Twitter Whatsapp	İnternet siteleri Broşürler Reklamlar, Sunumlar Eğitimler, Görsel sunumlar

Bilginin korunacak nitelikleri Tablo 2'de gösterilmiştir. Bunlar "Gizlilik", "Bütünlük" ve "Erişilebilirlik"tir. [2,3]

Tablo 2. Bilginin Korunacak Nitelikleri		
Gizlilik	**Bütünlük**	**Erişebilirlik**
Bilginin içeriğinin gizli kalmasıdır	Bilginin içeriğinin iletimde değiştirilememesidir	Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi konusuna değindikten sonra peki bu bilgi güvenliği nedir? Bilgi güvenliği, bilginin saklandığı bilgi sistemlerinin ve sistemlerin içerdiği bilginin yetkisiz kullanımına, değiştirilmesine, okunabilmesine veya yok edilmesine karşı korunması ve gereken bütün tedbirlerin alınması olarak tanımlanabilir. Bilgi güvenliğinin temel amacı [3]:

- Bütünlük,
- Erişilebilirlik,
- Gizlilik
- Kimlik Doğrulama
- Sistemin devamlılığının sağlanmasıdır

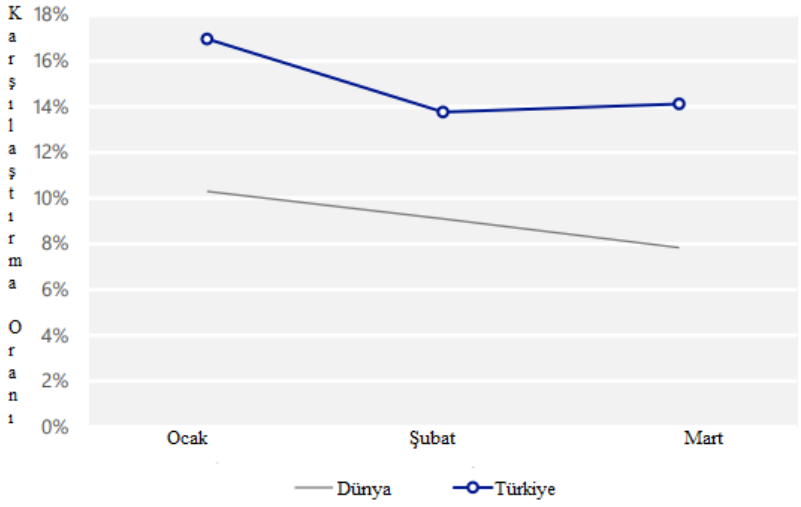
Peki, Türkiye'de bilgi güvenliği ne durumdadır?

Türkiye'de Bilgi Güvenliği

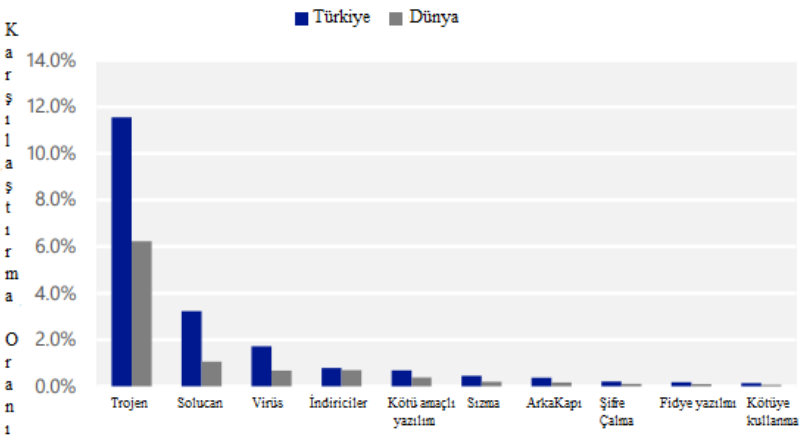
Mart 2017 tarihinde yayınlanan son Microsoft Güvenlik İstihbarat raporuna göre [4,5], Türkiye'deki bilgi güvenliğine ait verilen veriler iç açıcı gözükmemektedir. Bu rapor, dünya çapında en geniş veri kümesine sahip ve milyonlarca kullanıcının bilgisayarından kişilerin izinleri ile paylaşılan sonuçlara göre üretilmektedir.

Mart 2017'de dünyada kötücül yazılım bulunan bilgisayarların oranı % 7.8 iken bu oran Türkiye'de % 14.1 olmuştur. Şekil 1'de rapora göre son 3 ay içerisinde bir bütün olarak tüm dünya ile kıyasladığında Türkiye'deki zararlı yazılım bulaşma eğilimleri gösterilmektedir.

Şekil 1. Türkiye'de ve dünyada zararlı yazılım bulaşma eğilimleri



Şekil 2. Türkiye'de ve dünyada karşılaşılan zararlı yazılım kategorileri

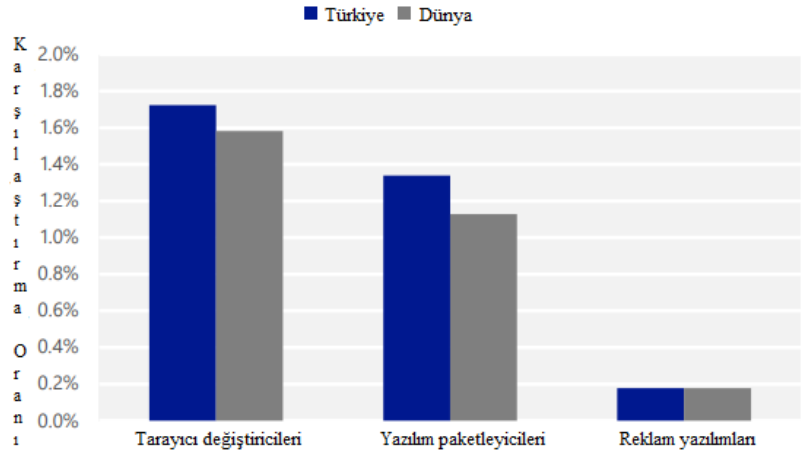


Şekil'de gösterildiği üzere Türkiye'de en yaygın karşılaşılan zararlı yazılım kategorisi trojenler olmuştur. Şubat 2017'de bu oran yüzde 10.45 iken Mart 2017 de bu oran yüzde 11.55 olmuştur.

İkinci en yaygın karşılaşılan zararlı yazılım kategorisini solucanlar oluşturmuştur. Şubat 2017'de bu oran yüzde 2.43 iken Mart 2017

de bu oran yüzde 3.23 olmuştur. Üçüncü olarak da virüsler 1.57'lik orandan 1.72 orana yükselmiştir.

Şekil 3. Türkiye'de ve dünyadaki istenmeyen yazılım kategorileri



Şekil 3'te görüldüğü üzere, Mart 2017'de Türkiye'de en yaygın istenmeyen yazılım kategorisi Tarayıcı Değiştiricileri oldu. İkinci en yaygın istenmeyen yazılım kategorisi Yazılım Paketleyicileri oldu. Üçüncü olarak istenmeyen yazılım kategorisi Adware olmuştur. Adware İngilizce açılımı ile advertising-supported software yani reklam destekli yazılım olarak ifade edilmektedir. En son 2018 yılında çıkan Microsoft güvenlik raporuna göre zararlı yazılımların birçoğu botnetler aracılığıyla yayılmakta, saldırganlar kolay bir yöntem olan kimlik avı gibi yöntemleri tercih etmekte; fidye yazılımları ile hızlı ve zarar verecek türde saldırılar gerçekleştirmektedir. Peki, bu tür saldırılar için nasıl önlem alabiliriz:

- Bilgisayarları kötü amaçlı yazılımarladan (Gamarue gibi) korumak için, genel ve sezgisel tekniklerinin yanı sıra gelişmiş makine öğrenim modelleri uygulayan güvenlik çözümleri kullanılmalıdır.
- İnsanlar genellikle bilgi güvenliğinin en zayıf halkası olarak görülür ancak doğru çalışma ve eğitim ile ilk savunma hattını oluştururlar.

- Bulut uygulamaları kullanılırken, yalnızca web oturumu koruması ve şifrelenmesine izin verilen uygulamaların kullanılmasına izin verilmelidir.
- Fidye yazılımı saldırılarına karşı alınacak en önemli önlem verilerin yedeklerinin alınmasıdır. Dosya yedekleme ve geri yükleme konusunda yardım edebilecek birçok uygulama bulunmaktadır. Ayrıca, yedeklerininizin çalıştığı düzenli olarak test edilmelidir.
- E-postaları ve e-postalara eklenen dosyaları tarayacak bir e-posta güvenlik çözümüne sahip olunmalıdır. En azından bir antivirüs programı, fidye yazılımının indirilmesi ve kurulması işlemlerini tespit edebilir ve engelleyebilir. Ancak bu tarz saldırıları engellemek için ek güvenlik korumaları gerekebilir. Bu tarz kötü amaçlı yazılımları tespit etmek için makine öğrenimi ve yapay zekâ teknolojilerini kullanan gelişmiş tespit önleme (koruma) sistemleri yardımcı olabilir.
- Fidye yazılımlarını giriş noktalarını en aza indirmek için işletim sistemi, web tarayıcı ve güvenlik yazılımları mutlaka güncel olmalıdır.
- Tüm sistemlerde benzersiz yedek yönetici şifreleri tanımlanmalıdır ve ayrıcalıklı hesapların korunması gerekmektedir.
- Eğer bilgisayarlarınızı son yazılım sürümlerine güncellemezseniz ve yamalarını yüklemezseniz, bu bilgisayarları internet ortamında izole edilmelidir.

Yukarıda bahsedilen önlemler ile bilgisayarınızın ve verilerinizin güvenliği belirli oranda sağlanabilmektedir. Ancak, internet ortamında iletilen bilginin gizlilik, bütünlük, kimlik doğrulama ve erişebilirliğinin sağlanması kriptolojik uygulamalar ile sağlanmaktadır.

Kriptoloji

Kriptoloji kelimesi, köken olarak eski Yunanca'da yer alan "kryptos logos" kelimelerinden gelmektedir. "kryptos" kelimesi "gizli dünya" anlamını, "logos" ise sebep-sonuç ilişkisi kurma, mantıksal

çözümleme alanı anlamını taşımaktadır. Kriptoloji, gönderici ve alıcı arasında gerçekleşen haberleşmenin güvenli olarak yapılmasını sağlayan, temelde matematiksel zor problemlere dayanan teknik ve uygulamaların bir bütünü olarak tanımlanmaktadır. Elektronik, matematik ve bilgisayar bilimleri gibi birçok alanı içeren bir bilim dalı olarak kullanılmaktadır. Kriptolojinin iki temel alanı bulunmaktadır. Bunlar kriptografi ve kriptoanalizdir [1].

Kriptografi, güvenli olduğu varsayılan bir haberleşme kanalı üzerinde gönderici ve alıcı arasında gerçekleşen iletişimin gizli olarak yürültülmesini sağlar. Kriptografi, şifreleme ve şifre çözme işlemini gerçekleştirmek için matematiksel fonksiyonlar kullanmaktadır. Kriptoanaliz ise, şifrelemede kullanılan anahtara sahip olmadan şifre çözme yöntemlerinin denenmesidir.

Kriptoloji çok eski çağlardan beri insanoğlu tarafından kullanılmaktadır. M.Ö.1900 yıllarda Mısır'da başlayan ve günümüze kadar olan gelişmeler Tablo 3'te gösterilmiştir.

Tablo 3. Kriptolojinin Tarihsel Gelişimi [6]

Tarih	Açıklama
M.Ö. 1900	Mısırda bulunan kitabelerdeki hiyeroglif işaretlerin kullanılması
M.Ö 60-50	Julius Cesear tarafından kullanılan alfabedeki harflerin 3 harf sonraki harfle değiştirilmesine dayanan şifreleme sistemi devlet haberleşmesinde uzun süre kullanılmıştır.
1000-1200	Gazneliler döneminde devlet makamlarında görev alacak olan kişilere yeni görev yerlerine giderken özel anahtar verilmesinden bahsedilmektedir.
1856	Blaise de Vigenère tarafından şifreleme kitabı yazılmıştır. Açık metin ve şifreli metin için anahtarlama yönteminden bahsedilmiştir ve halen kullanılmaktadır.
1623	Francis Bacon 5-bit ikili kod kullanarak karakter tipi değişikliği ile stenografiyi buldu.
1790	Strip cipher makinesi Thomas Jefferson tarafından

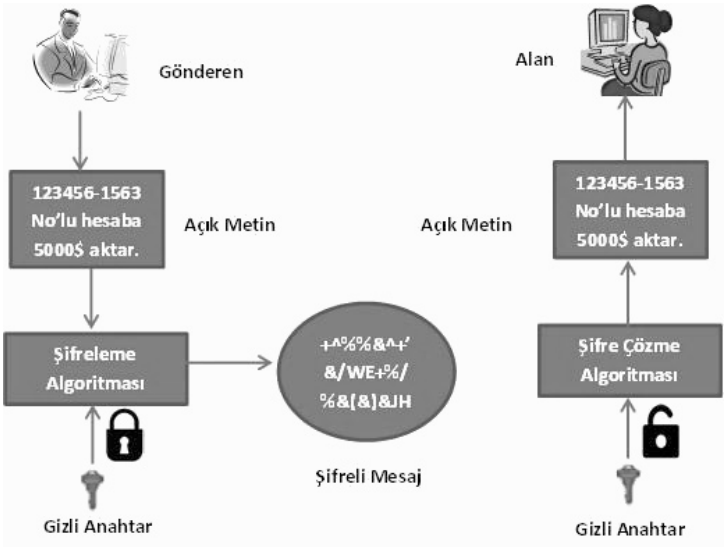
	geliştirildi ve 2.dünya savaşında ABD donanması tarafından kullanıldı.
1917	Tek yönlü şifreleme sistemi "One Time Pad" Joseph Mauborgne ve Gilbert Vernam tarafından geliştirildi.
1920-1930	William Frederick Friedman kendisinin kurduğu Riverbank Laboratuarlarında ABD için kriptoanaliz yaptı ve bunu 2. Dünya Savaşı'nda Japonların Purple Machine şifreleme sistemini çözmek için kullandı.
1945	2. Dünya Savaşı'nda Almanlar şifreleme için Enigma makinesini kullandı. Ancak, Alan Turing ve ekibi tarafından sistem çözüldü ve savaşın seyrini değiştirdi.
1952	ABD'de Ulusal Güvenlik Teşkilatı (NSA) kuruldu
1970	DES'in temeli olan Lucifer algoritması geliştirildi.
1976	DES, ABD tarafından şifreleme standardı olarak kabul edildi.
1976	Açık anahtar sisteminden Whitfield Diffie ve Martin Hellman tarafından ortaya konmuştur.
1978	Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular
1985	Eliptik eğri kriptografik (ECC) sistemleri Neal Koblitz ve Victor S.Miller tarafından çalışıldı.
1990	İDEA algoritması bulundu.
1991	Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı
1995	SHA-1 (*Secure Hash Algorithm*) özet algortiması NIST tarafından standart olarak yayınlandı
1997	ABD'nin NIST *(National Institute of Standards and Technology*) kurumu DES'in yerini alacak bir simetrik algoritma için yarışma açtı.
2001	Belçikalı Joan Daemen ve Vincent Rijmen'in geliştirdiği Rijndael algoritması NIST'in yarışmasını kazanarak, algoritma AES (*Advanced Encryption Standard*) adıyla standart haline getirildi
2005	Çin'li bir ekip tarafından SHA-1 algoritması kırıldı.
2007	SHA-1 algoritması kırıldıktan sonra daha güvenli bir algoritma geliştirmek için kriptografi konusunda ilk olimpiyatlar Belçika'nın Katholieke Üniversitesinde 25-28 Şubat tarihleri arasında yapıldı.

Kriptografi biliminin gelişimi her ne kadar bin yıllar boyunca sürmüş olsa da, asıl ivmelenme, son yüzyılda ve bilhassa bilgisayar çağı olarak nitelendirebileceğimiz son 50 yılda gerçekleşmiştir. Kriptoloji, bilgi güvenliğinin temel yapı taşlarından biridir. Aşağıda şekil 4'de şifreleme ve şifre çözme işlemi gösterilmektedir.

Şekil 4. Şifreleme ve şifre çözme aşamaları

Kriptografi, asimetrik ve simetrik şifreleme yöntemleri olmak üzere iki sınıfa ayrılır. Simetrik şifreleme yönteminde Şekil 5'te gösterildiği gibi tek anahtar kullanılmaktadır. Bu anahtar, "özel/gizli anahtar" olarak adlandırılmaktadır. Anahtar değeri saldırganlardan gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır. Gizli anahtar şifrelenmiş metinle birlikte alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir. DES (*Data encryption system*-veri şifreleme sistemi), AES (*advanced encrpytion system*-gelişmiş şifreleme sistemi) ve *skipjack* bilinen bazı simetrik şifreleme algoritmalarıdır [1].

Şekil 5. Simetrik Şifreleme



Simetrik kriptografinin kuvvetli yönleri aşağıdaki gibi özetlenebilir:

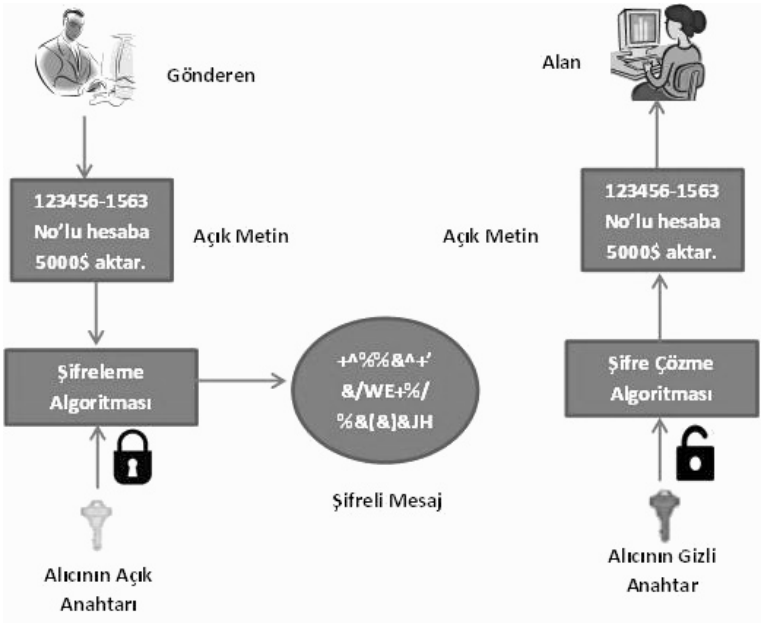
- Kullanılan şifreleme algoritmaları hızlıdır.
- Donanımda uygulanması kolaydır.
- "Gizlilik" sağlar.

Simetrik kriptografinin zayıf yönleri ise aşağıdaki gibidir:

- Ölçeklenebilir değildir
- Güvenli anahtar dağıtımı kolay değildir
- "Bütünlük" ve "Kimlik Doğrulama" gerçeklemek zordur.

Şekil 6'da gösterilen asimetrik kriptografide, iletişimi gerçekleştirecek olan taraflarda biri açık biride özel anahtar olmak üzere iki anahtar bulunmaktadır. Bu iki anahtar birbiri ile bağlantılıdır. Açık anahtar saldırganlarda dâhil olmak üzere herkes tarafından bilinmektedir. Ancak özel anahtar gizli kalmaktadır. RSA, elektronik imza ve özetleme hash algoritmaları bilinen asimetrik şifreleme algoritmalarıdır [1]. Bu sistemi kullanarak haberleşen taraflar aynı şifreleme algoritmasını kullanmaktadırlar.

Şekil 6. Asimetrik Şifreleme



Asimetrik kriptografinin kuvvetli tarafları aşağıdaki gibi özetlenebilir:

- Anahtar yönetimi ölçeklenebilir.
- Kırılması zordur.
- Güvenlik gereksinimleri sağlar.

Asimetrik kriptografinin zayıf yönleri ise aşağıdaki gibidir:

- Asimetrik kriptografi algoritmaları, simetrik kriptografi algoritmalarına göre oldukça yavaştırlar.
- Anahtar uzunlukları bazı durumlarda sıkıntı yaratmaktadır.

Asimetrik ve simetrik kriptografi sistemlerinin özelliklerinin karşılaştırmaları Tablo 3'te gösterilmiştir.

Tablo 3: Simetrik–Asimetrik Kriptografi Karşılaştırması

Konu	Simetrik Kriptografi	Asimetrik Kriptografi
Gizlilik	Sağlar	Sağlar
Bütünlük	--	Sağlar
Kimlik doğrulama	--	Sağlar
İnkâr Edemezlik	--	Sağlar
Performans	Hızlı	Yavaş
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı

Sonuç

Bilgi güvenliğinin temel yapı taşlarından biri olan kriptoloji, eski zamanlardan bu yana bilgi ve veri gizleme yöntemi olarak kullanılmaktadır. Kriptoloji, bigi güvenliği içinde gereksinim olan veri gizliliği, veri bütünlüğü, kimlik doğrulama ve inkâr edilemezlik ilkelerini sağlamaktadır. İnternet kullanımının yaygınlaşması ile birlikte bu gereksinimlerin sağlanması gerektiğinden kriptoloji ile bilgi güvenliği ayrılmaz bir bütün haline gelmiştir. Günümüzde ise kriptoloji, özellikle bilgi sistemlerine erişimin sınırlanması için, şifreli mobil iletişim alanında, e-posta gizliliğinin sağlanması,

elektronik imza gibi alanlarda yaygın kullanılan bir çözüm halini almıştır.

Kaynakça

[1] Avaroğlu, E. (2007).“Elektronik imza”, Yüksek Lisans Tezi, İnönü Üniversitesi,

[2] Güngör, M. (2015).“Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma”, Uzmanlık tezi, Kalkınma Bakanlığı,

[3] http://www.bilgimikoruyorum.org.tr

[4] http://blog.microsoft.com.tr/?p=62403

[5]https://info.microsoft.com/rs/157-GQE-382/images/EN-AU-CNTNT-eBook-Security-GDPR-Microsoft-SIR-Volume-23%5B1%5D.pdf

[6] https://www.wikiturk.net/Madde/56399/kriptolojinin-tarihcesi