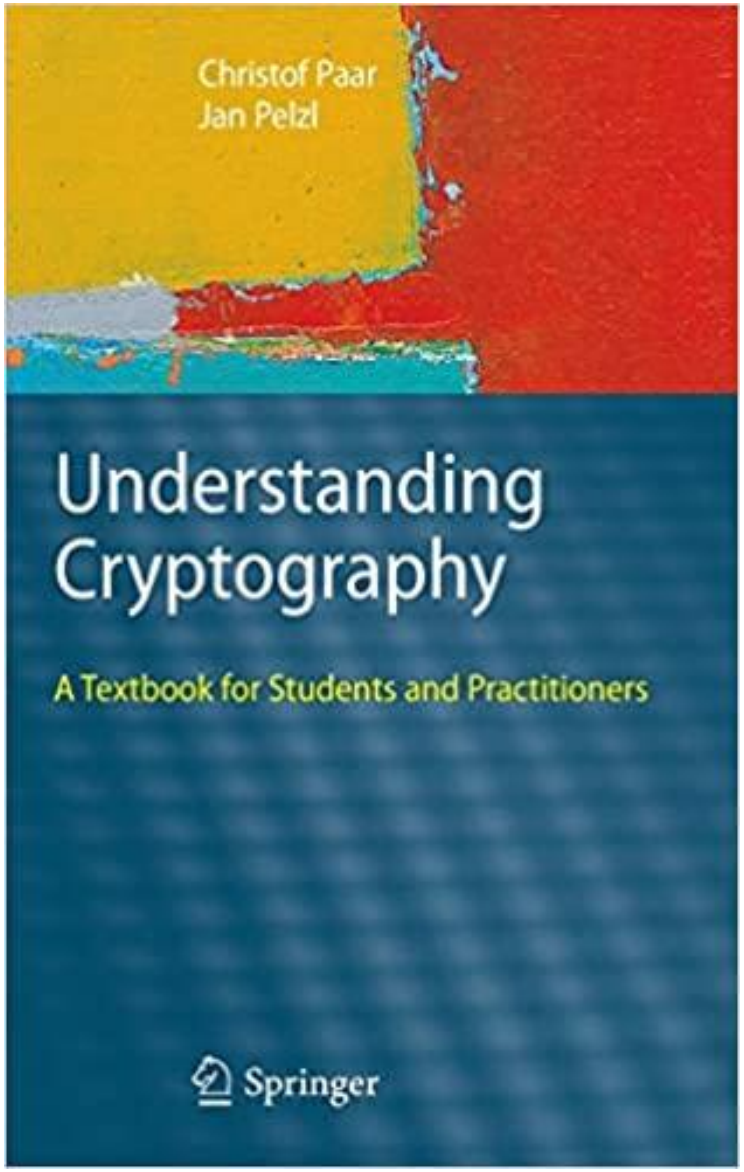
BİLGİ SİSTEMLERİ VE GÜVENLİĞİ

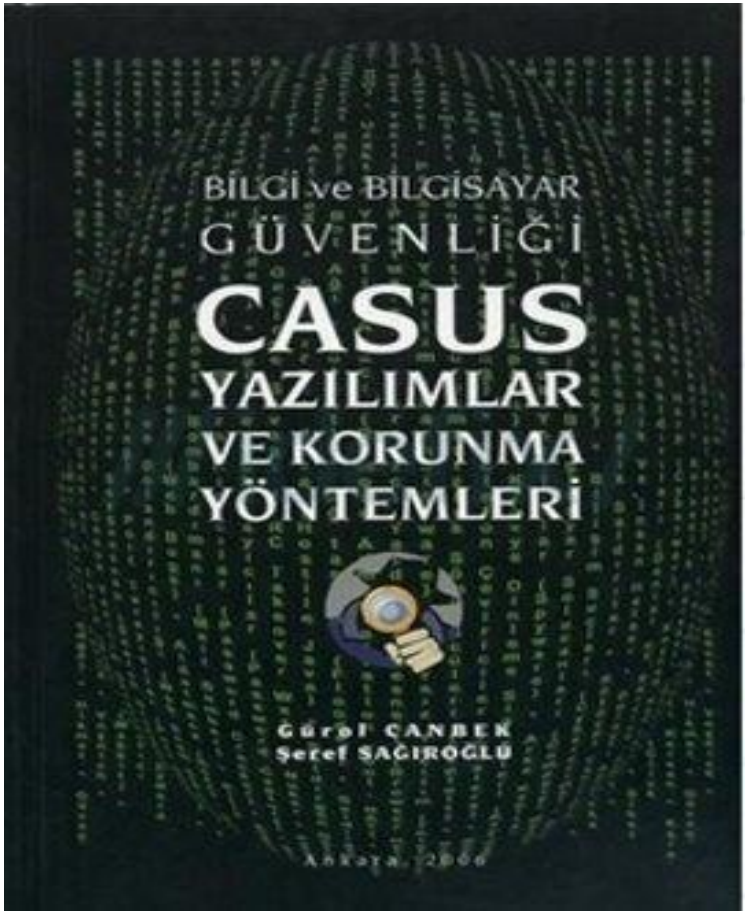
Giriş

- Kaynak ;



Giriş

- Kaynak ;



Dersin Amacı

Temel bilgi güvenliği konuları, simetrik şifreleme, blok şifreleme, DES, AES, gizli anahtar şifreleme, RSA, dijital imzalar ile Hash işlemleri hakkında bilgi ve beceriler kazandırmak.

Haftalık Ders Planı

Hafta	Konu
1	Bilgi güvenliğine giriş ve temel kavramlar
2	Şifre bilimi ve şifreleme teknikleri
3	Şifreleme tarihçesi
4	Simetrik şifreleme algoritmaları, Sezar, Affine
5	Simetrik şifreleme algoritmaları, Vigenere, Çoklu-Alfabe
6	Blok şifreleme
7	Veri şifreleme standardı (DES)
8	Gelişmiş şifreleme standardı (AES)
9	Blok şifreleme: çalışma modları
10	Açık anahtarlı şifrelemeye giriş
11	RSA şifreleme
12	Dijital imzalar
13	Hash fonksiyonları

1.Bölüm :Bilgi ve Bilgi Varlıkları

- Bilginin özellikleri [Housman,E.M; “The Nature of Information”]
  - ❖ Boşlukta ve zamanda yer kaplar
  - ❖ Gürültü çıkarmadan hareket etmez
  - ❖ Hareketi için enerji gerekir
  - ❖ Yaşam ve herhangi bir düzenli etkinlik için gereklidir
  - ❖ Hem maddesiz biçim hemde biçimsiz maddedir.

Bilginin Özellikleri

- Ağırlığa sahiptir. Bir giga byte, bir parmak izinden daha az ağırlıktadır.
- Zaman içinde hareketli ve donmuş olabilir
- Bir soruya tatmin edici, belki de rahatsız edici bir cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için kullanılan gerekli bilgi birbirine eşittir.
- Katı hale sahiptir donarak katılaşır (depolama)

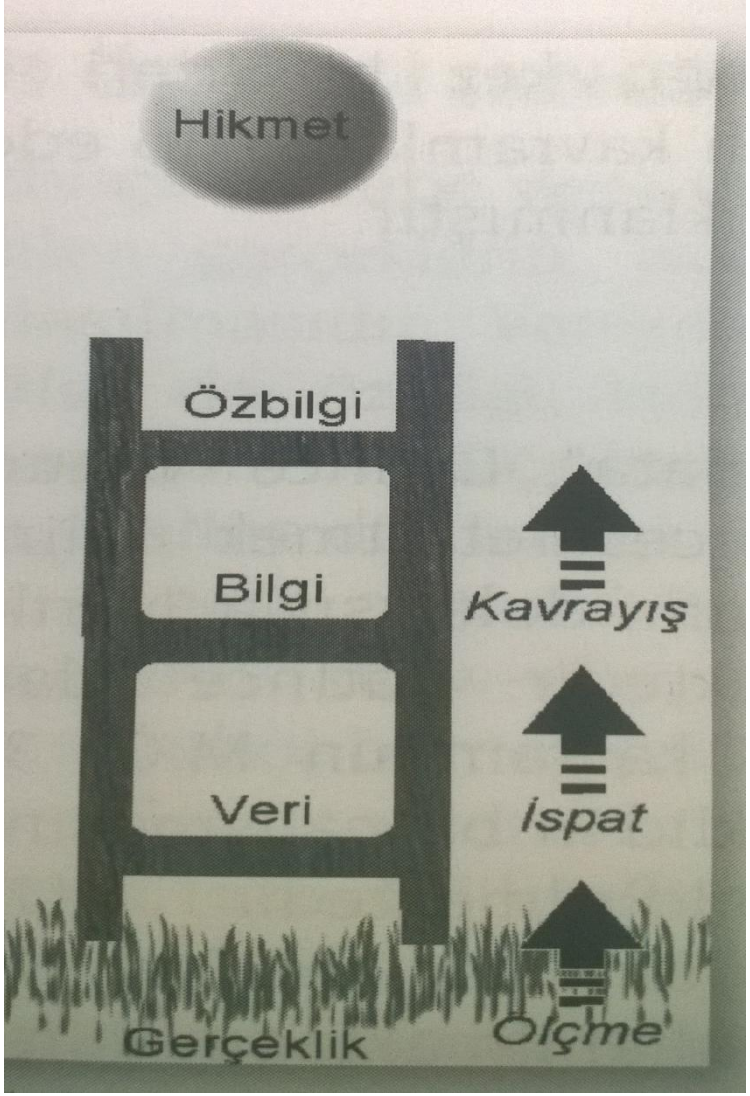
Bilginin Özellikleri

- Sıvı hale sahiptir; akar (iletişim).
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.

Gerçeklik (reality) ve Hikmet (wisdom)

- Bilgi çağında ilerlemek, bir merdivenin basamaklarını kullanarak bir üst seviyeye çıkmaya benzetilebilir.
- Yukarıya çıktıkça elimizdeki varlığın miktarı azalırken değeri artar. Bir üst basamağa çıkmak daha da zorlaşır.

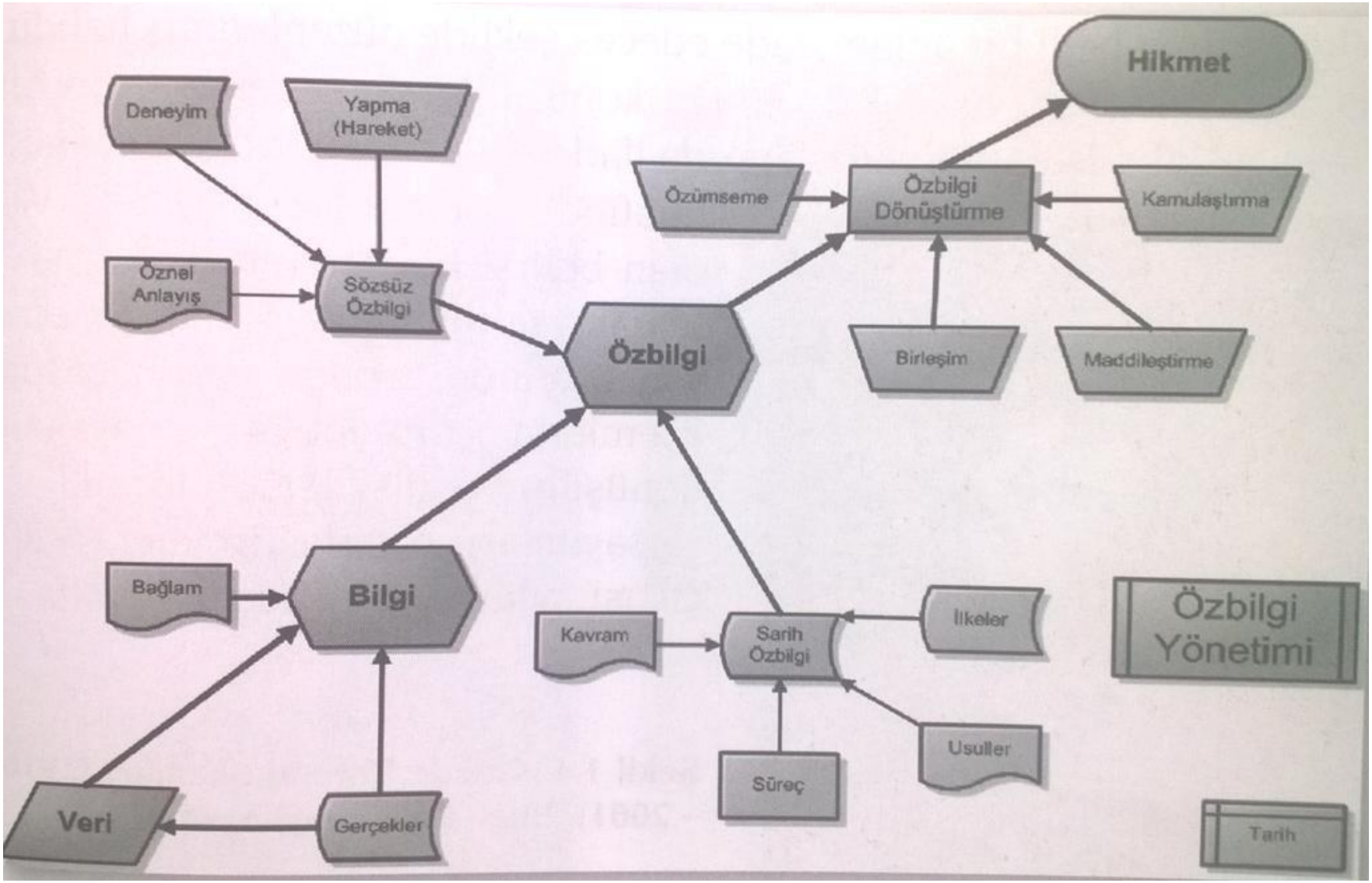
Gerçeklik (reality) ve Hikmet (wisdom) Bilgi Basamakları



Gerçeklik (reality) ve Hikmet (wisdom)

- Bilimde ;
  - Ölçme ile eldeki gerçeklikten veriye
  - İspat ile veriden bilgiye
  - Kavrayış ile bilgiden özbilgiye ulaşılır.
- Özbilgiden hikmete ulaşma sentezleme içeren bir düşünüş gerektirir.
- Alt basamaklarda, daha algoritmik ve programlanabilir bir yaklaşıma ihtiyaç varken yukarı basamaklar algoritmik olmayan ve programlanamayan bir yapı taşır.

Özbilgi (knowledge) Yönetimi



Kavramlar

- VERİ (data) :Sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizileri olarak tanımlanır.
- BİLGİ (information):
  - Verinin belirli bir anlam ifade edecek şekilde düzenlenmiş halidir. İşlenmiş veri olarak da ifade edilebilir. Bir konu hakkında var olan belirsizliği azaltan kaynak biçiminde de tanımlanan bilgi
    kısaca;
    - Veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan, dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s) çıktısı olarak ifade edilir.

Kavramlar

- ÖZBİLGİ (knowledge) :
  - Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.
  - Öz bilgi;
    - Ne olduğunu (know-what)
    - Niçin olduğunu (know-why)
    - Nasıl olduğunu (know-how)
    - Kim olduğunu (know-who)

  bilmek şeklinde dört sınıftan oluşur.

Kavramlar

- HİKMET (wisdom):
  - Bilgelik
  - Güvenilir yargıda bulunmak ve karar vermek için öz bilginin nasıl kullanılacağını kavramak,
  - Bir kişinin özel iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür.
  - Einstein, “hikmet, eğitim ve öğretimin ürünü değil; onu elde etmek için ömür boyu süren bir girişimin sonucudur.” der.

Fikri Mülkiyet

- İnternet kullanımı her geçen gün artmaktadır.
- İlerleyen teknoloji ile birlikte bilginin depolanması ve transferi kolaylaşmaktadır.
  - Örneğin; TUBİTAK Bilim ve Teknik Dergisinin 39 yıllık tüm sayıları 4,28 GB lık birDVD de toplanabilmiştir.
- İnternet bir bilgi servetidir.
- Birçok uygulama sayesinde aranan bilgiler saklanmaktır. (RSS gibi)

Fikri Mülkiyet

- Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi zor; aynı zamanda elde tutulması da zor bir metadır.
- Fikri mülkiyet (entelektüel mülkiyet, intellectual capital, property) olarak tanımlanan bu meta, bir kurumun bilgi ve özbilgi varlığıdır.
- Bu mülkün korunumu oldukça önemlidir. Bu yüzden patent, telif hakkı ve ticari marka gibi haklar, fikri mülkiyeti korumak amacıyla oluşturulmuştur.

2.BÖLÜM :
Bilgi Güvenliği Tarihçesi

Bilgi Güvenliği Tarihçesi

- Bilişim teknolojilerinin kullanımın hızla yaygınlaştığı günümüzde; bilgi, bilgisayar ve bilgisayar sistemleri güvenliği, en önemli ve kritik noktaların başında yer almaktadır.
- Bilgi güvenliğinin insanlığın var olduğu zamandan beri uygulana gelen ilk örneği şifrelemedir.

Bilgi Güvenliği Kavramları:

- **Gizlilik:** İletilen bilginin yalnızca yetkili kullanıcı tarafından erişilebilir olmasıdır. Bilgi diğer tüm ortam için özel ve gizlidir.
- **Bütünlük Sağlama:** İletilen bilgi yalnızca yetkili kişiler tarafından değiştirilir. Bunun dışında veri bütünlüğü korunur. Koruma özelliği aktif saldırılar ile ilgili bir özelliktir. Bu nedenle veri bütünlüğünün bozulduğu tespiti, bütünlüğü sağlamaktan daha önemlidir.
- **Kimlik Denetimi (Asıllama):** Bilgi kaynağının doğruluğunu kontrol eder. Güvensiz ortamdan gönderilen bilginin kaynağı, içeriği, gönderildiği saati, gönderen kaynağın saati gibi parametreler asıllanır.
- **İnkar Edememe:** Haberleşen noktaların daha önce gönderdikleri bilgileri ve yaptıkları istekleri inkar edememelerini sağlar.
- **Erişim Kontrolü:** Önceden tanımlı ve kimlik denetimi yapılmış varlıkların sadece kendilerine izin verilen oranda ilgili kaynaklara erişebilmelerini mümkün kılar. İzinsiz kişi ya da uygulamaların erişimlerini engeller.

Şifre Bilimi ve Şifreleme Teknikleri

- Veri, bilgi veya özbilginin şifrelenmesi, saklnması veya istenilmeyen kişilerin anlamasını zorlaştırma ve şifrelenmiş veri bilgi veya özbilgilerin çözülmesi üzerfine çalışan bilime şifreleme (kriptoloji) denir.
- Kriptoloji Yunanca "krptos logos" yani "gizli kelime"den gelir.
- Kısaca kriptoloji, matematiksel tabana dayanan uygulamalar ve teknikler üzerine çalışan bilim dalı olarak özetlenebilir.

Kriptolojinin Tarihçesi

- MÖ.1900 dolaylarında bir Mısırlı katip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı.
- MÖ.60-50 Julius Caesar (MÖ 100-44) normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullandı (Kendisinden k harf sonraki harfle değiştirilmesi).
- 725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı (Bu kitap kayıp durumdadır). Kitabı yazmasına ilham kaynağı olan, Bizans imparatoru için Yunanca yazılmış bir şifreli metni çözmesidir. Abu Abd al-Rahman, bu metni çözmek için ele geçirdiği şifreli mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır.
- 1000 - 1200 Gaznelilerden günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu.

Kriptolojinin Tarihçesi

- 1586 Blaise de Vigenère(1523-1596) şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin için otomatik anahtarlama yönteminden bahsedildi. Günümüzde bu yöntem hala DES CBC ve CFB kiplerinde kullanılmaktadır.
- 1623'de Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografı buldu.
- 1790'da Thomas Jefferson, Strip Cipher makinesini geliştirdi. Bu makineyi temel alan M-138-A, ABD donanmasının 2.Dünya savaşında da kullandı.
- 1917'de Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad'"i buldular.
- 1920 ve 1930'larda FBI içki kaçakçılarının haberleşmesini çözebilmek bir araştırma ofisi kurdu. William Frederick Friedman, Riverbank Laboratuarlarını kurdu, ABD için kriptoanaliz yaptı, 2. Dünya savaşında Japonlar'ın Purple Machine şifreleme sistemini çözdü.

Kriptolojinin Tarihçesi

- 2. Dünya savaşında Almanlar Arthur Scherbius tarafından icat edilmiş olan Enigma makinasını kullandılar. Bu makine Alan Turing ve ekibi tarafından çözüldü.
- 1970'lerde Horst Feistel (IBM) DES'in temelini oluşturan Lucifer algoritmasını geliştirdi.
- 1976'da DES (Data Encryption Standard), ABD tarafından FIPS 46(Federal Information Processing Standard) standardı olarak açıklandı.
- 1976 Whitfield Diffie ve Martin Hellman Açık Anahtar sistemini anlattıkları makaleyi yayınladılar.
- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.

Kriptolojinin Tarihçesi

- 1985'de Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif ettiler.
- 1990'da Xuejia Lai ve James Massey: IDEA algoritmasını buldular.
- 1991'de Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı.
- 1995'de SHA-1 (Secure Hash Algorithm) özet algortiması NIST tarafından standart olarak yayınlandı.
- 1997'de ABD'nin NIST (National Institute of Standards and Technology) kurumu DES'in yerini alacak bir simetrik algoritma için yarışma açtı.
- 2001'de NIST'in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standart haline getirildi.

2.1 Şifre Bilimi ve Şifreleme Teknikleri

- Kriptoloji

Kriptografi:
Geleneksel olarak bilginin anlaşılabilir bir formdan anlaşılamaz bir forma dönüştürülmesi.

Kriptoanaliz:
Şifreleme mekanizmalarının nasıl bozulacağını veya deşifre edileceği üzerine çalışan bir bilim dalıdır.

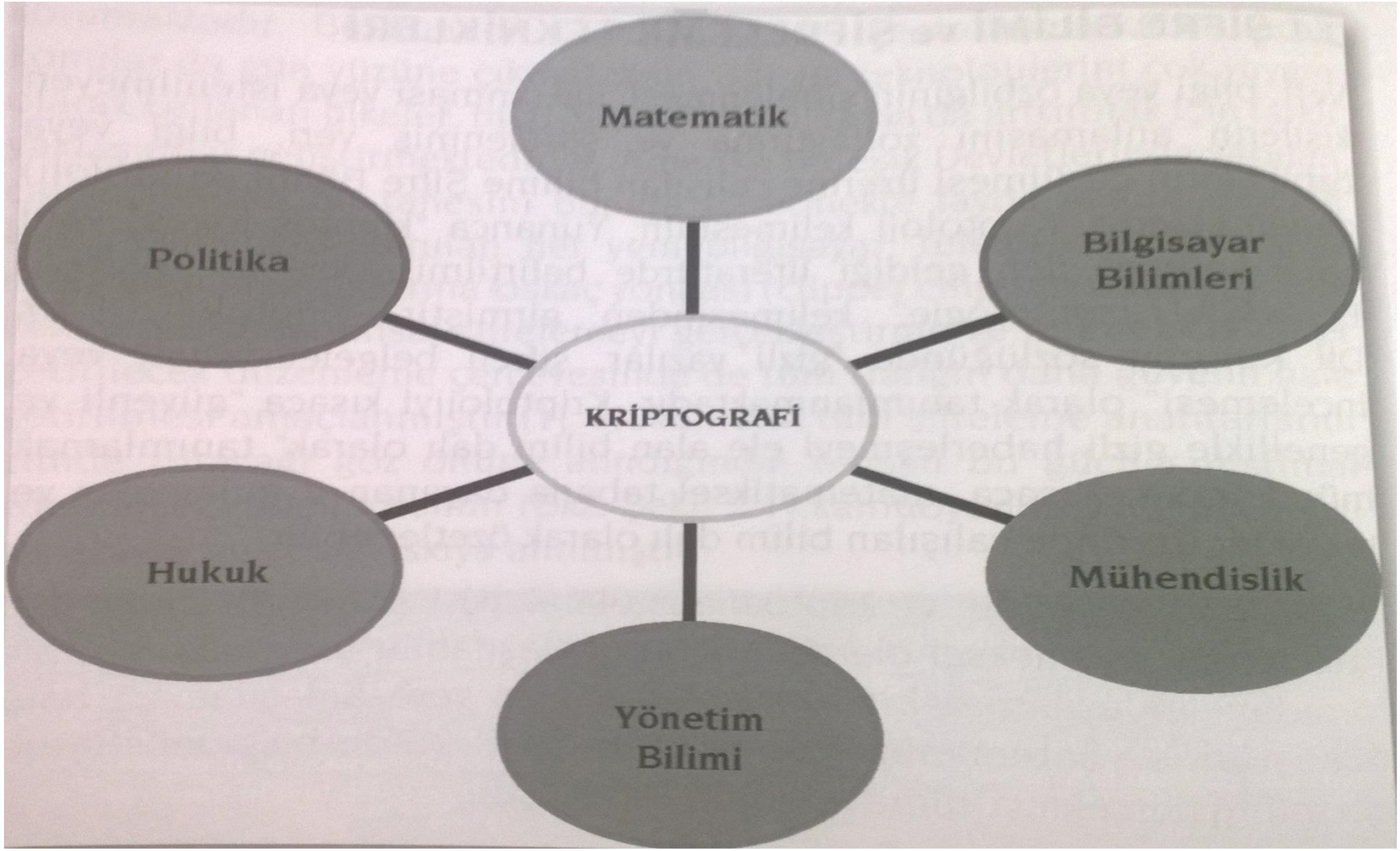
2.1 Şifre Bilimi ve Şifreleme Teknikleri

KRİPTOGRAFİ;

- Birçok disiplinin bir araya geldiği bir konudur. Özellikle;
  - Matematik
  - Bilgisayar Bilimleri
  - Mühendislik
  - Yönetim Bilimi (idari konular)
  - Hukuk
  - Politika

bu disiplinlerin başında gelmektedir.

2.1 Şifre Bilimi ve Şifreleme Teknikleri

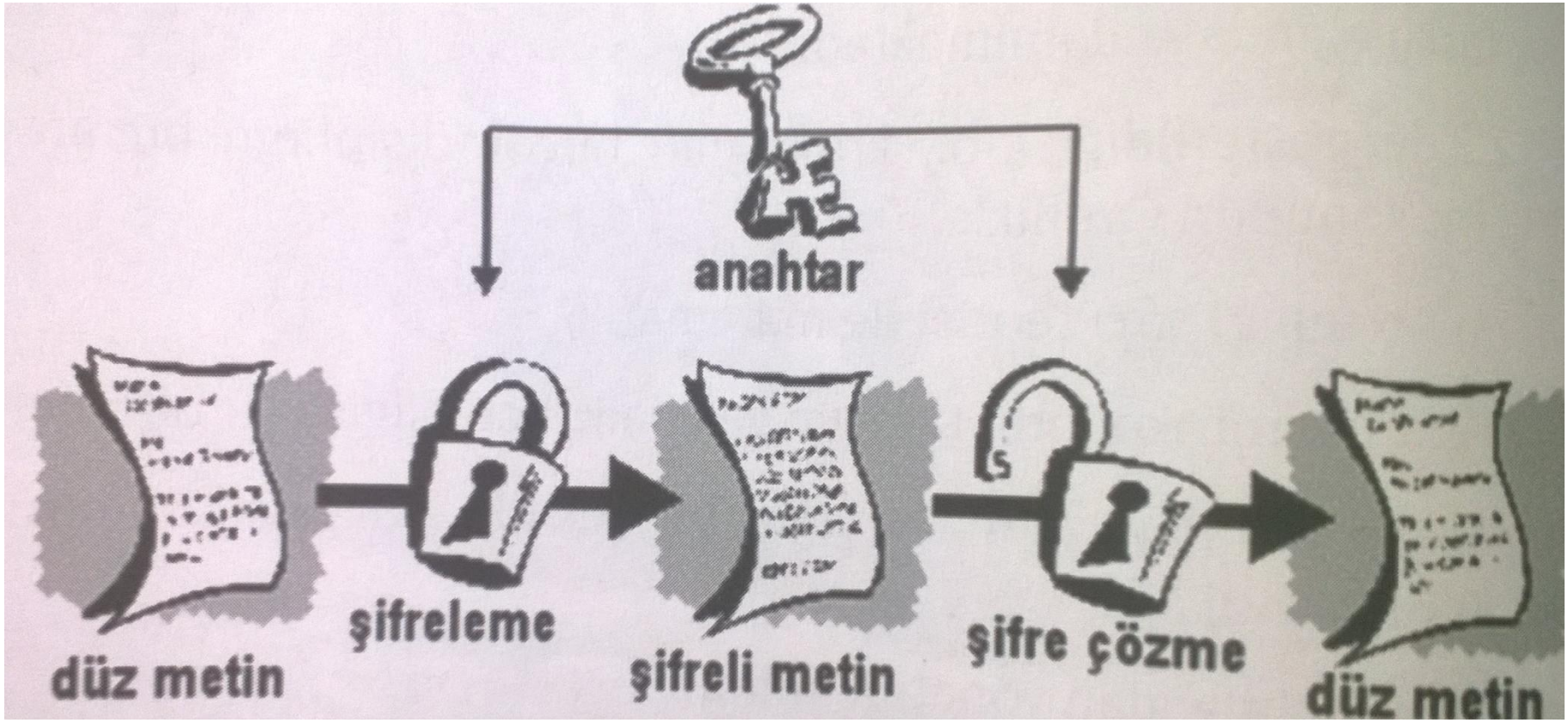


2.1 Şifre Bilimi ve Şifreleme Teknikleri

Şifreleme Kavramları

- ***Düz metin (plaintext):*** Kriptoloji sisteminin girdisi olan bilgidir
- ***Şifreli metin (ciphertext):***okunamaz anlaşılamaz çıktı
- ***Şifreleme (encrytion):*** düz metni şifreli metne çevirme süreci.
- ***Şifre***
- ***Kod kırma veya kod çözme (code breaking)***
- ***Anahtar (key)***

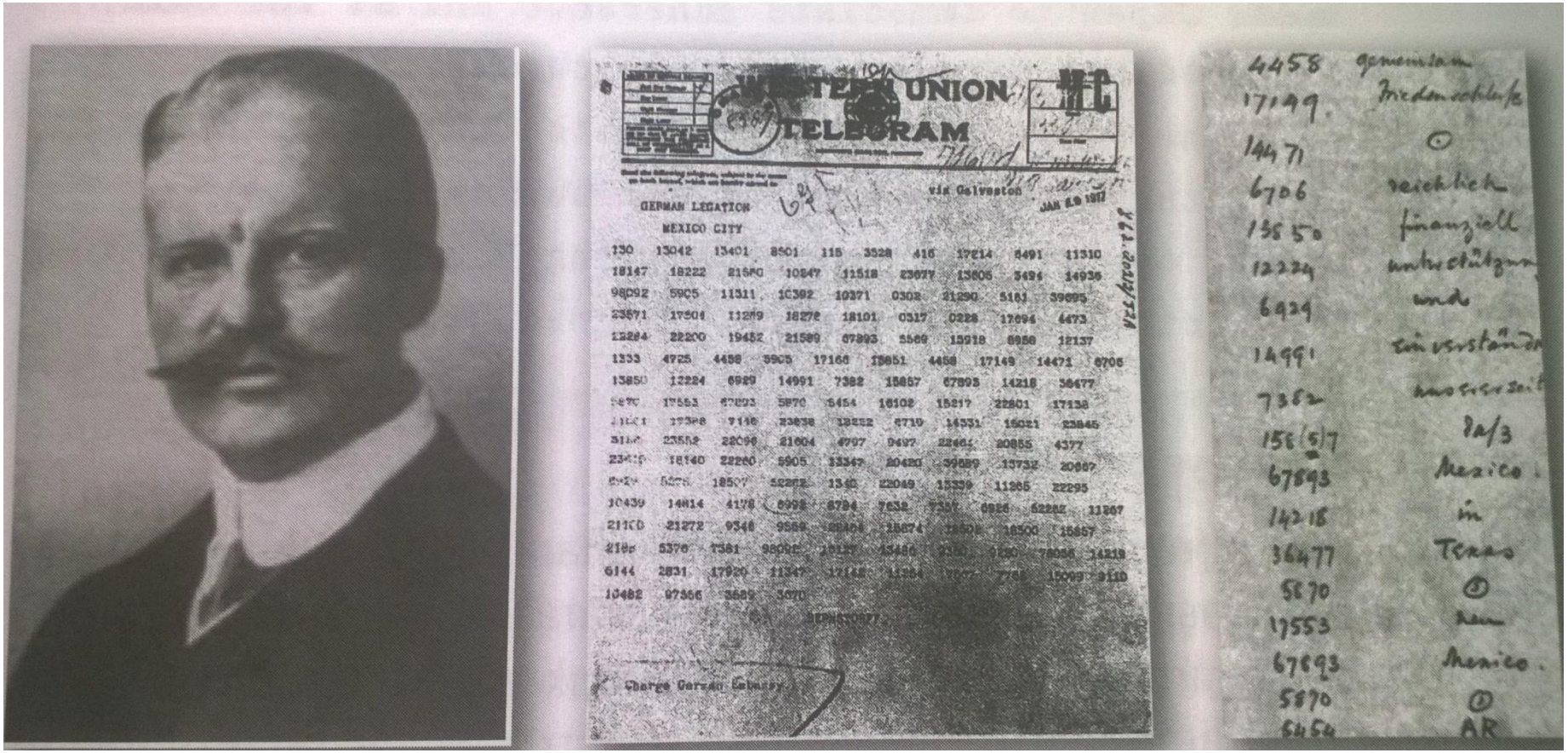
2.1 Şifre Bilimi ve Şifreleme Teknikleri



2.1 Şifre Bilimi ve Şifreleme Teknikleri

- **Tarihten örnek;**
  - **Zimmerman Paragrafı:** 16 Ocak 1917 de 1.Dünya savaşı sırasında alman imparatorluğunun dışişleri sekreteri Arthur Zimmermann tarafından Meksika'daki Alman elçiliğine gönderdiği şifreli telgraf. İngilizler tarafından kriptoanaliz ile çözülmüştür.
  - Bu metnin çözülmesi ile Almanya'nın Meksika'ya bir ittifak önerisinde bulunduğu anlaşılmış ve ABD'nin savaşa girmesi hız kazanmıştır.

2.1 Şifre Bilimi ve Şifreleme Teknikleri



2.1 Şifre Bilimi ve Şifreleme Teknikleri

- Genel olarak şifreleme yaklaşımları ikiye ayrılır.

Gizli Anahtarlı (simetrik)

Hem şifreleme hem de şifre çözmek için tek bir anahtar kullanılır.

<u>En popüler yaklaşım</u>: DES (Data Encryption Standard)

Açık anahtarlı (asimetrik)

Kullanıcı hem açık anahtara hemde gizli bir anahtara sahiptir .

<u>En popüler yaklaşım:</u> RSA (Rivest Shamir and Adleman)

- Simetrik algoritmaları hızlı mesaj şifrelemede,
- Asimetrik yaklaşımlarda yavaş olduklarından dolayı anahtar şifrelemede kullanılmaktadır.

2.1 Şifre Bilimi ve Şifreleme Teknikleri

KRİPTOANALİZ:

- Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içerir.
- İşlemler sırasında yoğun istatistik , matematik ve bilgisayar gücüne ihtiyaç duyulmaktadır.
- Kriptoanaliz yöntemleri kaba kuvvet ve diferansiyel kriptoanaliz olmak üzere ikiye ayrılır.

2.1 Şifre Bilimi ve Şifreleme Teknikleri

- **Kaba Kuvvet** bir şifreleme algoritması tarafından kullanılabilecek tüm anahtarları, tek tek veya belirli bir mantık çerçevesinde deneyerek kullanılmış olan şifreleme yaklaşımını bulma yaklaşımıdır.
- **Diferansiyel Kriptoanaliz** bilinen açık mesaj çiftleri arasındaki farkların hesaplanması temeline dayanır.

2.1 Şifre Bilimi ve Şifreleme Teknikleri

Şifreyi kırmaya yönelik ataklar:

1. Salt şifreli metin (chipertext); Kriptoanalistin sadece bir grup şifreli metne erişiminin olduğu durumdur.
2. Bilinen düz metin (known plaintext) : Kriptoanalist bir grup düz metne ait şifreli metne sahiptir.
3. Seçilebilen düz metin veya şifreli metin (chosen plaintext or chiper text): Atak eden kişinin kendisinin rasgele seçtiği düz metne karşılık gelen şifreli metinleri elde edbileceği kriptoanaliz senaryosudur.
4. Uyarlanır seçili düz metin (adaptive chosen plaintext): düz metin rasgele seçilmeyip daha önceki şifre çözmelerde öğrenilen bilgiler ışığında seçilir.
5. İlişkili anahtar atağı (related key attack): iki farklı anahtarla şifrelenmiş iki şifreli metne sahip olunan durumdur.