http://rumkin.com/tools/cipher/

ŞİFRELEME BİLİMİ

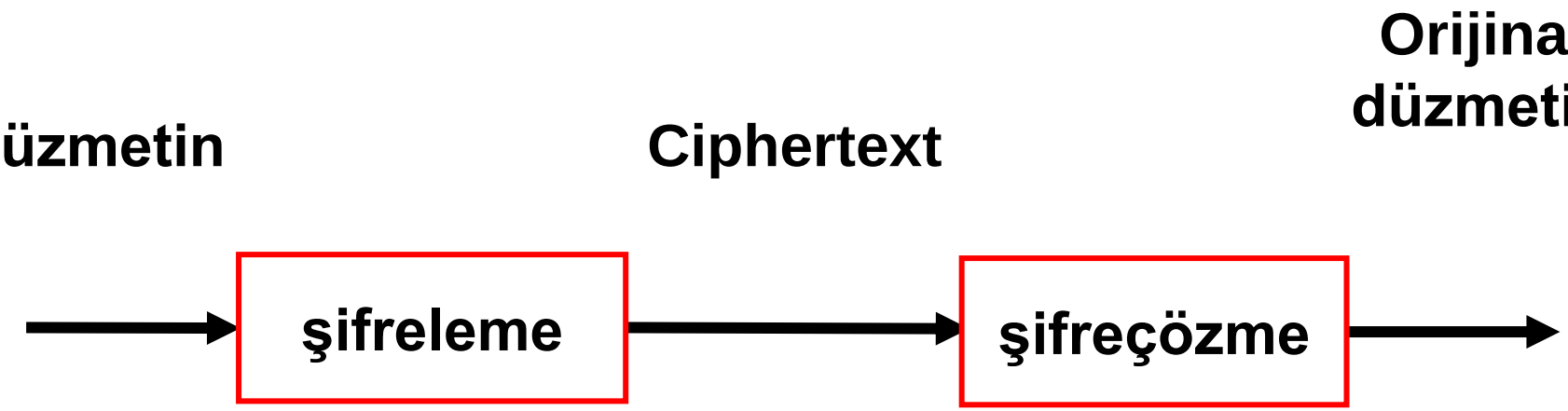
Kriptoloji?

- “Kryptos logos”, “gizli”, “dünya”
- Haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor ifadelere dayanan tekniklerin ve uygulamaların bütünüdür.
- “Matematik, elektronik, optik, bilgisayar, sosyal mühendislik bilimleri gibi bir çok disiplini kullanan özelleşmiş bir bilim dalı”

Kriptoloji?

- **Kriptografi**
  - Belgelerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemlere verilen addır.
- **Kriptoanaliz**
  - Kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır.

Kriptografi?



Kriptografi?

- Veri kaybetmeden veriyi işleme ve farklı bir forma dönüştürme (karşılıklı)
- Çoğunlukla bir formdan diğerine (one-to-one) dönüştürülür (not compression)
- Güvenlik için kullanılan yaygın bir yaklaşımdır.
- Analog kriptolama örneği: ses dönüştürücü

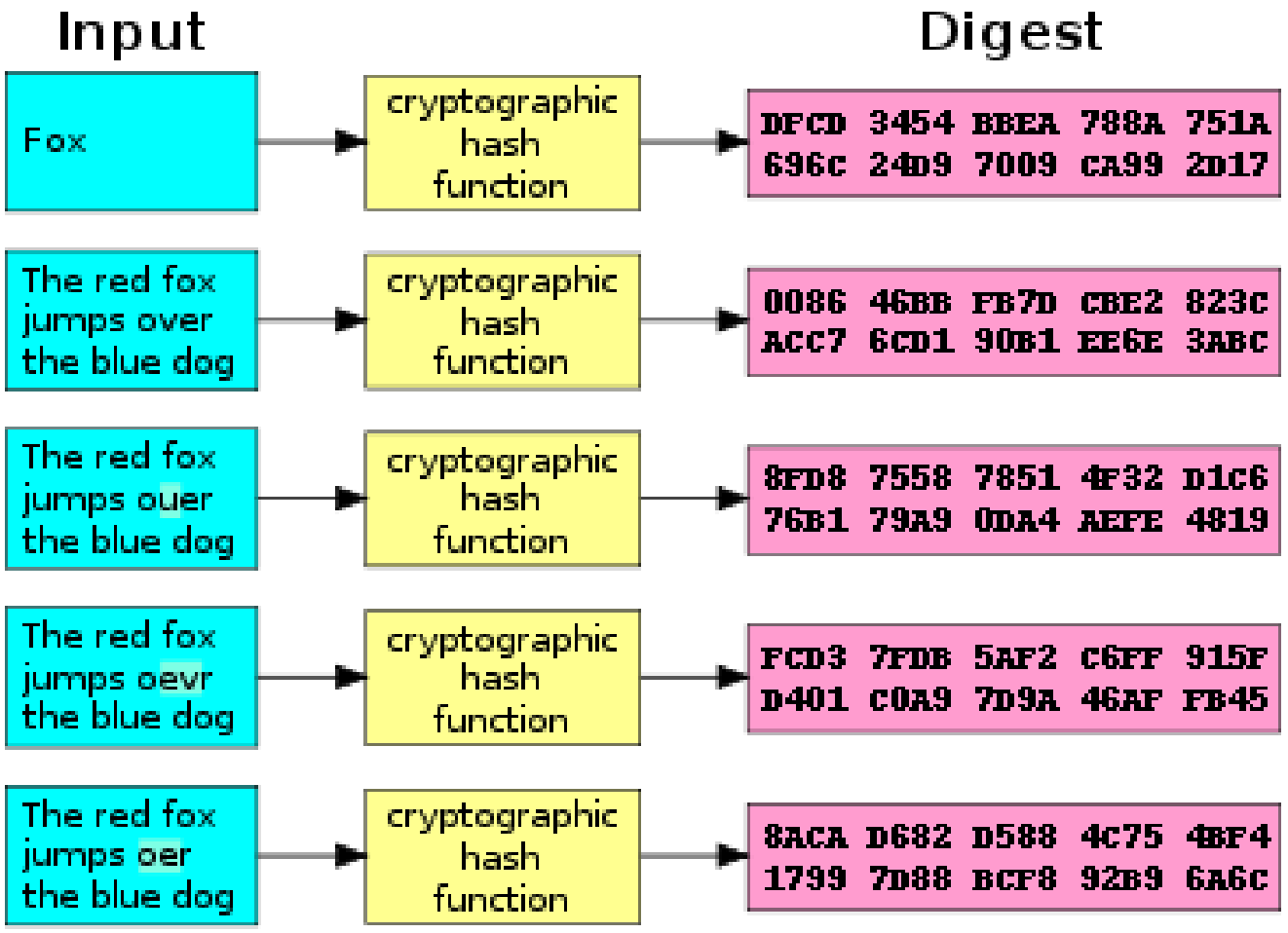
Kriptografi?

- Matematik temele dayanır.
- Matematik fonksiyonlar encryption ve decryption için kullanılır.
  - *Şifreleme (Encryption)*
    - Düzmetini şifreleme işlemi
  - Ciphertext
    - şifrelenmiş mesaj
  - Şifreçözme (Decryption)
    - Şifrelenmiş mesajı düzmetine dönüştürme işlemi

Kriptografi tipleri

- Hash fonksiyonları
  - anahtar yok
- Gizli anahtar (Secret key) şifreleme
  - Bir anahtar (one key)
- Açık anahtar (Public key) şifreleme
  - İki anahtar, açık veya genel ve gizli veya özel (public, private)

Hash Function Example



Veya Şifreleme Ana Dalları

- Konvansiyonel (simetrik) şifreleme: Klasik teknikler ve modern teknikler
- Açık anahtar şifreleme (asimetrik)
- Hibrit yaklaşımlar

ŞİFRELEME YÖNTEMLERİ ve ALGORİTMALARI

ŞİFRELEME YÖNTEMLERİ ve ALGORİTMALARI

Günümüzde şifreleme yöntemleri, matematiksel temelli hesaplamalara dayanan bilgisayar, elektronik, fizik gibi birçok bilim dalını ilgilendiren bir sistematiğe bürünmüştür.

ŞİFRELEME YÖNTEMLERİ ve ALGORİTMALARI

- ✓ Şifreleme ve şifre çözme işleminde kullanılan bir çok algoritma, teknik ve yaklaşım bulunmaktadır.

- ✓ Şifreleme algoritmalarının sağlamak zorunda OLDUĞU kriterler nelerdir?

ŞİFRELEME
Algoritmaları Kriterleri?

- Şifrelenmiş mesaj, deşifre edildiğinde bilgi kaybı olmamalıdır.
- Şifreleme işlemlerinde güvenlik seviyesi mümkün olduğunca yüksek olmalıdır.
- İhtiyaç duyulan güvenlik seviyesine göre güvenlik seviyesi seçilebilmelidir.
- Şifrelenmiş mesaj ile düz metin arasındaki ilişki zor kurulmalıdır.
- Şifreleme işlemleri basitçe ve kolaylıkla gerçekleştirilebilmelidir.

ŞİFRELEME
Algoritmaları Sınıflandırması?

Şifreleme algoritmalarını birkaç açıdan değerlendirip sınıflandırmak mümkündür.

Genel olarak şifreleme algoritmalarını,

- algoritmalarına,
- anahtar sayısına veya
- mesaj tipine

göre sınıflandırmak mümkündür.

Sonraki yansılarda bu sınıflandırma şekilleri irdelenecektir.

Kullanılan Algoritmalara Göre Şifreleme Teknikleri

Şifrelemenin tarihi gelişimine baktığımızda, şifreleme algoritmalarını

gizli şifreleme algoritmalı ve
açık şifreleme algoritmalı sistemler

olmak üzere ikiye ayırabiliriz.

Gizli Algoritmalı Şifreleme Teknikleri

- Gizli algoritmalı sistemler, tarihin ilk devirlerinden buyana dünyada kullanılmaktadır.
- Bu sistemlerde, şifreleme algoritması ve şifre çözme algoritması birbirinin tersidir.
- Öncelikle haberleşecek iki grup aralarında gizli bir algoritma tespit ederler.
- Eğer bu iki grup birbirleri ile yakın yerlerde değilse, güvenli bir iletişim kanalı veya güvenilir bir kurye ile bu algoritmayı birbirlerine ulaştırırlar.
- Bu sistemler, algoritmanın gizliliğinin sağlanması zorunluluğu nedeniyle sadece sınırlı kullanıma sahiptirler, yaygınlaşması ve standartlaşması oldukça zordur.
- Bu tür algoritmalara çoğunlukla kuşkuyla bakılmaktadır.
- Bu nedenle, gizli algoritmalı klasik şifreleme sistemleri, bankalar ve elektronik ticaret siteleri gibi uygulamalara uygun değildir.

Algoritması Açık Şifreleme Teknikleri -1

- Şifreleme algoritmalarının standart hale gelmesi için geniş bir kullanıma sahip olmaları gerekmektedir.
- Bu nedenle algoritması herkes tarafından bilinen sistemler tasarlanmıştır.
- Bu tür şifreleme sistemlerinde, P metni sadece alıcı ile göndericinin bildiği bir K anahtarı kullanılarak bilinen bir şifreleme algoritması ile şifrelenir. Bu nedenle bu sistemlere anahtara dayalı şifreleme sistemleri denir.
- Modern şifreleme teknikleri anahtar altyapısına dayanan, açık algoritmalı sistemlerdir.

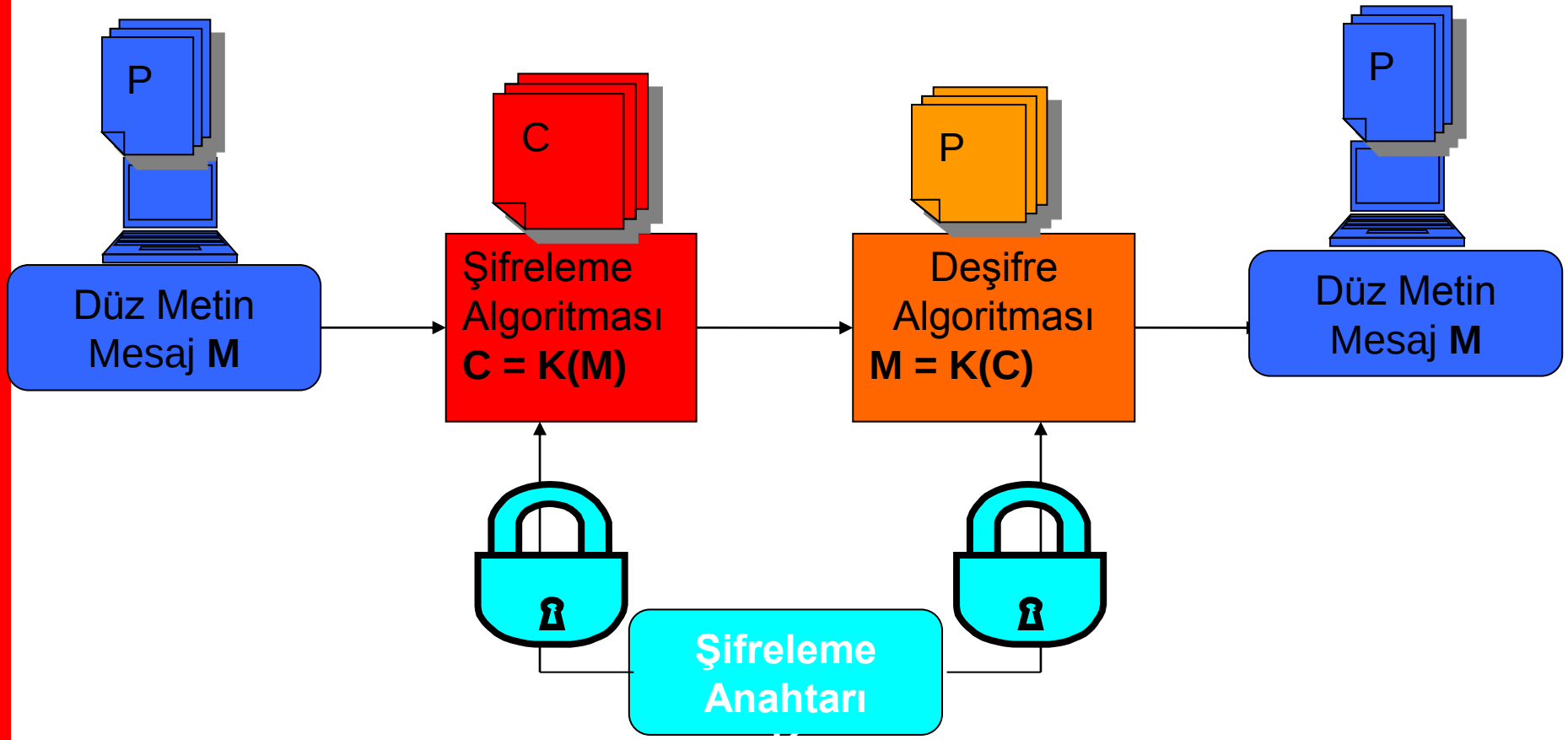
Algoritması Açık Şifreleme Teknikleri -2

- Kullanıcı bir mesajı göndermeden önce bir anahtar (k1) kullanarak şifreler.
- Şifreli metin açık bir kanaldan gönderilir. Mesajı okumak için alıcı (k2) anahtarını kullanarak şifreyi çözer ve mesajı elde eder.
- Aktif düşmanlar araya girip iletişimi dinleyebilir.
- Eğer k1 ve k2 eşitse, sistem simetriktir. Aksi takdirde bu sistem asimetrik olarak nitelenir.
- Güvenliğin garantilenmesi için k2 her zaman gizli olmalıdır, ancak k1'i kullanarak k2'yi elde etmek mümkün olmadığı sürece k1 açıklanabilir.
- Anahtar tiplerine göre de şifreleme algoritmalarını ikiye ayrılır.
  - Simetrik Anahtarlı Şifreleme,
  - Asimetrik Anahtarlı Şifreleme
- Bu ayrım, şifreleme algoritmalarının sınıflandırılmasında kullanılan en yaygın yöntemdir.

Simetrik Algoritmalı Şifreleme Teknikleri

- Bir taraf, şifreleme algoritmasında girdi olarak düz metin P'yi ve K anahtarını kullanarak şifreleme algoritmasını çalıştırıp şifreli metin C'yi elde eder.
- C şifreli metni mesaj alıcısına iletilir. Alıcı, şifre çözme algoritmasının girdileri olarak C şifreli metni ve K anahtarını kullanıp, P düz metnini elde eder.
- Bu tür şifreleme sistemlerinde, şifrelemek ve şifre çözmek için simetrik anahtarlar kullanıldığından simetrik anahtarlı şifreleme algoritmaları denir.
- Simetrik anahtarlı şifreleme sistemlerinde de kullanılan K anahtarı gizlidir.

Şifreleme Algoritmalarının Sınıflandırılması



Bazı Simetrik Algoritmalar

Bu şifreme sistemini kullanan algoritmalardan bazıları:

- **DES, 3DES, DESX,**
- **IDEA, XOR, SKIPJACK,**
- **RC2, RC4, RC5 şifreleme algoritmalarıdır.**

Asimetrik Algoritmalı Şifreleme Teknikleri -1

- Açık anahtarlı kriptografinin gelişmesi, bütün kriptografi tarihindeki en büyük devrimdir.
- Gizli anahtarlı kriptografinin aksine, açık anahtarlı kriptografi sistemlerinin kullanımı henüz çok yenidir.
- Açık anahtar tabanlı şifreleme sistemlerinin tarihi 1970'li yıllara dayanır.

Asimetrik Algoritmalı Şifreleme Teknikleri -2

- Açık anahtarlı kripto sistemleri üzerine ilk öneri 1976 yılında Diffie ve Helman'ın tarafından yapılmış, ardından 1977 yılında Rivest, Shamir ve Adleman RSA'yı önermişlerdir.
- El-Gamal açık anahtarlı kripto algoritması ve eliptik eğri açık anahtarlı kripto sistemi El-Gamal tarafından önerilmiştir.

Asimetrik Algoritmalı Şifreleme Teknikleri -3

- Diffie ve Helman'ın temellerini attığı bu sistemde zaman içerisinde birçok algoritma önerilmiştir.
- Temelde açık anahtarlı kriptografi sistemlerinin amacı, belli bir anahtar üzerinde anlaşmanın ve karşı tarafa bu anahtarı güvenli olarak ulaştırabilmenin zorunluluğunu ortadan kaldırmaktadır.

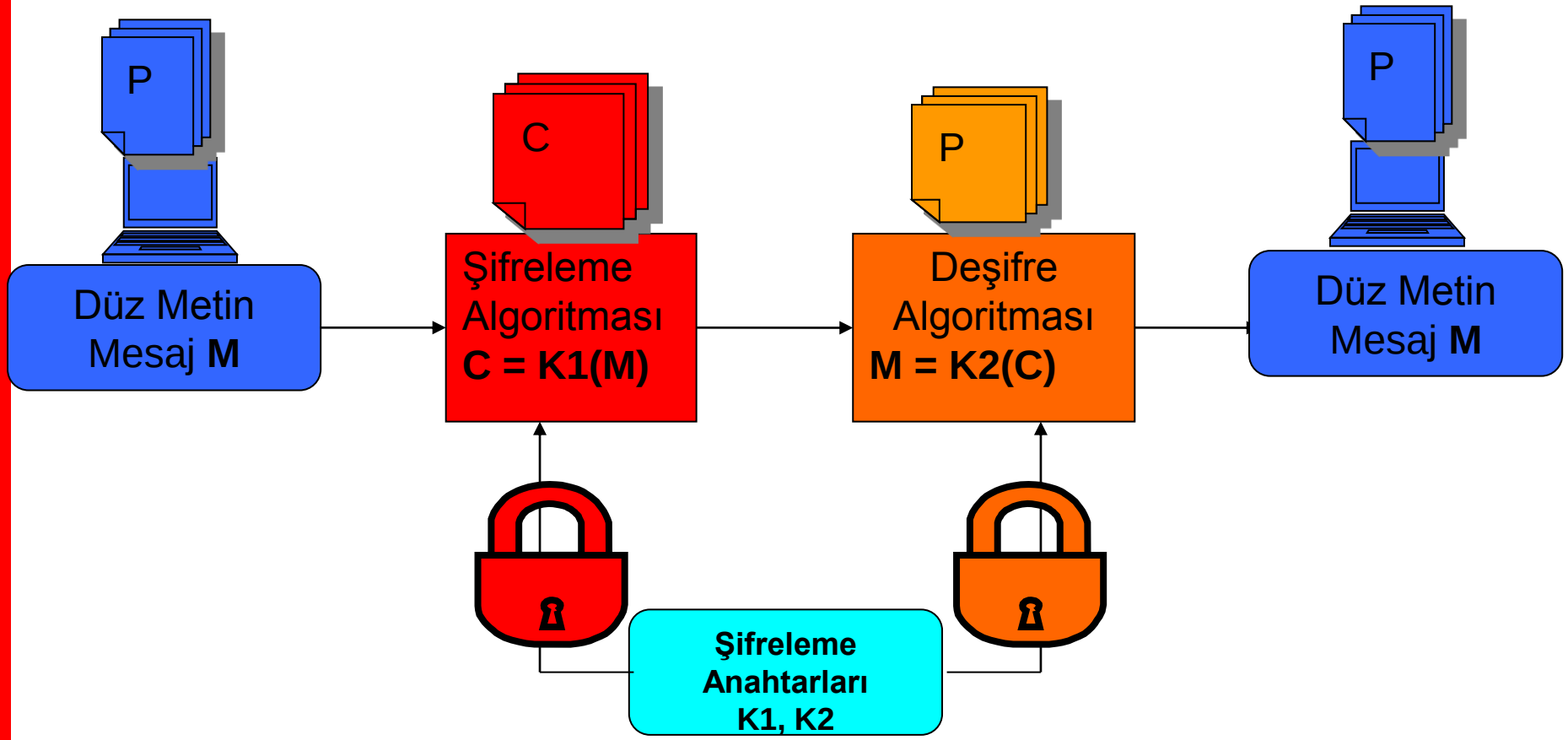
Asimetrik Algoritmalı Şifreleme Teknikleri -4

- Tek yönlü bir mesajlaşma söz konusudur. Mesaj alıcısı sadece kendi bileceği "Gizli Anahtar" ve diğer kişilere duyurabileceği bir "Açık Anahtar"dan oluşan anahtar çiftini belirler.

Asimetrik Algoritmalı Şifreleme Teknikleri -5

- Mesaj göndericisi, alıcıya ait herkes tarafından bilinen açık anahtarı kullanarak mesajı şifreler ve alıcıya gönderir, mesajı alıcı kendi gizli anahtarı ile deşifre eder.
- En yaygın açık anahtarlı şifreleme algoritması RSA'dır.
- Asimetrik anahtarlı şifreleme, simetrik anahtarlı şifrelemeden daha uzun zaman almaktadır.
- Bu zaman, mesajın büyüklüğüne ve anahtara bağlı olarak üssel olarak artar ve kırılması daha zordur.

Şifreleme Algoritmalarının Sınıflandırılması



Şifreleme Algoritmalarının Sınıflandırılması

- **Şifrelenen Mesaj Tipine Göre Algoritmalar :**

- **Şifreleme algoritmalarını sınıflandırmanın bir diğer yolu da, şifrelenen mesajın tipine göre ayrım yapmaktır. Buna göre, algoritmaları ikiye ayırabiliriz;**

- **Dizi Şifreleyiciler,** Stream Cipher

- **Blok Şifreleyiciler.** Block Cipher

Şifreleme Algoritmalarının Sınıflandırılması

- **Dizi Şifreleyiciler :**
  - **Bu çeşit şifrelemede algoritmanın girdisi anahtardır. Algoritma, anahtardan rasgele olarak bir diziye çok benzeyen kayan anahtar dizisi üretir.**
  - **Daha sonra, kayan anahtar dizisinin elemanları ile açık metin veya şifreli metin dizisinin elemanları ikili tabanda toplanarak şifreleme ve şifre çözme işlemi tamamlanır.**

Şifreleme Algoritmalarının Sınıflandırılması

- **Dizi Şifreleyiciler :**

- **Dizi şifreleme algoritmaları; mesajı bit bit (dizi olarak) veya byte byte işler.**

- **Bu yöntemde en meşhur şifreleme algoritması, basit olarak mesaj bitlerini rasgele anahtar bitlerine ekleyen 1917'de Vernam tarafından bulunan Vernam cipher (one time pad)'dir.**

Şifreleme Algoritmalarının Sınıflandırılması

- ✓ **Dizi Şifreleyiciler :**

  ✓ **RC4 ve SEAL algoritmalarının yanında, en meşhur şifreleme algoritması, basit olarak mesaj bitlerini rasgele anahtar bitlerine ekleyen 1917'de Vernam tarafından bulunan Vernam cipher (one time pad)'dir.**

Şifreleme Algoritmalarının Sınıflandırılması

- **Blok Şifreleyiciler :**

  - Mesaj tipine göre sınıflandırılan şifreleme algoritmalarında en yaygın şifreleme yöntemi mesajı blok blok şifrelemektir.

  - Şifreleme ve şifre çözme işleminde metinler, sabit uzunluktaki dizilere bölünüp blok blok şifrelemeye tabi tutulurlar (Örn: 8,16,32bit veya byte) .

Şifreleme Algoritmalarının Sınıflandırılması

- **Blok Şifreleyiciler :**
  - **Anahtar uzunluğu ise yine sabittir.**
  - **Blok şifreleme, dizi şifrelemeye göre daha avantajlıdır. Çünkü bloklardan karakterleri tahmin etmek daha güçtür.**

Şifreleme Algoritmalarının Sınıflandırılması

- **Blok Şifreleyiciler :**
  - **Blok şifreleme kullanan bazı algoritmalar;**
    - **DES,**
    - **FEAL,**
    - **IDEA,**
    - **RC5 olarak göze çarpmaktadır.**