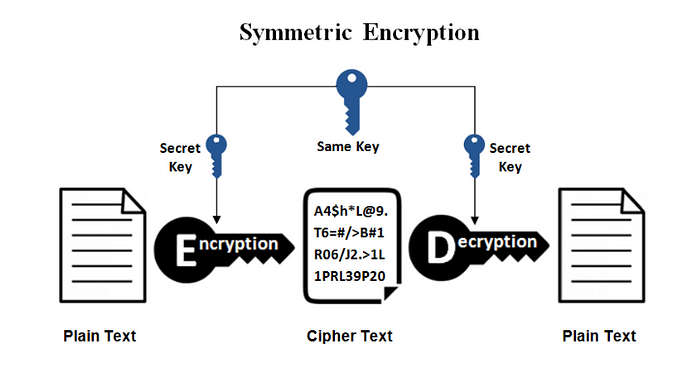
# KRİPTOGRAFİDE SİMETRİK VE ASİMETRİK ALGORİTMALAR

## Simetrik Anahtarlı Algoritmalar

Simetrik şifreleme, bilgileri şifrelemek ve deşifre etmek için yalnızca bir gizli anahtar içeren en basit şifreleme türüdür. Simetrik şifreleme, kriptografi teknikleri ve şifreleme algoritmaları içinde en eski ve en iyi bilinen tekniktir. Bir sayı, bir kelime veya rastgele harfler dizisi olabilen gizli bir anahtar kullanır. Gönderen ve alıcı, tüm mesajları şifrelemek ve şifresini çözmek için kullanılan gizli anahtarı bilmelidir. İşlem süresinin hızlı olması simetrik şifreleme algoritmalarının en önemli avantajlarındandır. Blowfish, AES, RC4, DES, RC5 simetrik şifrelemeye örnektir.



### Blowfish

Piyasada kullanılan en hızlı blok şifreleyicilerdendir. Karmaşık anahtar çizelgesi kullanarak kırılmasını zorlaştırır. Blowfish, 23'den 448 bite kadar anahtar uzunluklarına sahiptir. Çalışabilmesi için 4 kilobyte RAM’den daha fazla belleğe ihtiyaç duyarlar. Bu nedenle en küçük gömülü sistemlerde kullanılamazlar.

### DES (Data Encryption Standart)

Dünyada en çok kullanılan simetrik şifreleme algoritmalarından birisidir. Feistel şifreleme metodunu kullanır. Blok şifreleme kullanan DES, işlem sırasında 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. Anahtar uzunluğunun kısa olması nedeniyle kırılmıştır. Bunun üzerine Triple-DES, (encrypt-decrypt-encrypt)yani 3DES olarak geliştirilmiştir. 3DES, DES’in üst üste 3 kere kullanılmasıdır. Yani normal DES’e göre 3 kat yavaştır ama günümüzde SSH gibi uygulamalarda kullanılır. AES’in çıkması üzerine DES popülerliğini kaybetmiştir. Çünkü AES’e göre 6 kat daha yavaştır.

### AES (Advanced Encrption Standart)

DES kırıldıktan sonra yeni bir arayışa girilmiş ve AES simetrik şifreleme algoritması oluşturulmuştur. DES’in zayıf yönleri kuvvetlendirilmiş halidir ve blok şifreleme algoritmasını kullanır. DES’e göre daha hızlı ve güvenlidir. Uzunluk olarak 128, 192 ve 256 bit anahtarları destekler. DES’e göre anahtar boyu ve block size daha uzundur. Bu da daha güçlü bir anahtar sağlar. Günümüzde de en popüler algoritmalardan birisidir ve brute force saldırılarına karşı dayanıklı olduğu düşünülmektedir.

### RC4 (Rivest Encryption 4)

Şifrelenecek veriyi akan bir bit dizisi olarak algılar. RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır. Genellikle hız gerektiren uygulamalarda kullanılır. Şifreleme hızı yüksektir ve MB/sn seviyesindedir. Güvenliği rastgele bir anahtar kullanımına bağlıdır. Anahtar uzunluğu değişkendir. 128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme olarak kabul edilir. Bankacılık ve Dökümantasyon(PDF) şifrelemelerinde yaygın olarak kullanılır.

### RC5 (Rivest Encryption 5)

Modern şifreleme algoritmaları sınıfında yer almaktadır. 16–32 ve 64 bitli kelime uzunlukları ile çalışabilmektedir. Anahtar boyutu ve döngü sayısı değişken olarak alınabilir. Böylece, yüksek anahtar boyutu ve fazla döngü sayısı ile uzun çalışma zamanı fakat kırılması neredeyse imkansız şifreler; düşük anahtar boyutu ve az döngü sayısı ile kısa çalışma zamanı ve bununla beraber daha güçsüz şifreler arasında seçim yapılabilme olanağını sağlar. Bellek gereksiniminin de düşüklüğü ile cep telefonlarından süper bilgisayarlara kadar her yerde çalışabilir bir algoritmadır.

### TWOFISH

AES kadar hızlıdır. DES gibi Feistel yapısını kullanır. DES’den farkı anahtar kullanılarak oluşturulan değişken S-boxlara(Blok şifrelerde genellikle anahtar ve şifre metni arasındaki ilişkiyi gizlemek için kullanılırlar.) sahip olmasıdır. Metinleri 32 bitlik parçalara ayırarak işleme sokar ve blok algoritması olarak çalışır. Şifreleme ve deşifreleme algoritmalarının birbirinden farklı olması uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını yavaşlatmıştır.

### IRON

Feistel yapısını kullanır. 64 bitlik veri bloklarını 128 bit anahtarla şifreler ve 16 ile 32 döngü sayısında çalışır. Alt anahtarların sayısı döngü sayısına eşittir. Bu nedenden dolayı algoritma anahtar bağımlıdır. Bu algoritmanın avantajı, bitler yerine 16-tabanındaki sayılarda kullanılması, dezavantajı ise yazılım için tasarlanmış olmasıdır.

### IDEA

Açılımı “International Data Encryption Algorithm” olan IDEA bir blok şifreleme algoritmasıdır. Aynı zamanda Ascom tech adlı firmanın tescilli algoritmasıdır. PGP‘nin temelini oluşturan algoritmalardan birisidir. Bilinen en güçlü algoritmalardandır. IDEA, şifrelenecek olan 64 bitlik metin ve 128 bitlik anahtarı kullanarak 64 bitlik şifrelenmiş metni oluşturur.

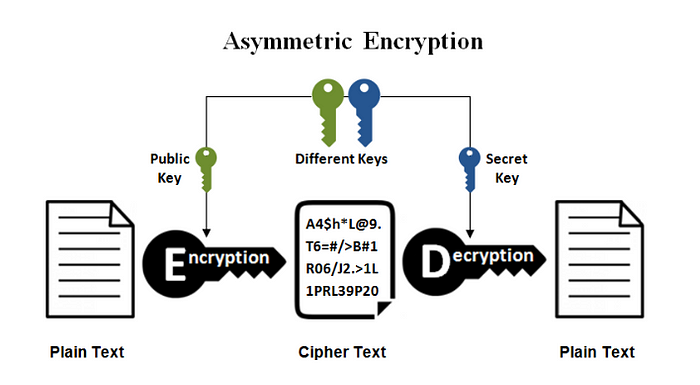
### CAST-128

GPG ve PGP’nin bazı versiyonlarında varsayılan şifre olarak birçok üründe kullanılan simetrik bir anahtar bloğu şifresidir. Kanada Hükümeti’nin kullanımı tarafından kullanılmaktadır. 64 bit blok boyutu ve anahtar boyutu 40 ile 128 bit arasında olan (ancak yalnızca 8 bitlik artışlarla) 12 veya 16 yuvarlak Feistel bir ağdır. Anahtar boyutu 80 bit’ten uzun olduğunda 16 turun tamamı kullanılır.

## Asimetrik Anahtarlı Algoritmalar

Şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık (gizli olmayan) anahtardır. Bu anahtarlardan bir tanesiyle şifreleme yapılırken diğeriyle de şifre çözme işlemi gerçekleştirilir. Bu iki anahtar çifti matematiksel olarak birbirleriyle bağlantılıdır. Gizli anahtarın sadece bir sahibi vardır. Gizli anahtara sahip olan taraf gizli anahtar aracılığıyla, kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir. Açık anahtar herkesin erişimine açıktır. Bu algoritma açık anahtarla şifreleme ve gizli anahtarla deşifreleme yapılmasını kolayca gerçekleştirirken, yalnızca açık anahtarı bilerek gizli anahtarın bulunmasını zor kılar. Bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir.

Açık anahtar altyapısı internet üzerinde güvenli haberleşmeyi sağlayan TLS (SSL’in gelişmiş hali) protokolü, güvenli e-posta haberleşmesinde kullanılan PGP protokolü ve dosya şifreleme ve çözmeye yarayan GPG gibi protokollerde kullanılmaktadır.



### (D-H) Diffie-Hellman anahtar değişimi

Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır. DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür. Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır. Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

### RSA (Rivest-Shamir-Adleman)

Üç bilim adamının baş harflerinden oluşan RSA, dijital imzalama içinde kullanılmaktadır. Güvenilirliği, çok büyük asal sayıların işlem yapma zorluğuna dayanan bir algoritmadır. Günümüzde bankacılık sistemleri ve ticari sistemlerde öncelikli tercih edilen şifreleme tekniğidir. Bu büyük sayılar nedeniyle oldukça güvenilirdir ama işlemler yavaştır. Bu nedenle fazla bant genişliği harcaması yüzünden kablosuz ağ sistemlerinde kullanılması bazı sorunlara yol açabilir.

### El Gamal

Diffie-Hellman anahtar alışverişine dayanan bir açık anahtarlı şifreleme yöntemidir. Anahtar üretimi ve şifreleme/açma olarak iki aşamadan oluşur. Matematiksel zorluk olarak dairesel gruplar üzerindeki ayrık logaritmalara dayanan bir dijital imzadır.

### DSA (Digital Signature Algorithm)

NIST tarafından sayısal imza standardı olarak tasarlanmıştır. DSA algoritması da, RSA gibi açık anahtarlı bir kriptografik algoritmadır. Dijital imza algoritması, ElGamal imza algoritmasının bir varyantıdır.

### Merkle-Hellman

RSA asimetrik şifreleme sisteminden farkı şifreleme işleminin tek yönlü çalışmasıdır. Açık anahtar sadece şifreleme yaparken, gizli anahtar sadece şifre çözme işlemini gerçekleştirir. Bu nedenle de Dijital İmzalama için kullanılamaz. Düşünce olarak RSA’dan daha basit ve zekice olmasına rağmen kırılmıştır.

### (ECC) Elliptic Curve Cryptography

Eliptik Eğri Kriptolojisi (Elliptic Curve Cryptography), sonlu cisimler üzerindeki eliptik eğrilerin cebirsel topolojisine dayanan bir açık anahtar şifrelemesidir. Eliptik eğri kriptografisinin en büyük özelliği depolama ve iletme gereksinimlerini azaltarak daha küçük anahtar boyutuna sahip olmasıdır. Bir eliptik eğri grubu, büyük modülerli ve buna bağlı olarak büyük anahtar boyutlu RSA tabanlı sistem ile aynı güvenlik seviyesi sunabilir. Örneğin; Eliptik eğri ile 256-bitlik anahtar boyutunda elde edeceğimiz güvenliği RSA ‘de 3072-bitlik anahtar ile sağlanabilir. Bu algoritma IHA’larda güvenlik açısından kullanılabilir. Ayrıca ECC smart kartlar,cep telefonları, PDA’lar (personal digital assistant), sayısal posta işaretleri gibi zorunlu ortamlara uygundur.

Bazı güvenlik sistemleri 1024-bit RSA genel anahtarlama planının uygulamasını yaymaya çalışır, çünkü kuruluşlar bunun yeterince iyi olduğunu düşünürler. Bununla birlikte bu tehlikeli bir yaklaşımdır. Çünkü genel anahtarlama sisteminin güvenliği kullanılan simetrik şifrelemeyle birebir eşleşmiş olmalıdır. Tabloda görüldüğü gibi, 1024-bit RSA simetrik şifrelemede kullanılan 128-bit güvenlik seviyesiyle uyuşmuyor.Bu gereksinimi karşılamak yani genel anahtarlama planını eşleştirmek için istenen 3072- bit RSA ya da 256-bit ECC kullanılmasıdır. Bu sayede işlemci gücü, saklama kapasitesi, bant genişliği, güç tüketimi gibi durumlarda RSA’ya göre avantaj sağlar.