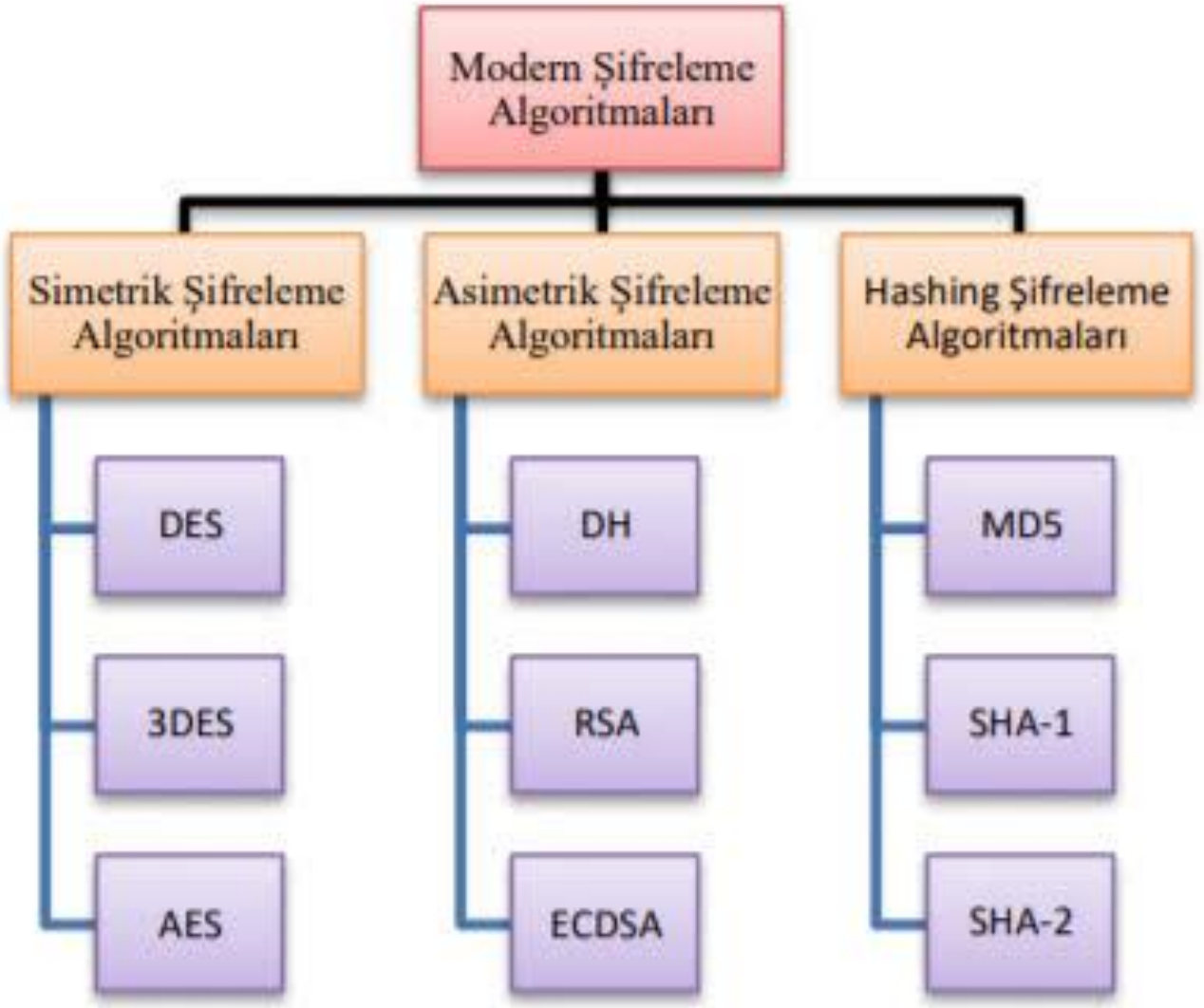
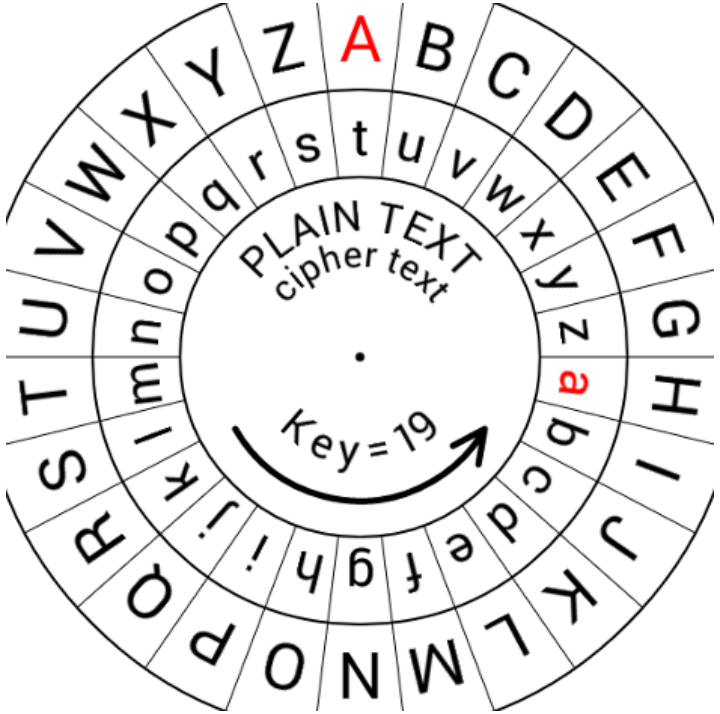
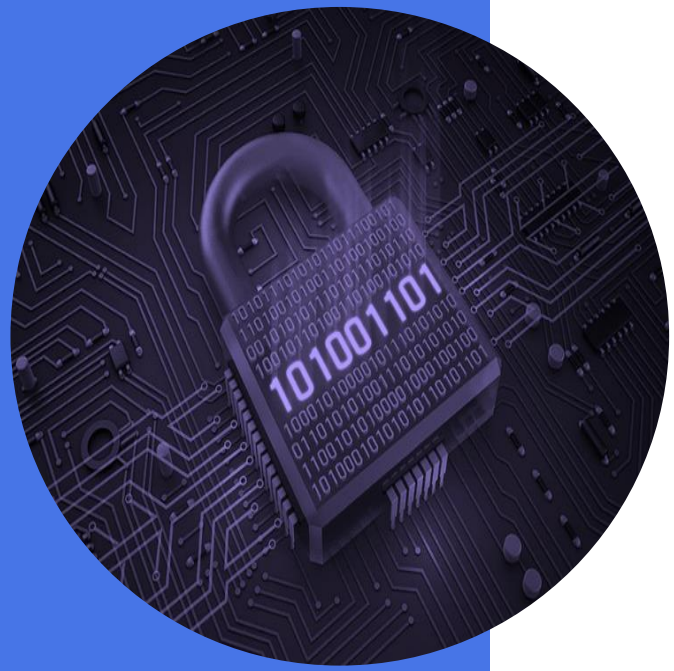

Modern Şifreleme Algoritmaları
Simetrik Şifreleme Algoritmaları
Asimetrik Şifreleme Algoritmaları
Hashing Şifreleme Algoritmaları
DES
3DES
AES
DH
RSA
ECDSA
MD5
SHA-1
SHA-2

# Günümüzde kriptografik sistemler
# Modern Şifrelemeler

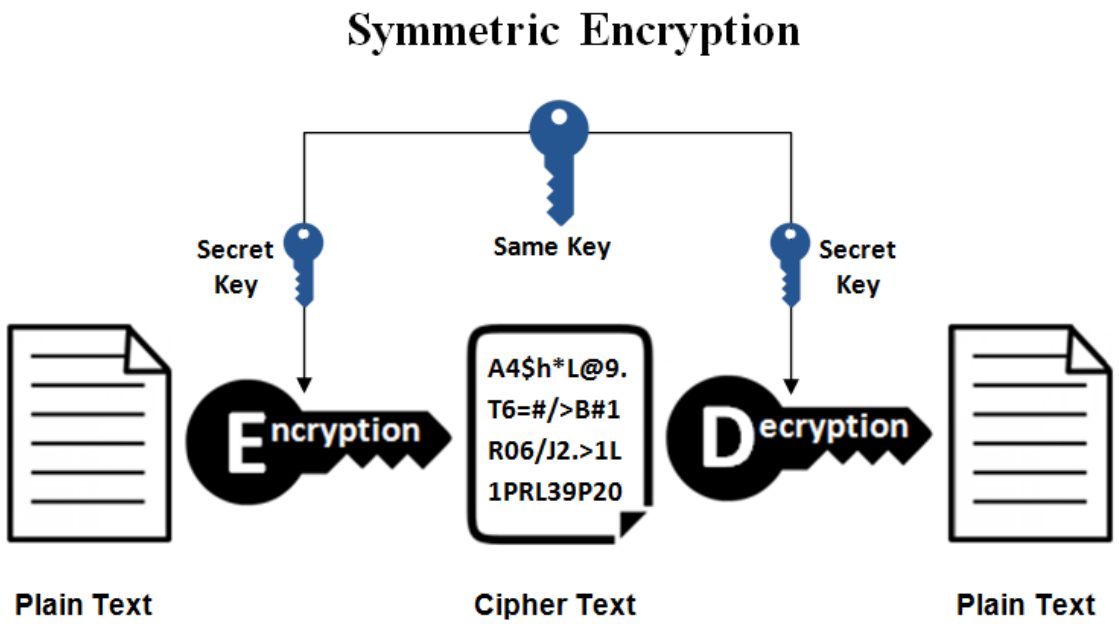



Bugün, kriptografi çok geniş uygulama alanlarına dahil olarak günlük hayatın önemli bir parçası olmuştur:

- sim kartlar,
- cep telefonları,
- uzaktan kumandalar,
- online bankacılık,
- online alışveriş,
- uydu alıcıları,




# Gizli Anahtarlı Şifreleme Yöntemleri




Simetrik şifreleme, elektronik veriyi şifrelemek ve çözmek için sadece tek bir anahtar kullanan şifreleme tipidir. Simetrik şifreleme algoritmaları da kendi içerisinde ikiye ayrılır.

**Blok algoritmalar:** Blok şeklinde olan elektronik verileri özel anahtarı kullanarak bitlerin uzunluğunu belirler. Veri şifrelendiği esnada sistem veriyi bloklar tamamlanana kadar kendi belleğinde tutar.

**Akış algoritmaları:** Veri, sistemin belleğinde durmak yerine akışlar ile şifrelenir.

# Simetrik Şifreleme Algoritmaları

- Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır. Gönderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

# Simetrik Şifreleme Algoritmaları

- Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır. Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır. Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır. Ayrıca simetrik algoritmalarda kullanılan anahtarın boyutu ve dolayısıyla bit sayısı çok daha küçüktür.

# Simetrik Şifreleme Algoritmaları

Kuvvetli Yönleri;

- Algoritmalar olabildiğince hızlıdır.
- Donanımla birlikte kullanılabilir.
- Güvenlidir.

Zayıf Yönleri;

- Güvenli anahtar dağıtımı zordur.
- Kapasite sorunu vardır.
- Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

# Simetrik Şifreleme Algoritmaları

- Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır. Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir. Bazen bağımsız bazen birbirine bağlı olarak şifrelemektedir. Bu algoritmalarda iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır. Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir.

# Simetrik Şifreleme Algoritmaları

- Dizi şifreleme algoritmaları ise veriyi bir bit dizisi olarak almaktadır. Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir. Kayan anahtar üretimi zamana bağlıdır ve bu yüzden bu algoritmalara aynı zamanda hafızalı şifreleme denir. Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır.

# Blok Şifreleme (Block Cipher)

- Şifreleme algoritmalarında kullanılan bir yöntem olan blok şifreleme, açık mesajın (plain text) belirli uzunluklarda bloklara bölünmesi ile çalışır.
- Bu yönteme göre bölünen bütün bloklar ayrı ayrı şifrelenecek ve sonuçta üretilen şifreli metin (cipher text) bu blokların dizilimi ile elde edilecektir.
- En ilkel uygulaması vignere şifreleme yöntemidir.

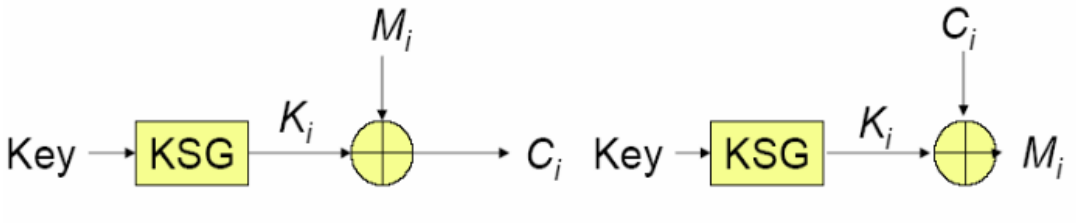
- Örneğin şifrelenecek olan mesaj: “Alibabavekırkharamiler” olarak kabul edilsin ve yöntemimizdeki blok uzunluğu 5 karakter olsun. Bu durumda bloklarımız:

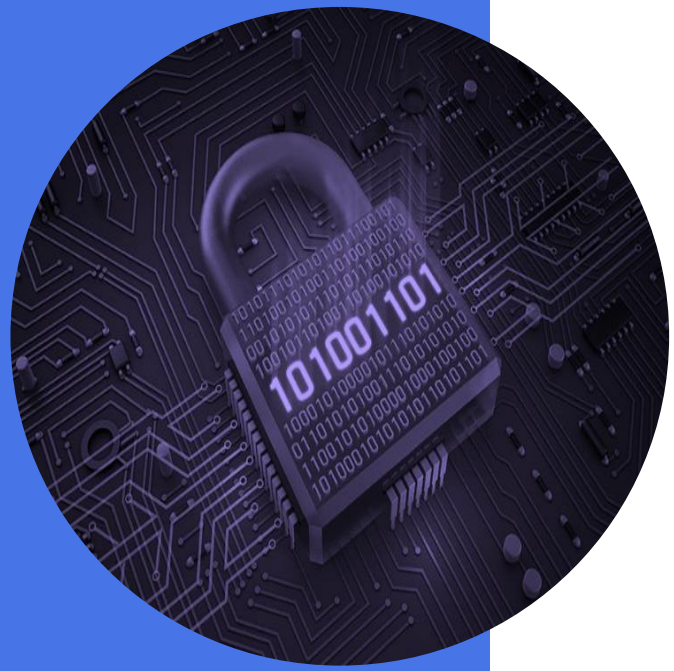
1. aliba
2. bavek
3. ırkha
4. ramil
5. er

- şeklinde olacaktır. Şifreleme yöntemi her bloğu ayrı ayrı şifreleyecek ve çıkan sonuçları birleştirerek şifreli metni elde edecektir.

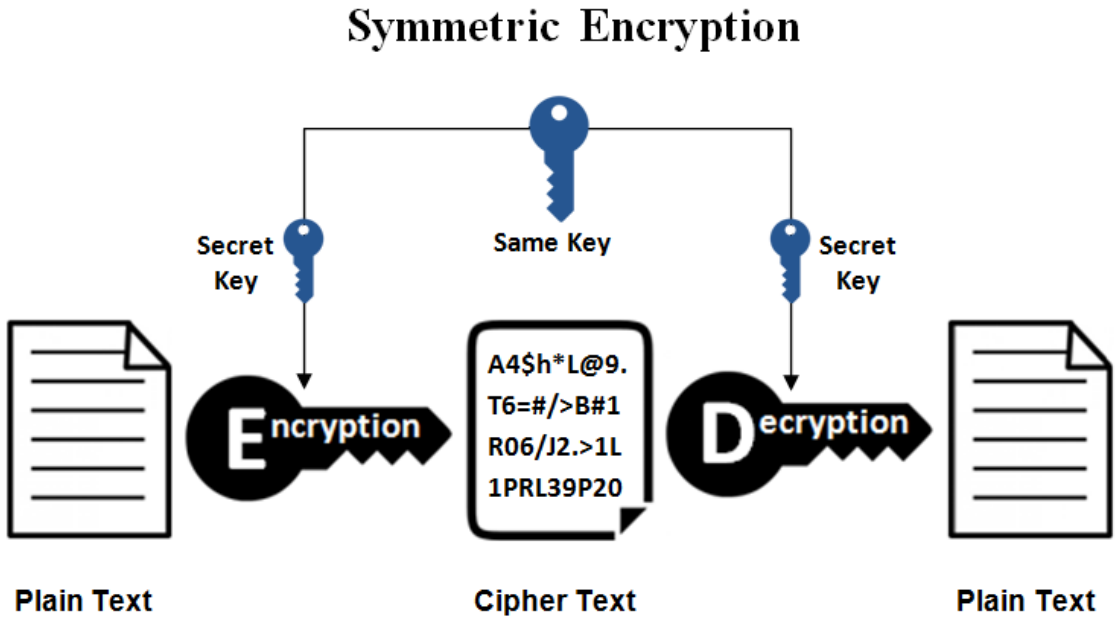
# Dizi Şifreleme (Array Cipher)

- Dizi şifreleme sistemleri gizli anahtarlı şifreleme algoritmalarının önemli bir sınıfını oluşturur.
- Dizi şifreleme sistemleri genel olarak şekilde verilen yapıya sahiptirler. Şifrelenecek olan düz metnin bit dizisi şeklindeki ifadesi olan M dizisinin bir biti ile üretilen anahtar dizisinin bir biti xor işlemine tabii tutularak şifrelenmiş metine ait olan C biti elde edilir. Bu işlem düz metine ait bütün bitler için uygulanarak istenilen şifrelenmiş metin elde edilir.
- Şifrelenmiş metinden düz metin elde edilmek istendiği takdirde ise xor işleminin özelliğinden faydalanarak ; aynı şekilde şifrelenmiş metinin bir biti, biti şifrelemek için kullanılan aynı anahtar biti ile xor işlemine tabii tutulur. Bu işlem şifrelenmiş metine ait bütün bitler için tekrarlandığı takdirde düz metin elde edilmiş olur.






# Gizli Anahtarlı Şifreleme Yöntemleri

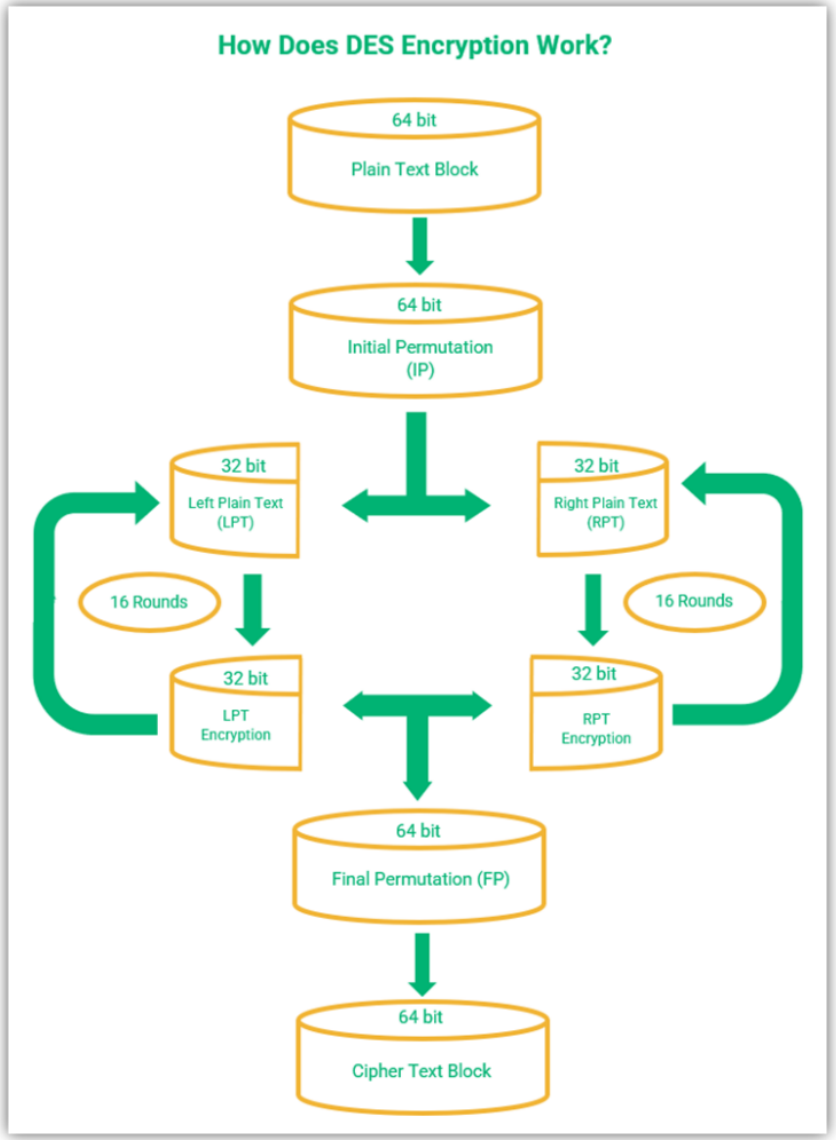



Bazı simetrik şifrelemelere örnek vermek gerekirse;

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- 3DES (Triple DES)
- Blowfish

# DES (Data Encrytion Standard - Veri Şifreleme Standardı)

- Blok şifreleme algoritmasıdır. Şifrelemeyi metin uzunlukları belli olan bloklar halinde gerçekleştirir. DES algoritması 64 bitlik anahtar uzunluğuna sahip olmasına rağmen 56 bit uzunluğunda simetrik kriptolama tekniği kullanan bir sistemdir. Her kullanımında o kullanıma özel yeni bir anahtar oluşturması DES'in güçlü yanı olup, günümüz teknolojisi için algoritmanın yavaş ve 56-bit'lik anahtar uzunluğunun yetersiz kalması DES'in zayıf yönleridir. 2000'li yılların başında kırılmasıyla günümüz teknolojsi için yetersiz kaldığı görülmüştür ve itibarını kaybetmiştir.

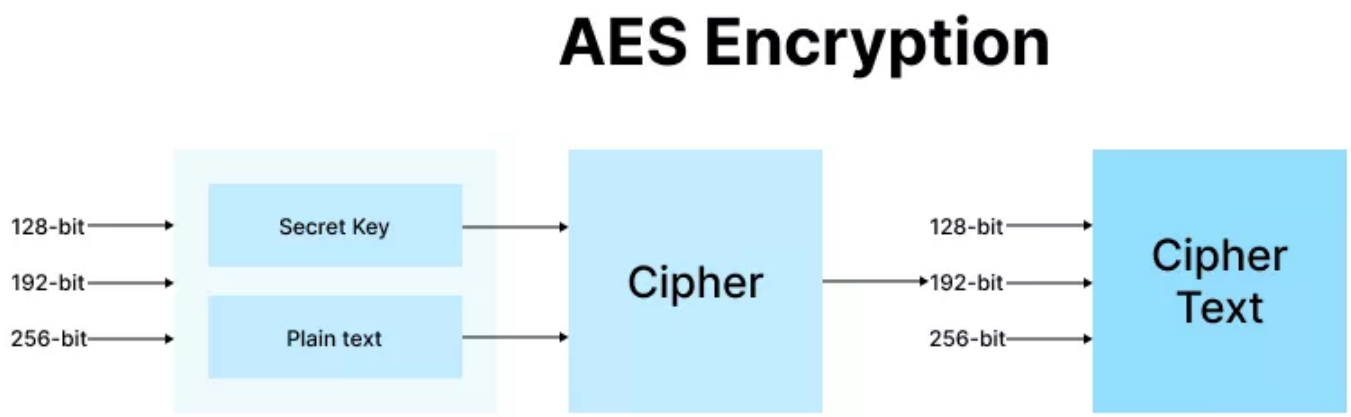


# DES (Data Encrytion Standard - Veri Şifreleme Standardı)

- DES"in algoritmasından kaynaklanan bu sorunlar "Triple DES" ya da "DES-3" olarak bilinen yeni bir algoritma ile düzeltilmiştir. SSH gibi günümüzde kullanılan çoğu uygulama 3DES"i kullanmaktadır. 3DES algoritması DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışır. Bu yüzden DES'e göre 3 kat daha yavaştır. Bununla birlikte 3DES şifreleme yapmak için uzunluğu 24 bayt olan bir anahtar kullanılır. Her bayt için 1 eşlik biti vardır. Dolayısıyla anahtarın uzunluğu 168 bittir. AES'in geliştirilmesiyle etkinliğini kaybetmiştir çünkü daha gelişmiş bir algoritmaya sahip olan AES şifreleme yöntemine göre 6 kat daha yavaş çalışır.

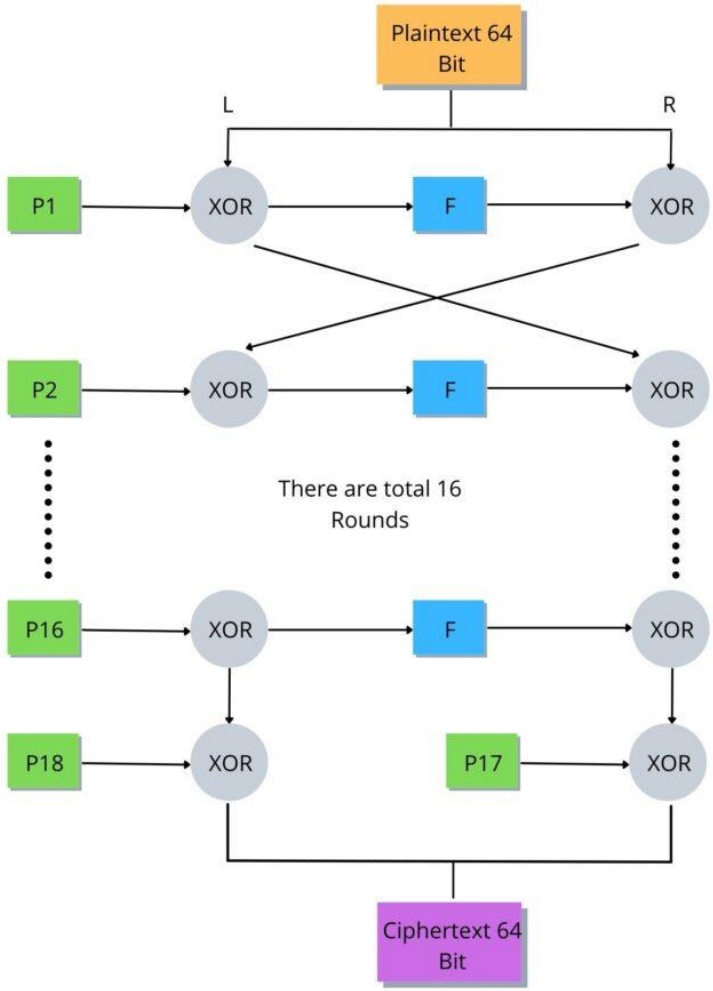
# AES (Advanced Encrytion Standard - Gelişmiş Şifreleme Standardı)

- Des'e göre daha güvenli bir sistemdir. Çeşitli bilim adamları tarafından DES'in kırılması üzerine 2001 yılında geliştirilmiştir. Belçikalı Vincent Rijmen ve Joan Daemen tarafından bulunmuş, DES'in zayıf yönlerini tamamen düzelterek, matematikle oluşturulmuş bir blok şifreleme algoritmasıdır. 128 bit, 192 bit ve 256 bit olmak üzere üç farklı anahtar uzunluğuna sahip olabilir. AES'in DES'in aksine donanımda ve yazılımda hızlı olması, daha kolay uygulanabilir olması ve çok daha az hafızaya gerek duyması güçlü yönleri olarak söylenebilir. Günümüzde bilinen tüm akademik, pratik ve doğrudan (brute force) saldırılara karşı dayanıklı olduğu düşünülmektedir. En yaygın olarak kullanılan simetrik şifreleme algoritmasıdır.



# Blowfish

- Blowfish, 64-bit öbek büyüklüğüne ve 32 bit'ten 448 bit'e kadar anahtar uzunluğuna sahiptir. , DES'in eksik kalmaya başlamasından sonra onun yerini alması amacıyla tasarlanmıştır. Blowfish algoritması en az 4 kb ram'a ihtiyaç duyar. Bu yüzden akıllı kartlar gibi en küçük sistemlerde kullanılamaz. Yüksek şifreleme ve e-posta gibi rutin kullanıcı uygulamaları konusundaki etkinliğiyle başarılı bir algoritma olarak değerlendirilmektedir. Blowfish kullanımını artıran en önemli özelliklerinden birisi yapıldığı zamanda kullanılmakta olan şifreleme algoritmaları lisanslı ve paralı satılmasına rağmen, Blowfish'in tamamen ücretsiz olmasıdır. Blowfish piyasada kullanılan en hızlı öbek şifreleyicilerindendir ve içerdiği karmaşık anahtar çizelgesi şifrenin kırılmasını zorlaştırmıştır.

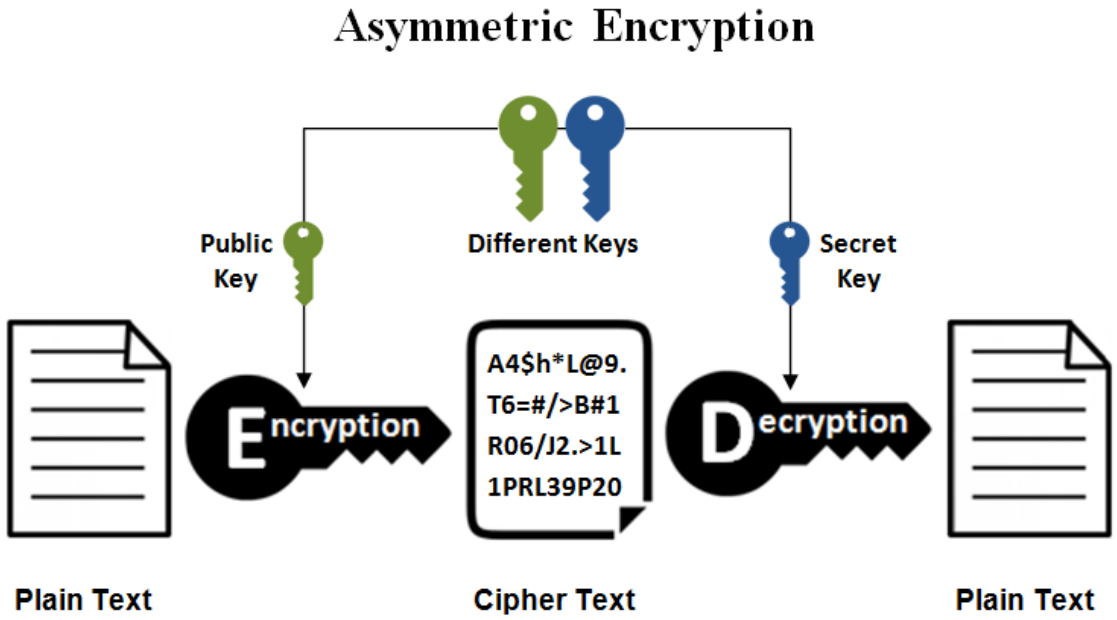



Blowfish Encryption Working

# Anahtarsız Algoritmalar

- Simetrik ve asimetrik şifrelemelerin haricinde girdi olarak anahtar kullanmayan algoritmalar da bulunmaktadır. Bu algoritmalar genel olarak bir sistemde yalnız olarak kullanılmazlar. Sistemde bulunan simetrik ve asimetrik diğer algoritmalara yardımcı olmak için yapılmışlardır. Özet fonksiyonu (Hash Functions) adı verilen algoritma en çok tercih edilendir. Bütünlük denetiminde ve güvenli şifre saklama işlemlerinde oldukça kullanılır. Bununla birlikte sayısal imza uygulamalarında asimetirik şifreleme kullanmak uygulamanın oldukça yavaş çalışmasına neden olmaktadır. Bu yüzden bu tür uygulamalarda özet fonkisyonları da kullanmak hız problemini azaltmaktadır.

# Açık Anahtarlı Şifreleme Yöntemleri




Asimetrik şifreleme, içerisinde bir özel ve bir açık anahtar bulunduran bir şifreleme algoritmasıdır. Açık anahtar güvenilir veya güvenilir olmayan herkese verilebilirken özel anahtarın güvenilir bir kişiye veya kişilere verilmesi gerekmektedir.

# Asimetrik Şifreleme Algoritmaları

- Simetrik şifreleme algoritmalarında  bulunan en büyük problem anahtar dağıtımıdır. Simetrik algoritma kullanan çok kullanıcılı bir sistemde anahtarın bütün kullanıcılara aynı anahtarın dağıtılması güvenlik açısından problemli olabilir. Her kullanıcıya farklı bir anahtar vermek ise sistemde bir çok farklı anahtar olacağı için sıkıntılı olabilir. Bu sorunları çözüm getirmek için asimetrik şifreleme algoritmaları geliştirilmiştir. Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı birbirinden farklıdır. Şifreleme yapan anahtara açık anahtar, şifreyi çözen anahtar ise özel anahtardır. Açık anahtarlar herkese dağıtılabilir, ancak hangi anahtarın kime ait olduğundan da emin olunmalıdır. Bu yüzden sertifikalar kullanılmaktadır.

# Asimetrik Şifreleme Algoritmaları

- Sertifika açık anahtar ile sahibinin kimliği arasındaki bağlantının belgesidir. Özel anahtar ise sadece şifreyi çözecek kullanıcıda bulunur.  Bu yüzden asimetrik şifreleme güvenlik açısından simetriğe göre çok daha başarılıdır. Az sayıda anahtar kullanarak simetrik şifreleme yapan çok kullanıcılı uygulamalarda ortaya çıkabilecek anahtar fazlalığı durumunu engeller.  Bununla birlikte hız ve donanımsal uygunluk gibi konularda asimetrik şifreleme simetriğe göre geri planda kalmıştır. Asimetrik algoritmaların güvenliğini sağlayabilmek için çok büyük asal sayılar kullanılmaktadır. Bu da zaman açısından çok büyük problemler getirmektedir. Asimetrik bir algoritmayı kullanan sistemler simetrik algoritmaları kullanan sistemlere göre çok daha yavaştır. Ayrıca asimetrik şifreleme algoritmalarının çok büyük sayılar kullanmasından dolayı donanımsal yapılara uyum sağlaması çok zor olmaktadır.

# Asimetrik Şifreleme Algoritmaları

**Kuvvetli Yönleri;**

- Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
- Anahtarı kullanıcı belirleyebilir.

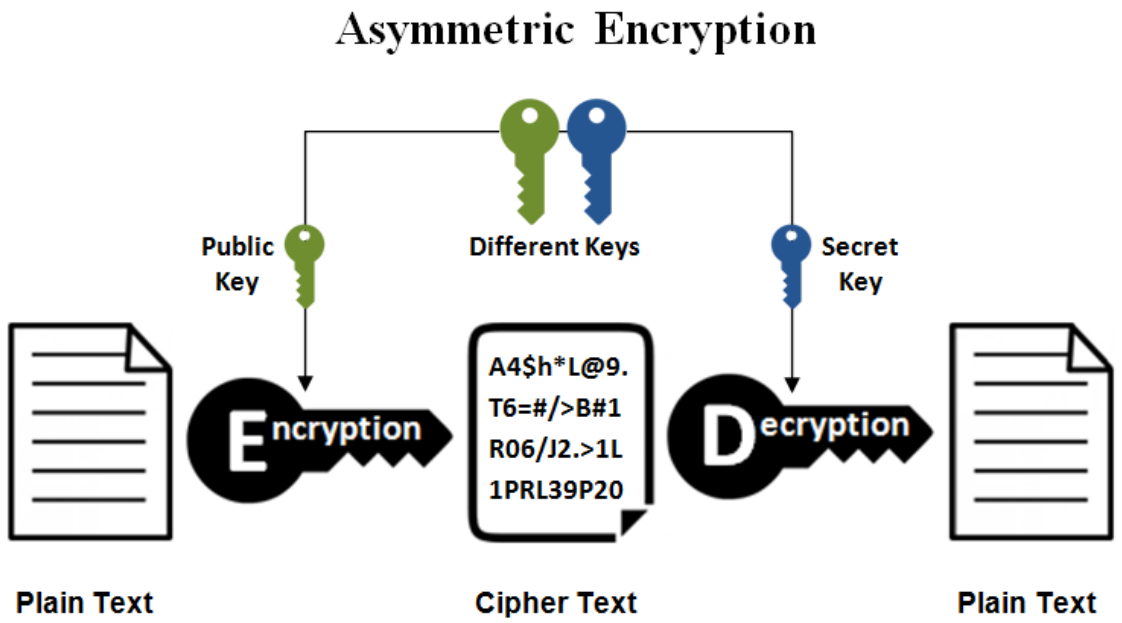
**Zayıf Yönleri;**

- Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.
- Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

# Asimetrik Şifreleme Algoritmaları

- Günümüzde simetrik ve asimetrik şifreleme algoritmalarını birlikte kullanarak hem yüksek derecede güvenlik hem de yüksek hızlı sistemler şifrelenebilmektedir. Bu gibi sistemlere melez sistem adı verilir. Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

# Açık Anahtarlı Şifreleme Yöntemleri




Asimetrik şifrelemenin iki ana kullanım amacı vardır. Bunlar doğrulama ve gizliliktir. Asimetrik şifreleme kullanılarak mesajların özel anahtar ile imzalanabildiğini ve mesajı alan kişi kendi özel anahtarı ile mesajı doğrulayarak mesajın doğru olduğunu teyit edebilmektedir.
Günümüzde en çok kullanılan asimetrik şifreleme algoritmaları ise aşağıdaki gibidir;

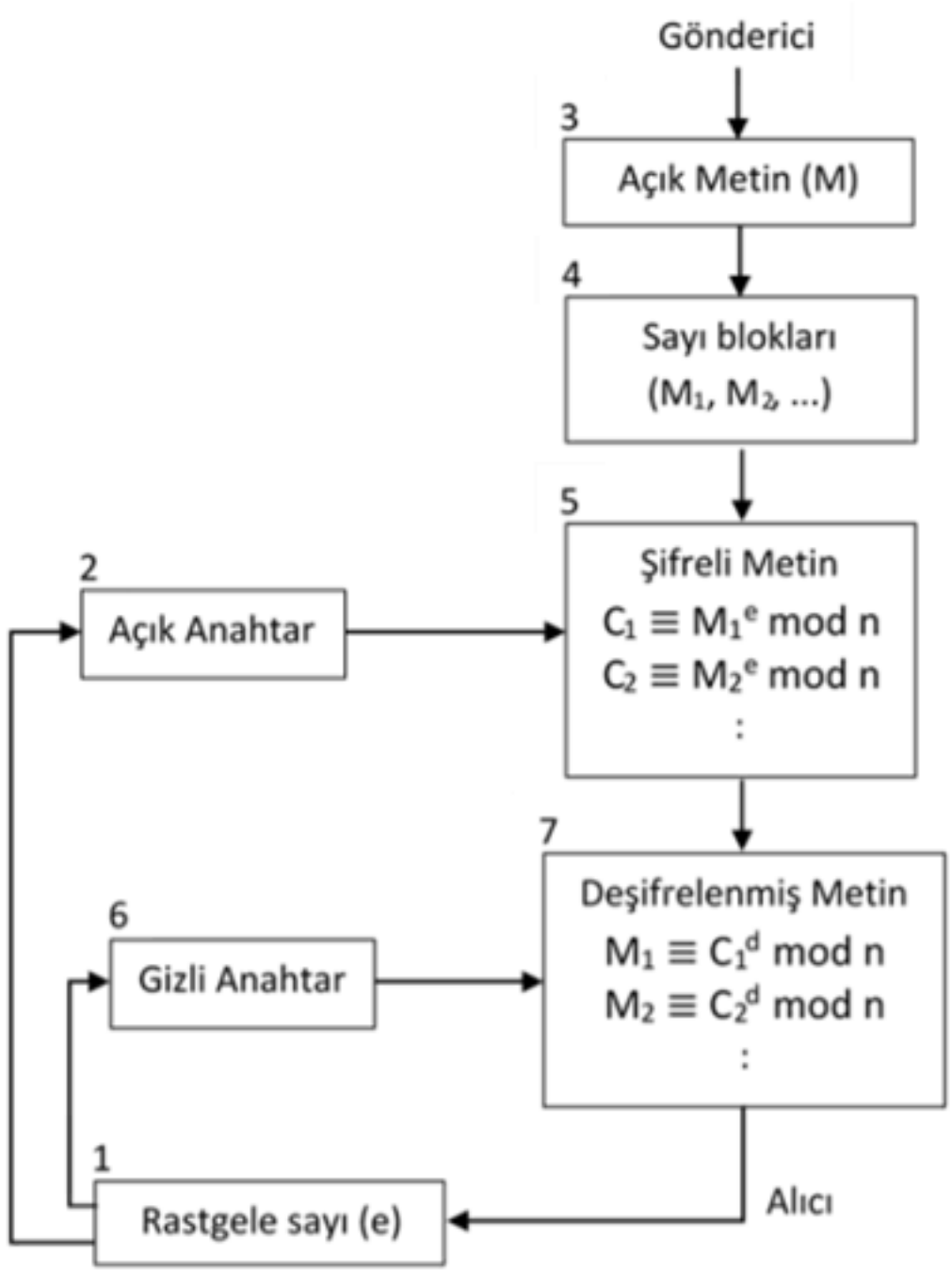
- RSA (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- DH (Diffie-Hellman)

# RSA (Rivest-Shamir-Adleman)

- 1977 yılında R.Rivest, A.Shamir ve L.Adleman isminde üç bilim adamının oluşturduğu yeni asimetrik şifreleme algoritması RSA, anahtar dağıtımının yanında şifreleme ve şifre çözme işlemlerini de gerçekleştirmektedir. RSA, güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Genel olarak RSA hem mesaj şifreleme hem de elektronik imza amacıyla kullanılan daha çok ticari uygulamalarda tercih edilen tam sayılar üzerinde en iyileştirme yapılarak oluşturulan değerlerden anahtarların üretildiği bir şifreleme teknolojisidir.

# RSA (Rivest-Shamir-Adleman)

- RSA algoritmasında sistemin güvenilirliğinin yanı sıra hızının da yüksek olması için, kullanılacak anahtarın sayısal büyüklüğü önemlidir. Yeterli güvenilirlik derecesine ulaşmak için gerekli büyüklük Eliptik Eğri Şifreleme (ECC) Algoritması kullanılarak belirlenmektedir. RSA ile günümüzde 1024 bitlik bir anahtar (yaklaşık 300 basamaklı bir sayı) basit uygulamalar için yeterli bir şifreleme tekniği olarak kullanılabilir. RSA algoritması, bir şifreleme algoritması için oldukça basit bir algoritmadır. Buna karşın sürekli çok büyük asal sayı oluşturmak oldukça zor bir işlemdir.
- RSA şifreleme sistemin oluşturulmasıyla birlikte asimetrik şifreleme algoritmalarının günümüzde daha yaygın olarak kullanılması sağlanmıştır.


Gönderici
3
Açık Metin (M)
4
Sayı blokları
(M1, M2, ...)
5
Şifreli Metin
C1 ≡ M1^e mod n
C2 ≡ M2^e mod n
:
2
Açık Anahtar
7
Deşifrelenmiş Metin
M1 ≡ C1^d mod n
M2 ≡ C2^d mod n
:
6
Gizli Anahtar
1
Rastgele sayı (e)
Alıcı

# 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.

# DH (Diffie-Helman)

- 1976 yılında 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.