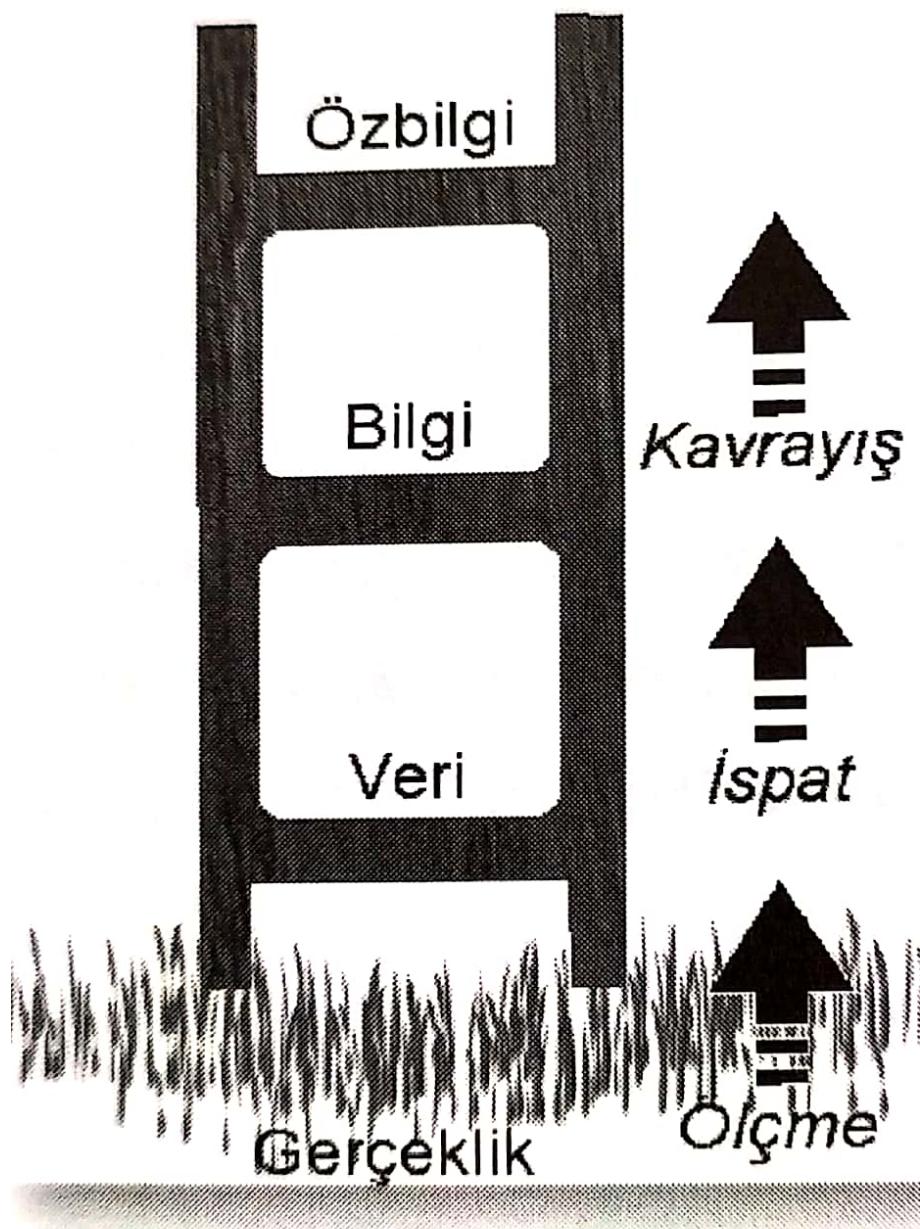


Bilgi ile ilgili birçok şey söylenebilir. Bilginin doğası ile ilgili aşağıda derlenen sözler, bilginin değerini ve boyutlarını bir kez daha gözler önüne sermek açısından faydalı olabilir [10]. Bilgi;

- Boşlukta ve zamanda yer kaplar.
- Gürültü çıkarmadan hareket edemez.
- Hareketi için enerji gereklidir.
- Yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Hem maddesiz biçim; hem biçimde maddedir.
- Ağırlığa sahiptir. Bir giga bayt, bir parmak izinden daha az ağırlıktadır.
- Zaman içinde hareketli veya donmuş olabilir.
- Bir soruya tatmin edici, belki de rahatsızlık verici bir cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için gerekli bilgi birbirine eşittir.
- Katı hale sahiptir; donarak karşılaşır (depolama).
- Sıvı hale sahiptir; akar (iletişim).
- Bir yerlerde bilgi hareket eder; evren gümbürder ve gerceği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma, baş sallama, bakış veya iç çekistir ve
- Rastsallık denizinde parlar.

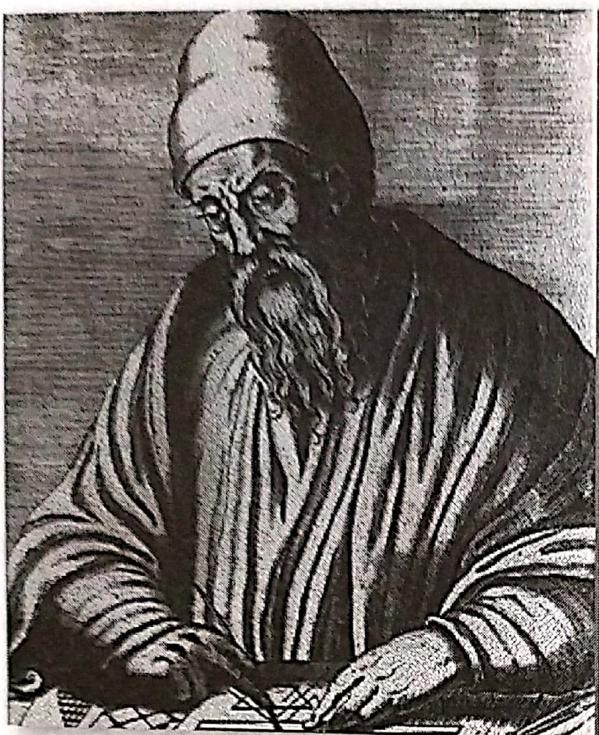
Hikmet



Şekil 1.1. Gerçeklikten hikmete ulaşmak için asılması gereken bilgi basamakları

1.1 VERİ

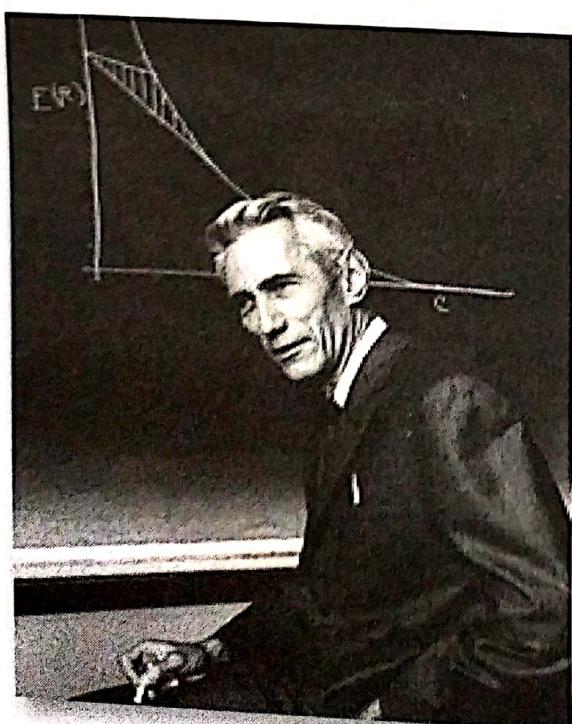
Verinin; İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinden (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey") gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir [17]. Dilimizde ise veri "verilen şey" anlamında kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.



Şekil 1.3. Öklid (M.Ö. 325 – 270) ($\Delta\text{E}\Delta\text{OMENA} = \text{DEDOMENA} = \text{DATA}$)

1.2 BİLGİ

Bilgi; verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bu aşamada, veri ve ilişkili olduğu konu, bilgi üretecek şekilde bir araya getirilir. İşlenmiş veri olarak da ifade edilebilecek bilgi, Shannon tarafından "bir konu hakkında var olan belirsizliği azaltan bir kaynak" olarak tanımlanmıştır [18]. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.



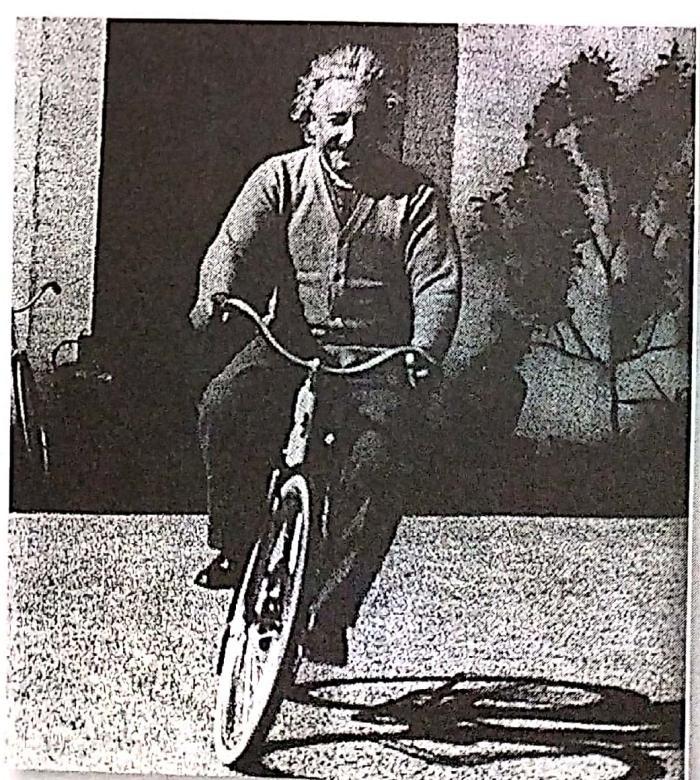
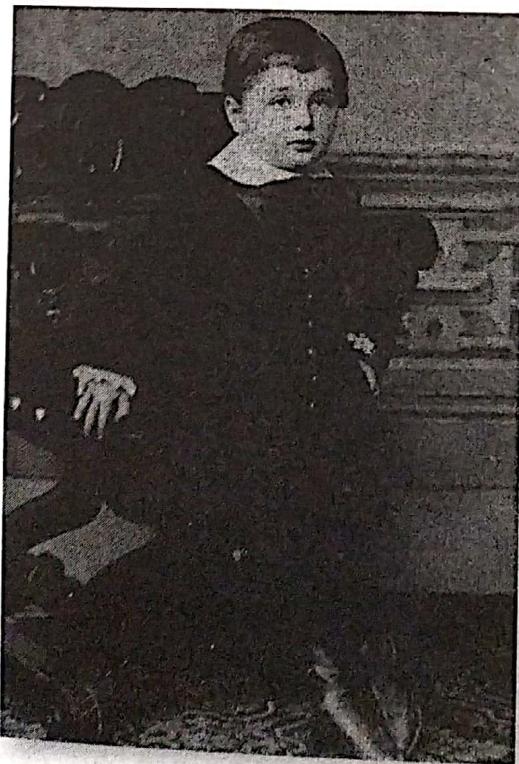
Şekil 1.4. Claude Elwood Shannon (1916 – 2001), Bilgi: Belirsizliği Azaltır.

1.3 ÖZBİLGİ (KNOWLEDGE)

Özbilgi; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip işlenmesiyle bilgi elde edilse de; özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir. Özbilgi, ne olduğunu (know-what), niçin olduğunu (know-why), nasıl olduğunu (know-how) ve kim olduğunu (know-who) bilmek şeklinde dört sınıftan oluşur. Ne olduğunu bilmek, gerçeklerin toplamıdır ve bilgiye en yakın olan sınıftır. Niçin olduğunu bilmek, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel özbilgidir. Nasıl olduğunu bilmek, bir şeyi yapabilme becerisidir. Kimin olduğunu bilmek, kimin neyi ve kimin neyi nasıl yapılacağını bildiğini bilmek olarak özetlenebilir [19].

1.4 HİKMET

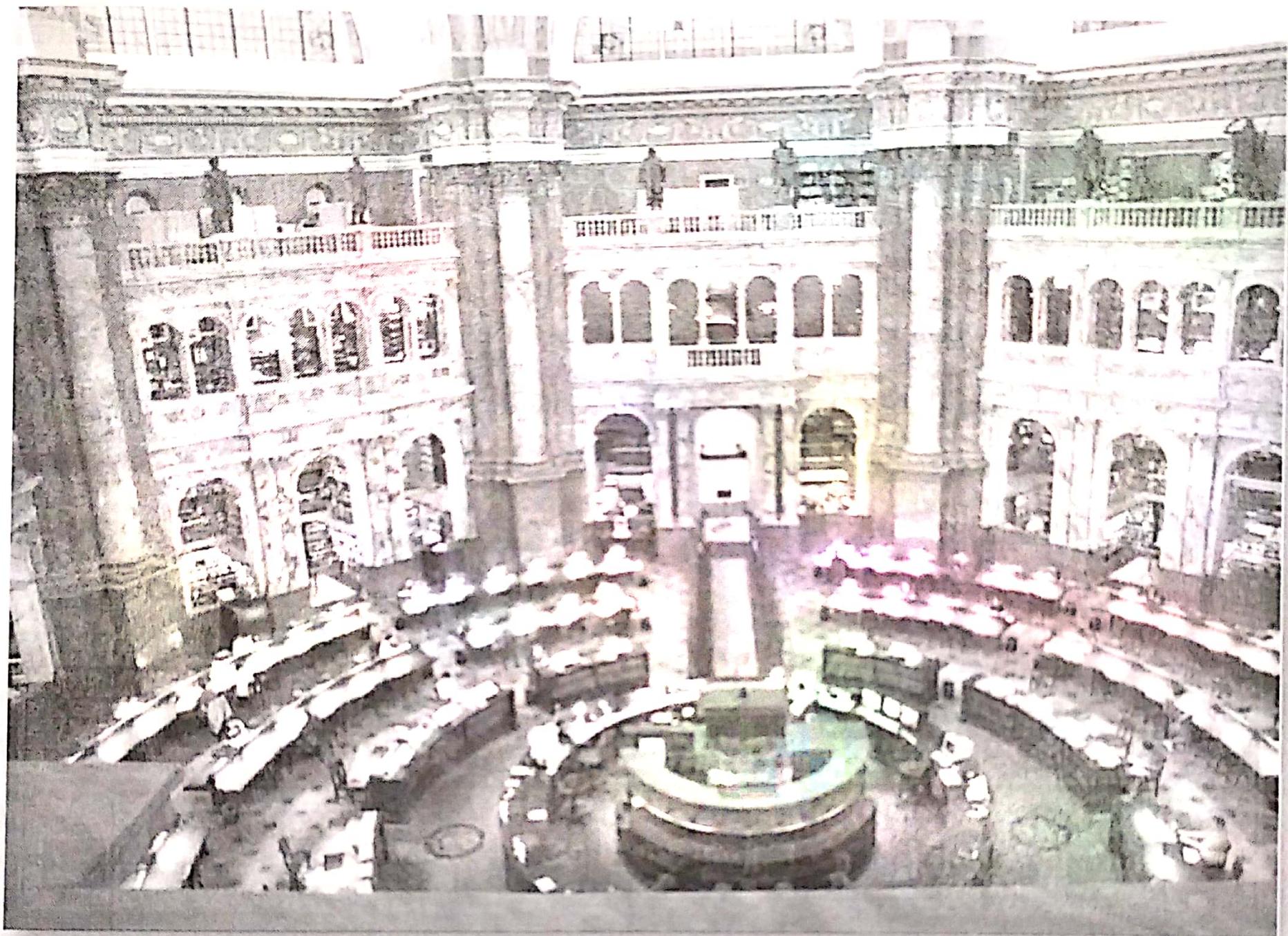
Hikmet (wisdom); tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür [20]. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır [21]. 1954 yılında Einstein hikmet için, "Hikmet, eğitim ve öğretimin ürünü değil; onu elde etmek için ömür boyu süren bir girişimin sonucudur" demiştir [22].



Şekil 1.5. Albert Einstein (1879–1955)



Şekil 1.6. Popüler Internet arama motorları



Şekil 1.7. Amerikan Kongre Kütüphanesi (The Library of Congress)

Çizelge 1.3. Şubat 2005 itibarıyle bazı haber sitelerinde sunulan çevrimiçi sayfa sayıları [26]

Internet Haber Sitesi	Ülke	Sayfa Sayısı
bbc.co.uk	İngiltere	1.270.000
cnn.com	ABD	1.220.000
hurriyetim.com.tr	Türkiye	834.000
usatoday.com	ABD	813.000
timesonline.co.uk	İngiltere	740.000
guardian.co.uk	İngiltere	639.000
washingtonpost.com	ABD	631.000
nytimes.com	ABD	627.000
cbsnews.com	ABD	491.000
independent.co.uk	İngiltere	346.000
sabah.com.tr	Türkiye	298.000
msnbc.com	ABD	298.000
ntvmsnbc.com	Türkiye	86.700
milliyet.com	Türkiye	25.400

ESKİ YOL



Bilgiyi aramak zorundasınız

YENİ YOL



Abone olduğunuz bilgi size gelir

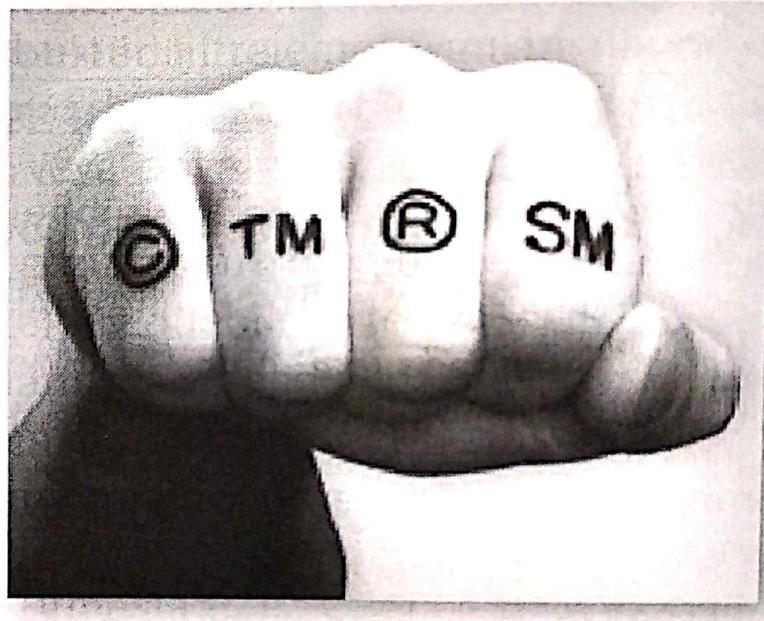
Şekil 1.8. RSS'den önce ve sonra

Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanmasını gerekmektedir. Bilgi, en basit benzetme ile para gibi bir metadır. Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi zor; aynı zamanda elde tutulması da zor bir metadır. Fikri mülkiyet (entellektüel mülk, intellectual capital, property) olarak tanımlanan bu meta, bir kurumun bilgi ve özbilgi varlığıdır [28]. Bu mülkü'n korunması, hayatı bir önem arz etmektedir. Bu korunma, bilgi kullanımındaki karmaşayı, yozlaşmayı ve kötüye kullanımımı önleyeceği gibi; bilgiyi bir çaba göstererek elde eden tüzel veya gerçek kişilerin haklarının korunmasını da sağlayacaktır. Bu sayede firmalar, çetin rekabet ortamında, sahip oldukları fark yaratan ve aynı zamanda koruyabildikleri entellektüel mülk ile avantajlı konumlarını koruyabilmektedirler [29].



Şekil 1.9. Fikri mülkiyet günümüzün ve geleceğin en önemli varlığıdır

İşte bu yüzden patent, telif hakkı ve ticari marka gibi haklar, fikri mülkü korumak amacıyla oluşturulmuştur [30]. Fakat bilginin korunması, daha doğrusu bilginin güvenliği, özellikle elektronik ortamda çok daha kapsamlı bir konudur.



Şekil 1.10. Fikri mülkün korunması

Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark yaratması nedeniyle bilgi, korunması gereken bir varlık olarak görülmektedir [31]. Bu açıdan bilginin korunmasına yönelik olarak, bilgi güvenliği, dünya gündeminde olan ve bundan sonra daha da önemini artırarak devam eden bir konu olarak karşımıza çıkmaya devam edecktir.

Bu bölümü gelecekte bilgi erişiminin nasıl olabileceğini gösteren bir uyarlama ile bitirelim. Her ne kadar Şekil 1.11, içerisinde güzel bir espri içerse de; geleceğe ışık tutacağı da düşünülmektedir.



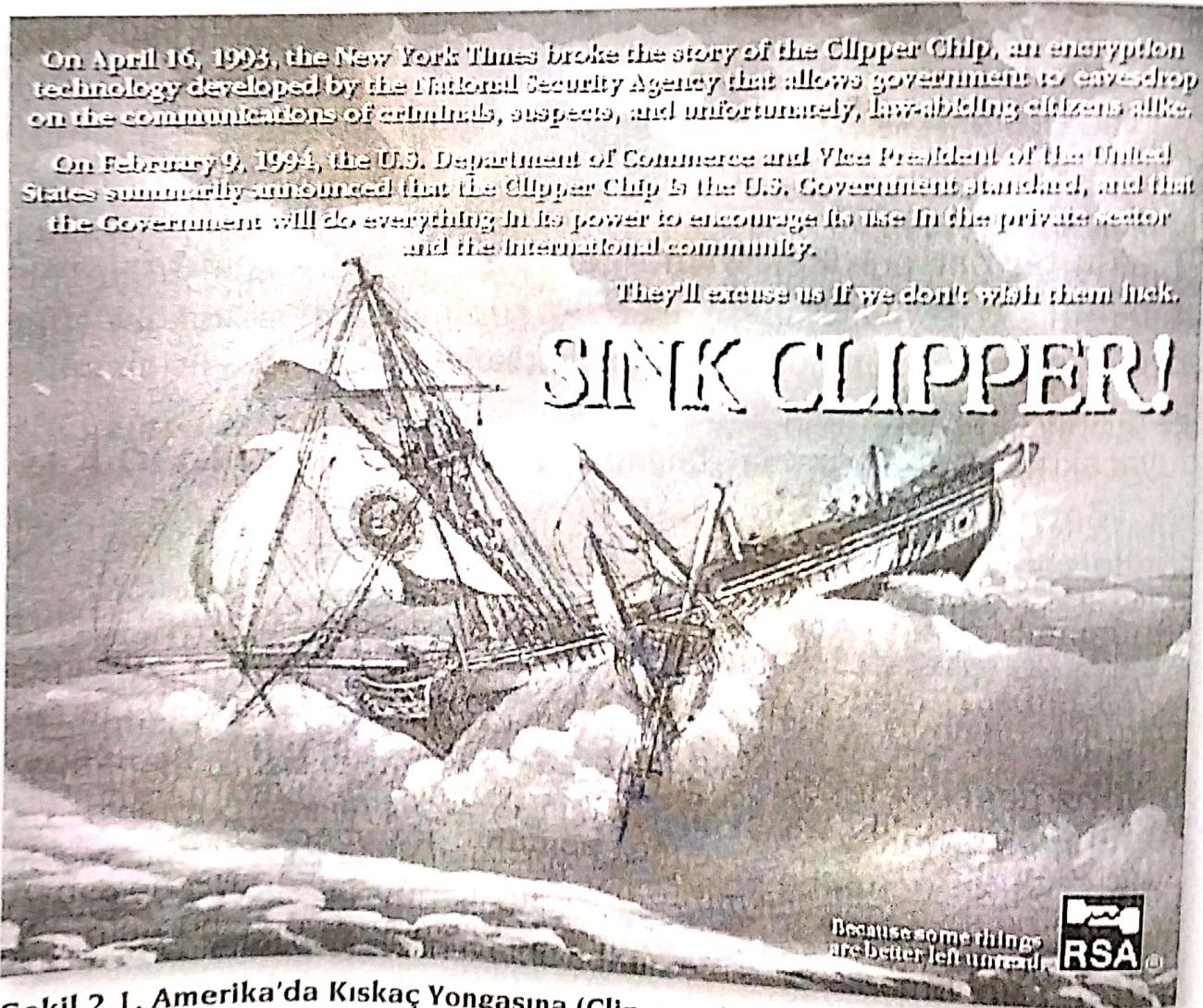
BİLGİ GÜVENLİĞİ TARIHÇESİ

Tarihi bir perspektiften konu incelendiğinde herhangi bir uygarlık belirli bir seviyeye ulaşır ulaşmaz kriptografinin ortaya çıktığını görmek mümkündür. Sosyal hayatın herhangi bir anında iki veya daha fazla kişi bilgi alışverişi sırasında mahremiyete er ya da geç ihtiyaç duyacaktır. Bu durumda bilginin şifrelenmesi uygulanılabilecek tek yöntem olarak gözükmektedir. Gelişmelere göz atıldığında şifrelemenin sanıldığı gibi sadece hükümet veya askeri ihtiyaçlar karşısında olduğu düşünülmemelidir. Sivil veya amatör birçok yaklaşımda yepyeni ve etkin uygulama sahaları bulunmaktadır.

Bilişim teknolojilerinin kullanımının hızla yaygınlaşlığı ve arttığı günümüzde; bilgi, bilgisayar ve bilgisayar sistemleri güvenliği, en önemli ve kritik konuların başında yer almaktadır. Konunun önemini anlamak için bilgi ve güvenlik kavramlarının ve felsefesinin iyi anlaşılması ve üzerinde ayrıntılı düşünülmesine ve analiz edilmesine ihtiyaç vardır. Tarihi bir perspektiften bakıldığından bilgi güvenliğinin insanlığın var olduğu zamandan beri uygulana gelen ilk örneği şifrelemedir. Şifrelemenin, tarihin ilk dönemlerinden beri kullanılıyor olması, şifrelenen bilginin öneminin farkında olunduğunun bir işaretidir.

Şifreleme sadece eski zamanlarda kullanılan bir yöntem değildir. Günümüzde de bilgi güvenliği açısından önemini artan bir şekilde

korumaktadır. Bu konuda oldukça güncel ve tartışma oluşturacak konular da gün yüzüne çıkmaktadır. Bilişim teknolojilerini çok yaygın olarak kullanan ülkeler, bilgi güvenliklerini daha da artırmak için farklı yaklaşımlar geliştirmektedirler. Amerika Birleşik Devletlerinde yapılan çalışmalarlardan bir tanesini burada zikretmekte fayda vardır. ABD'de haberleşmede kullanılan her yeni bilgisayar, telefon, modem veya diğer iletişim aygıtlarına kıskaç yongası (clipper chip) adında yonga eklerek donanımsal şifrelemeyi gerçekleştireme ve bununla beraber getirilecek düzenleme çerçevesinde de tüm trafiğin daha güvenli hale getirilmesi amaçlanmıştır [1]. Hükümetin tüm şifreleme anahtarlarını elinde tutacağı göz önüne alındığında; oluşan bu gücün suiistimal edebileceği düşüncesinin (Bkz. Şekil 2.1) kamuoyunda yaygınlaşması sebebiyle bu proje askıya alınmıştır.



Şekil 2.1. Amerika'da Kıskaç Yonasına (Clipper Chip) karşı tepkileri dile getiren bir ilan

Ülkemizde sayısallaşma oranı yüksek olmasa da, kritik kamu kurum ve kuruluşlarında TÜBİTAK-UEKAE tarafından geliştirilen milli kripto cihazları ile haberleşme yapıldığı, ülkemizde de bilgi güvenliği konusuna önem veren kurum ve kuruluşların sayısının her geçen gün

2.1 ŞİFRE BİLİMİ ve ŞİFRELEME TEKNİKLERİ

Veri, bilgi veya özbilginin şifrelenmesi, saklanması veya istenilmeyen kişilerin anlamasını zorlaştırmaya ve şifrelenmiş veri, bilgi veya özbilgilerin çözülmESİ ÜZERİNE ÇALIŞILOLAN BİLİMİ ŞİFRE BİLİMİ (KRIPTOLOJİ) DENİLMEKTEDİR. KRIPTOLOJİ KELİMESİNİN, YUNANCA “KRYPTOS LOGOS” YANI “GİZLİ KELİME” DEN GELDİĞİ LITERATÜRDE BELİRTİLMİŞ OLSA DA DİLİMİZE FRANSIZCA “CRYPTOLOGIE” KELİMESİNDEN GİRMİŞTİR. KRIPTOLOJİ, TÜRK DİL KURUMU SÖZLÜĞÜNDE “GİZLİ YAZILAR, ŞİFRELİ BELGELER BİLİMİ Veya İNCELEMESİ” OLARAK TANIMLANMAKTADIR. KRIPTOLOJİYİ KİSACA “GÜVENLİ VE GENELLİKLE GİZLİ HABERLEŞMЕYİ ELE ALAN BİLİM DALI OLARAK” TANIMLAMAK MÜMКÜNDÜR. KİSACA, MATEMATIKSEL TABANA DAYANAN UYGULAMALAR VE TEKNİKLER ÜZERİNDE ÇALIŞILOLAN BİLİM DALI OLARAK ÖZETLENEBİLİR.

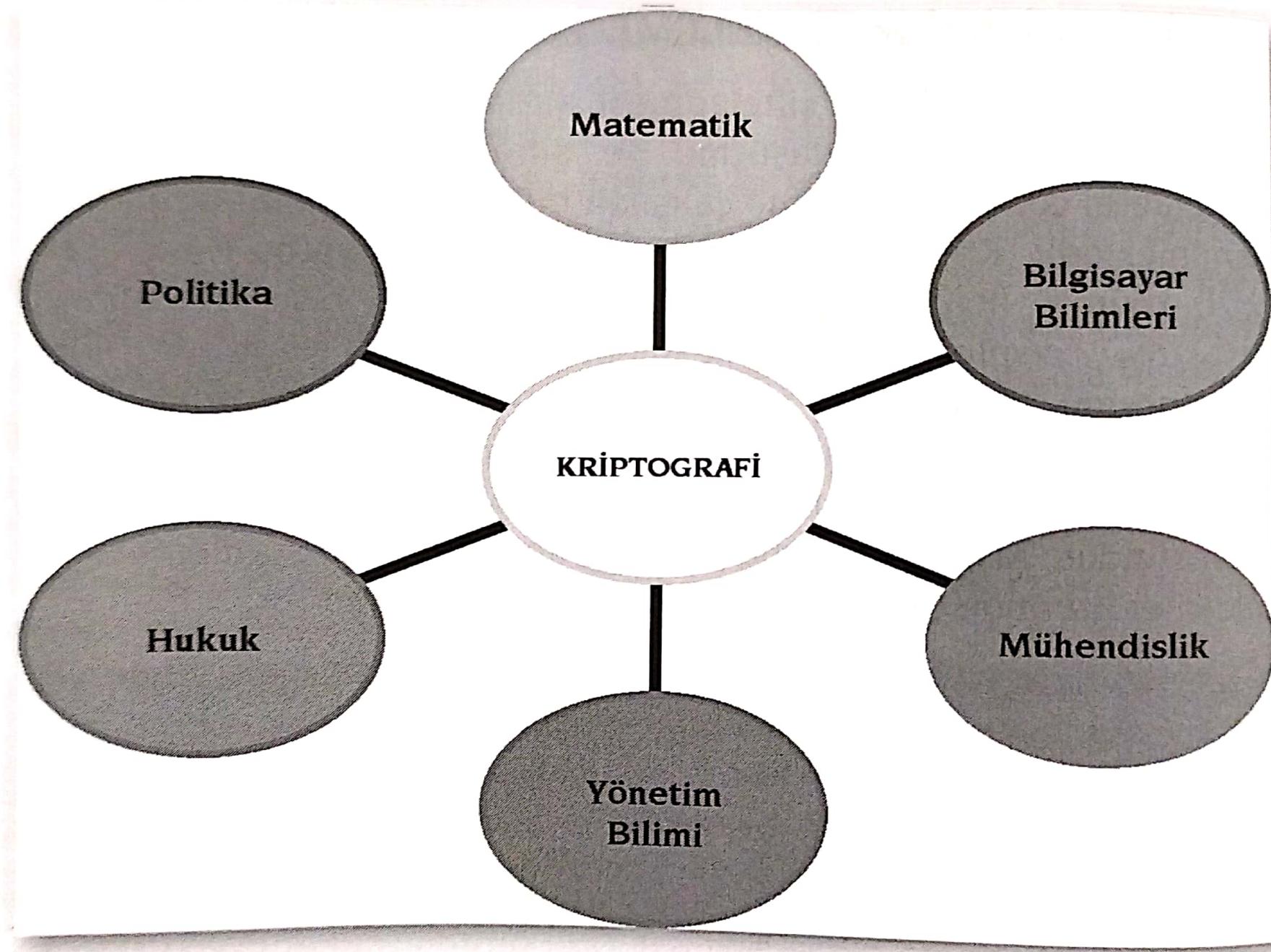
Kriptoloji, kriptografi ve kriptoanaliz olarak iki kısımda incelenebilir. Kriptografi, geleneksel olarak, bilginin anlaşılabilir (normal olan) bir formdan, anlaşılamaz bir forma (okunamaz veya anlaşılamaz) hale dönüştürme yöntemlerini içermektedir. Şekil 2.3'de bu dönüştürme işleminin gerçekleştirilme adımları verilmiştir.

Kriptografi, geçmişte polis, asker ve özel birimler ile diplomatlar için haberleşmelerde gizliliği temin için kullanılmış olsa da günümüzde, teknolojinin hayatımızın bir parçası haline gelmesi ile gizli ve güvenilir bir ortamda tutulması gereken her türlü veri, bilgi veya özbilginin şifrelenerek saklanmasıyla başlayıp, e-imza, e-banka, e-ticaret vb. gibi birçok farklı alanda kullanılmaktadır.

Şekil 2.2'de gösterildiği gibi, kriptografi birçok disiplinin bir araya geldiği bir konudur. Özellikle,

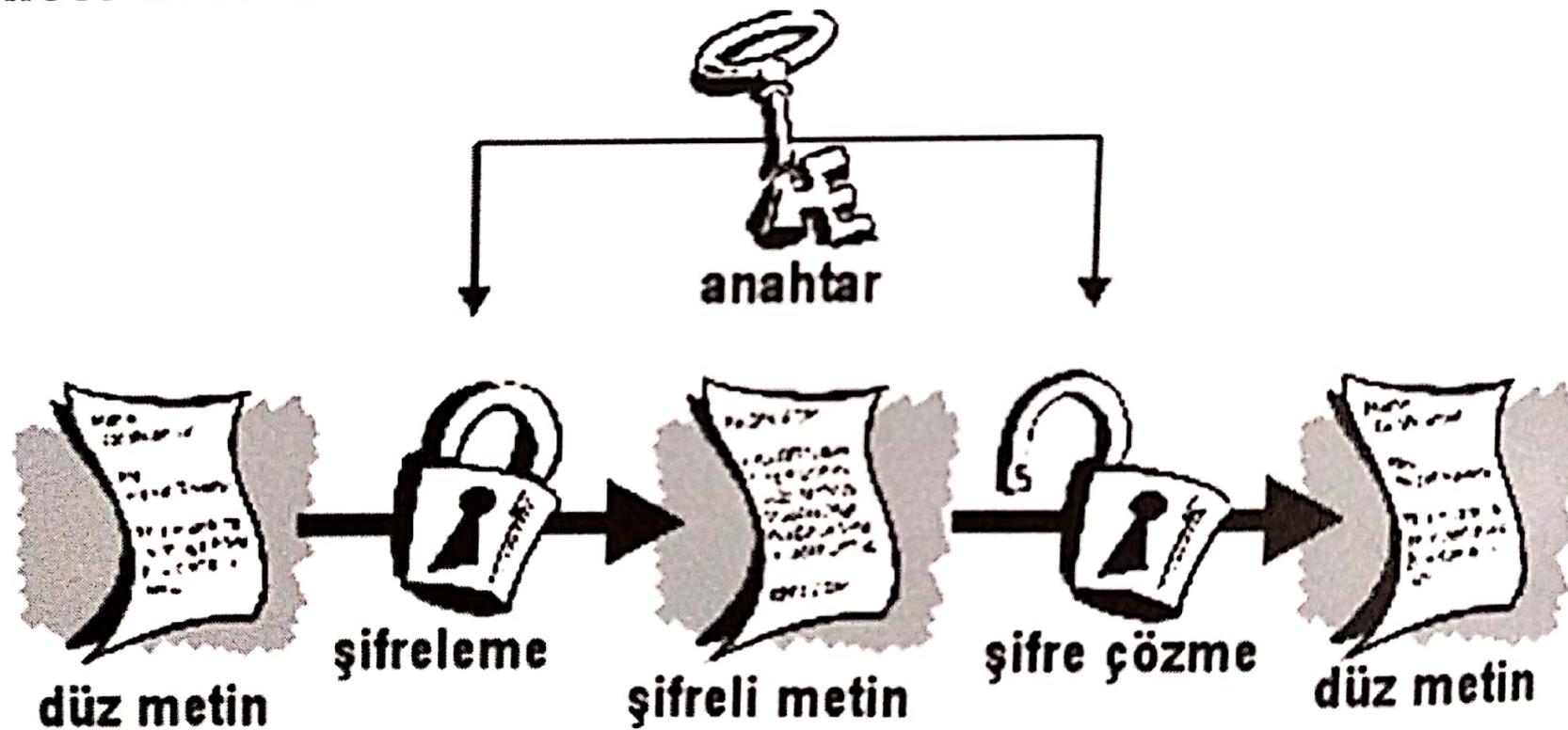
- Kullanılan temel sayı teorisi ile matematik;
- Kriptografik protokollerin tasarım ve analizinde bilgisayar bilimleri;
- Bu protokollerin güvenli ve etkin bir şekilde gerçekleştirilemesini sağlayan mühendislik;
- İdari konuları ele alan yönetim bilimi;
- Patent, sayısal imzanın geçerliliği ve yükümlülük gibi konular için hukuk ve
- Yöntemlerin ihracının denetimi, şifreleme kullanımının sınırlandırılması ve endüstri standartlarının belirlenmesi gibi konular için politika,

bu disiplinlerin başında gelmektedir.



Şekil 2.2. Criptografi ve etkileştiği disiplinler

Kriptoanaliz, şifreleme mekanizmalarını nasıl bozacağını veya deşifre edileceği üzerine çalışılan bir bilim dalıdır.



Şekil 2.3. Şifreleme – Şifre Çözme İşlemleri

Şifrelemede kullanılan düz metin, şifreli metin, şifreleme, şifre çözme, şifre ve anahtar terimleri sırasıyla açıklanmıştır:

Düz metin (plaintext), kriptoloji sistemlerinin girdisi olan bilgidir. Bu bilgi, diplomatik bir mesaj, bir banka işlemi, bir e-posta içeriği, hatta bir günlüğe yazılmak istenen not olabilir.

Şifreli metin (ciphertext) ise, kriptoloji sistemlerinin okunamaz veya anlaşılamaz çıktısıdır.

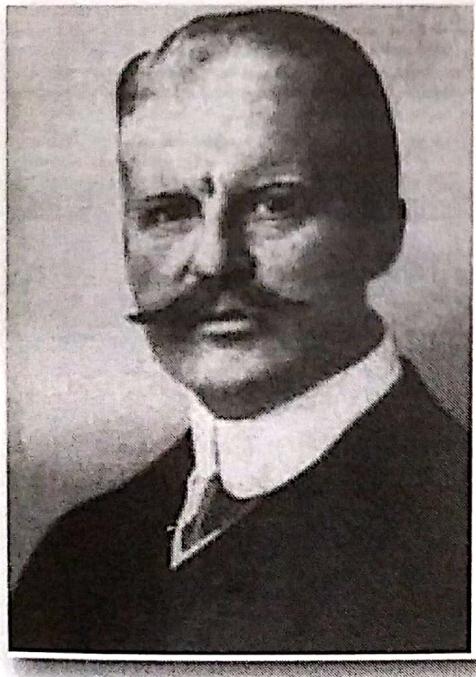
Şifreleme (encryption), düz metni şifreli metne çevirme sürecidir. Şifre çözme (decryption) ise şifreli metinden düz metin elde etme sürecidir.

Şifre ise, kullanılan şifreleme ve şifre çözme algoritması veya anahtarıdır. Konuşma dilinde kullanılan kod kelimesi de şifre yerine geçmektedir.

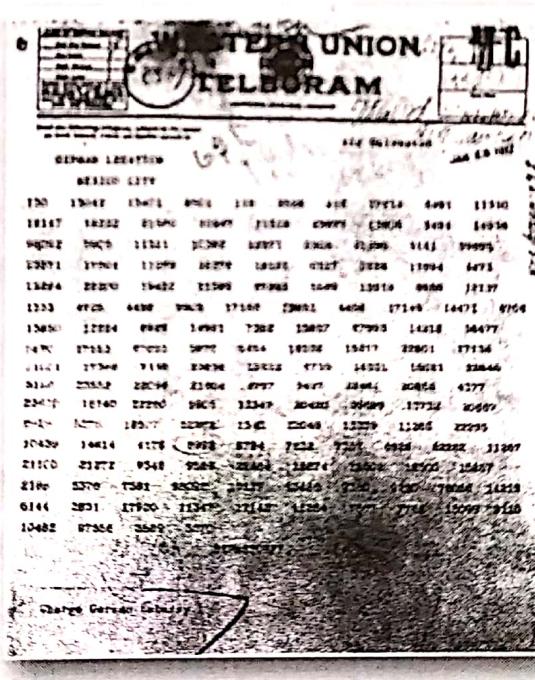
Kod kırma veya kod çözme (code breaking) gibi deyimler bu alanda çalışan kişiler tarafından kullanılmaktadır.

Anahtar (key) ise şifreli metnin (veya bazı durumlarda düz metnin) nasıl elde edildiğine dair bilgi parçasıdır. Bu anahtara sahip olan kişi duruma göre şifreli metinden düz metni yada düz metinden şifreli metni elde edebilir.

Bu kavramlarla ilgili tarihi ve çok önemli bir örnek verilebilir. Şekil 2.4'de şifreleme tarihinde çok önemli bir yeri olan ve "Zimmerman Telgrafı" olarak adlandırılan şifreli metin gösterilmektedir. 16 Ocak 1917'de I. Dünya Savaşı sırasında Alman İmparatorluğu'nun Dışişleri Sekreteri Arthur Zimmermann tarafından Meksika'daki Alman Elçiliğine gönderdiği şifreli telgraf, İngilizler tarafından ele geçirilmiş ve Şekil 2.4 (c)'de gösterildiği gibi yapılan kriptoanaliz ile çözülmüştür. Burada Arizona'nın Alman kod karşılığı bulunmadığından kelime hecelerine ayrılmıştır.



(a)



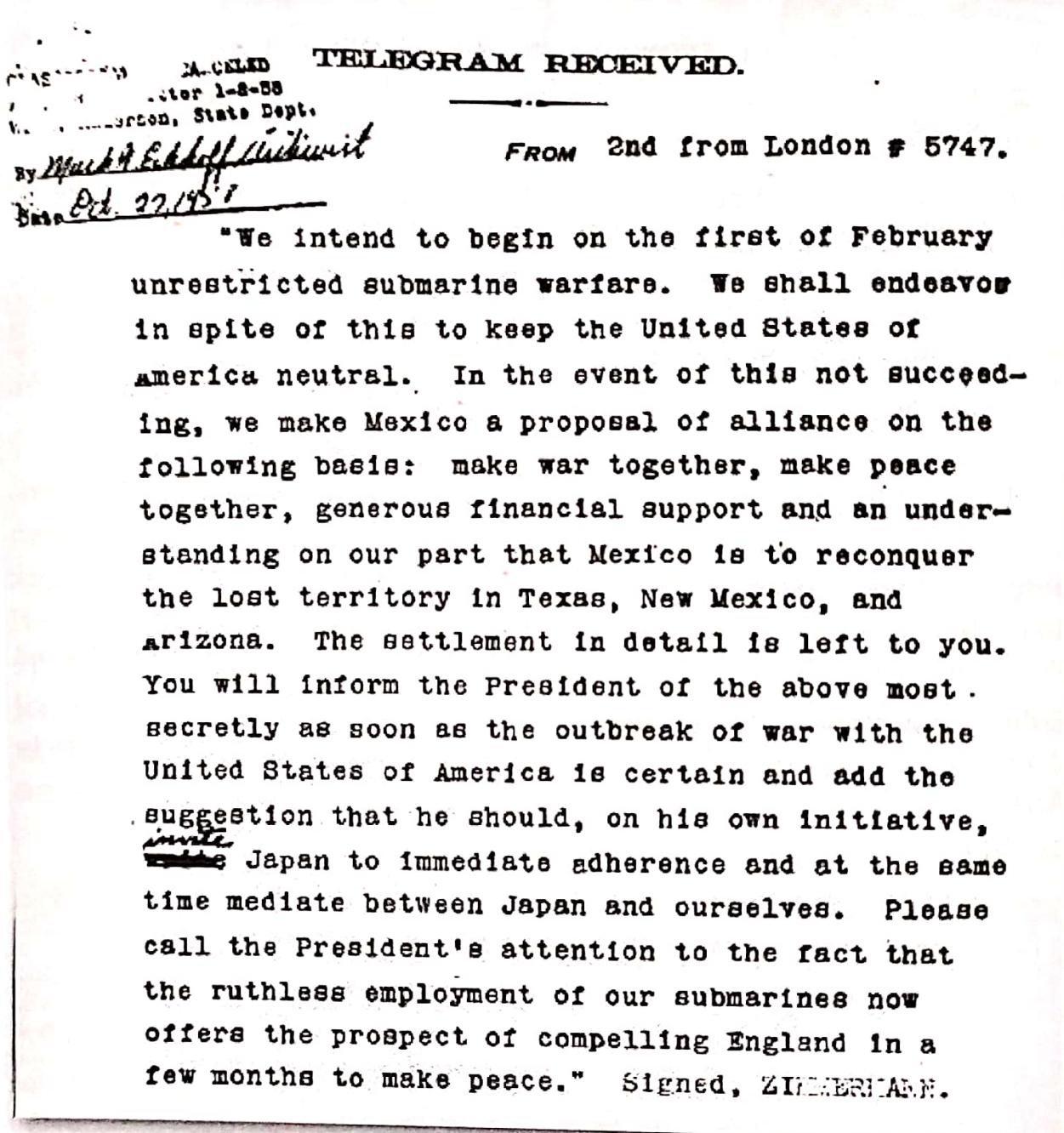
(b)

4458	gemeinsam
17199.	Mexikanische
14471	O
6706	reiehlich
13850	finanziell
12234	unterstützung
6429	und
14991	zu verstehen
7362	ausser seit
158(5)7	Pa/3
67893	Mexico.
14218	in
36477	Texas
5870	O
17553	Reich
67893	Mexico.
5870	O
5454	AR

(c)

Şekil 2.4. Zimmerman şifreli metni (a) Arthur Zimmermann (1864–1940) (b) Şifreli telgrafın aslı (şifreli metin) (c) Kriptoanaliz çalışmaları

Şekil 2.5'de İngilizler tarafından çözülen ve İngilizceye çevrilen düz metin gösterilmektedir. Bu metinin açığa çıkması ile Amerika Birleşik Devletleri, kendisine karşı Almanya'nın Meksika'ya bir ittifak önerisinde bulunduğu anlamış ve bu da Amerika'nın I. Dünya Savaşına girmesini hızlandırmıştır.



Şekil 2.5. İngilizceye çevrilmiş düz metin

Şifreleme ve şifre çözme işlemlerinde kullanılan birçok algoritma, teknik ve yaklaşım mevcuttur. Genel olarak değerlendirildiğinde şifreleme yaklaşımları, gizli anahtarlı ve açık anahtarlı olmak üzere ikiye ayrılır. Gizli anahtarlı yaklaşımlar, simetrik yaklaşımlar olarak ta bilinmektedir. Bu yaklaşımda, hem şifreleme hem şifre çözme için tek bir anahtar kullanılır. En popüler gizli anahtarlı şifreleme yaklaşımı veri şifreleme standardı olarak isimlendirilen DES (Data Encryption Standard)'dır. Açık anahtarlı yaklaşımlar, asimetrik yaklaşımlar olarak

ta bilinmektedir. Kullanıcı bir çift anahtara yani hem açık bir anahtara hem de gizli bir anahtara sahiptir. Bu anahtarlar, özel (private) veya gizli ve genel (public) veya açık olarak da isimlendirilir. Açık (genel) anahtar herkese açıkken, gizli (özel) anahtar ise sadece kişiye özel olarak saklı tutulmaktadır. Şifreleme açık anahtarla yapılırken, şifre çözme işlemi gizli anahtarla yapılmaktadır. Bunun tersi de mümkündür. Açık anahtarlı şifreleme yaklaşımlarında en popüler yaklaşım RSA (Rivest, Shamir ve Adleman)'dır.

Simetrik ve asimetrik yaklaşımlar güvenlik unsurları açısından değerlendirildiğinde, simetrik algoritmaları hızlı mesaj şifrelemede, asimetrik yaklaşımların da yavaş olduklarından dolayı anahtar şifrelemede kullanılmaktadır. Genel olarak ise, asimetrik yaklaşımlar, hesaplama hızları düşük olsa da güvenlik unsurlarının tamamını desteklemeleri açısından çok önemli yaklaşımlardır.

Sezar, MD2, MD4, MD5, RSA, Lucifer, Iraqi block cipher, KASUMI, Khafre, KHAZAD, Khufu, LOKI89/91, LOKI97, Lucifer, Red Pike, S-1, Square, TEA, SAFER, Serpent, SHARK, MAGENTA, MARS, MISTY1, MMB, Blowfish, Twofish, 3-Way, Camellia, AES, CMEA, DEAL, FEAL, GDES, CAST-128, CAST-256, DES, 3DES, DES-X, IDEA, SkipJack, GOST, El-Gamal, Schnorr, Elliptic Curve, Needham-Schroeder Protokolu ve Diffie-Hellman Anahtar Değişimi, Steganografi, PGP, S/MIME, IPSec, Kerberos, RIPEMD-160, HMAC, RC5, RC6, XTEA SHA-1, SHA-2, HAVAL, N-Hash, Snefru, Tiger ve Whirlpool gibi güvenli bir iletişimde kullanılan şifreleme tekniklerinin ve protokollerinin bazlarıdır.

Kriptoanaliz, kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir. Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içerirler. Bu yaklaşım, ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya çıkarmak için kullanılabileceği gibi, şifrelerin çözülmesi için de kullanılabilir. Bu bilim dalı, düzmetni şifrelenmiş metinden elde etme işlemi olarak bilinir ve bu işlem çoğunlukla şifreleme anahtarına sahip olmadan yapılır. Bu daldı, farklı bilgi birikimlerine, deneyimlerine, tekniklerine ve yaklaşımlara ihtiyaç duyulabilir. İşlemler sırasında, yoğun istatistik, matematik ve bilgisayar gücüne ihtiyaç duyulmaktadır. Bundan dolayı da uygulama alanı sınırsızdır. Kriptoanaliz yöntemleri, kaba kuvvet ve diferansiyel kriptoanaliz olmak üzere ikiye ayrılır. Kaba kuvvet, bir şifreleme algoritması tarafından kullanılabilecek tüm anahtarları, tek tek veya belirli bir mantık çerçevesinde deneyerek, kullanılmış olan şifreleme anahtarını bulma yaklaşımı iken, diferansiyel kriptoanaliz ise; bilinen açık şifreli mesaj çiftleri arasındaki farkların hesaplanması temeline dayanır.

Kriptoanalizde uygulanacak yöntemler, genelde eldeki bilgi ile belirlenebilir. Bu tür durumlar, kriptoanaliz senaryoları veya çoğunlukla şifreyi kırmaya yönelik ataklar olarak adlandırılmaktadır. Yani şifreyi çözmek için uygulanan her girişim birer ataktır. Çok genel hatları ile ne tür atak kullanılabileceği bellidir. Bu atakların en genelleri aşağıda listelenmiş ve aşağıda kısaca açıklanmıştır:

Salt şifreli metin (chiphertext only): Kriptoanalisten sadece bir grup şifreli metine erişiminin olduğu durumdur. Atağıın başarılı olması için şifreli metne karşılık gelen düz metnin ya da daha da iyi olarak şifrelemede kullanılan anahtarın kendisinin elde edilebilmesi gereklidir. Yeni şifreleme tekniklerinin şifreli metin ataklarına karşı yeterli seviyede bir güvenlik sağlama ilk istenen şarttır.

Bilinen düz metin (known plaintext): Kriptoanalist, bir grup düz metne ait şifreli metne sahiptir. Sıkıştırılmış dosya arşivleri bu tür ataklara çok eğilimlidirler.

Seçilen düz metin veya şifreli metin (chosen plaintext or ciphertext): Atak eden kişinin kendisinin rasgele seçtiği düz metne karşılık gelen şifreli metinleri elde edebileceği kriptoanaliz senaryosudur. İlk başta biraz gerçekçi görünmese bile modern kriptoanalizde bu tür durumlar olabilir. II. Dünya Savaşında müttefiklerin Almanlara karşı kullandığı "bahçıvanlık" (gardening) yöntemi buna örnektir. Örneğin, Almanlar tarafından mayınlanmış bir bölgeyi kasten tekrar mayınlayıp akabinde gönderilen mesajlarda mayın, mayın temizleme v.s. gibi kelimelerin olduğunu düşünmek. Bu tür düz metinlere o sıradı "yemlik" (crib) adı verilmiştir.

Uyarlanır seçili düz metin (adaptive chosen plaintext): Seçilen düz metin veya şifreli metin durumunun aynısıdır. Tek fark düz metnin (veya şifreli metin) rasgele seçilmeyip daha önceki şifre çözmelerde öğrenilen bilgiler ışığında seçilmesidir.

İlişkili anahtar atağı (related key attack): İki farklı anahtarla şifrelenmiş iki şifreli metne sahip olunan durumdur. Anahtarlar bilinmese de; şifreli metinler incelenerek bir sonuca varılabilir.

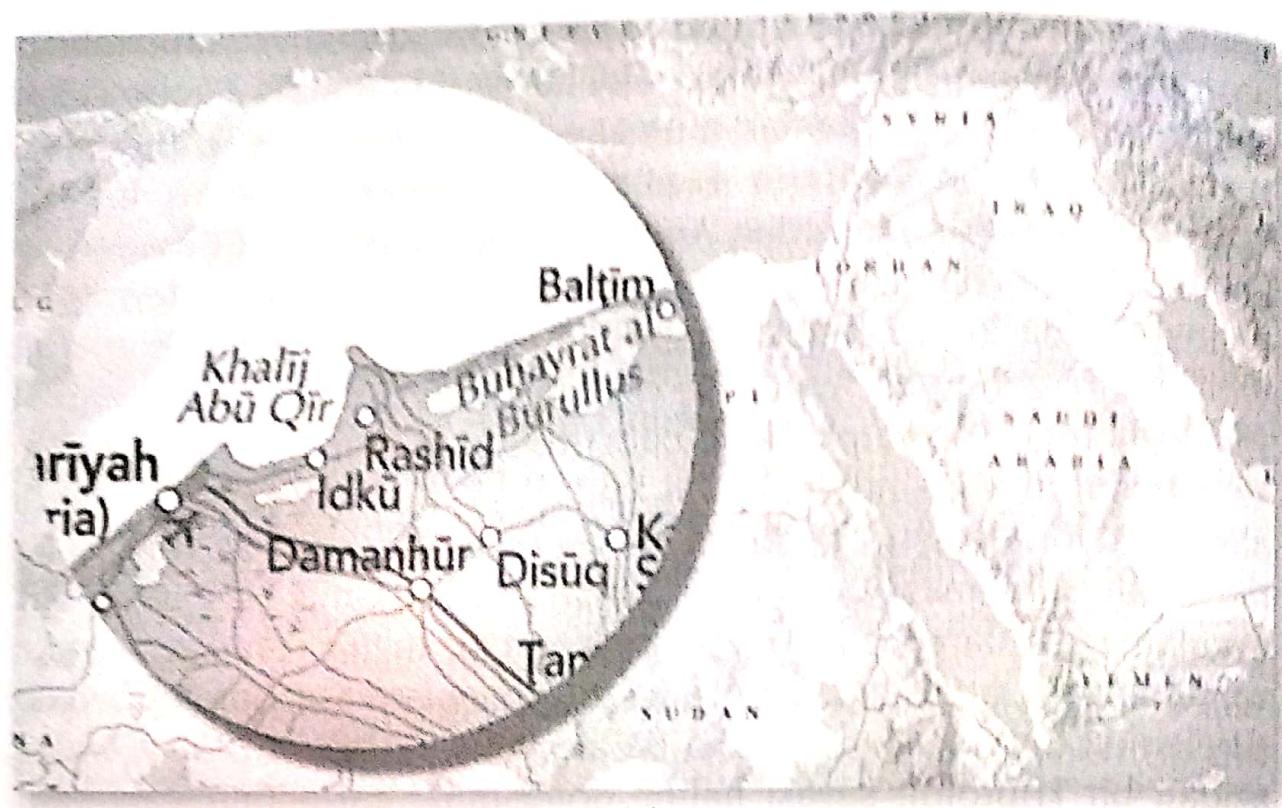
2.2 ŞİFRELEME TARİHÇESİ

Bilinen en eski kriptografi örneği günümüzden 4000 yıl öncesine kadar gitmektedir. Mısır, Hindistan, Mezopotamya, Babiller, Asurlar, Yunan, Roma, Persler, Anglosakson İngiltere ve İskandinavya gibi tarihi uygarlıklarda kriptografi ile ilgili birçok gelişme gerçekleşmiştir. Bu noktaya kadar yapılanlar sadece düz metnin anlaşılmaz biçimde

dönüştürülmesine yöneliktir. Tarihi olarak kriptografinin kullanıldığı bir başka alanda din ve benzeri alanlardır. Burada da birçok ilginç yöntem ve konuya rastlamak mümkündür. Kriptolojinin kriptoanaliz kısmı, 7. yüzyılda harflerin konumlandırılmaları ile ilgili frekans analizi yöntemlerini keşfeden Araplarla başlamaktadır. Rönesans ile beraber Avrupa'da gizli yazma ile ilgili çalışmalar artış göstermiştir. Politik alanda kriptografi kullanımı 13. yüzyılda Venedik, Roma ve Vatikan gibi yerlerden Avrupa'ya yayılmıştır. 17. yüzyılda çok alfabeli yer değiştirme (polyalphabetic substitution) sistemi geliştirilmiştir. 19. yüzyılın ilk yarısında telgrafın icadı kriptografinin bugünkü halinimasına yol açmıştır. I. Dünya Savaşı'na yaklaşlığında telefon ve radyonun bulunması ile iletişim kanalları genişlemiş ve kriptografik uygulama alanları artmıştır. Savaşta birçok İngiliz, Fransız, Alman ve Amerikalı kriptologlar çalışmalar yapmışlardır ve bu dönemde şifreleme biliminin önemi daha da artmıştır. II. Dünya Savaşı birçok açıdan bir kriptoloji savaşı haline dönüşmüştür; başta Enigma olmak üzere kriptoloji ve bilgi güvenliği ile ilgili birçok ilginç hadise meydana gelmiştir. Bu gelişmeler soğuk savaş dönemindeki gelişmelere taban oluşturmuş ve konu önemini yitirmemiştir. Bilgisayarın insan hayatının her alanına girmesi, bilgisayar ağlarının, Internet'in ve mobil iletişimimizin yoğun kullanımı konularının önemini oldukça artırılmıştır. Günümüzde bilgi güvenliğine yönelik yüzlerce şifreleme yöntemi geliştirilmiş ve hız kesmeden geliştirilmeye devam etmektedir. Gelinen aşamayı daha iyi anlamak için geçmişten günümüze şifre bilimi tarihini incelemek gereklidir. Bu çerçevede şifre bilimi tarihi sıraya göre takip eden başlıklarda gözden geçirilmiştir.

2.2.1 Rosetta Tableti

M.Ö. 1900 yıllarında şifreleme ve çözümüyle ilgili ilk örneğin Rosetta Tableti olduğu kabul edilmektedir. 1799 yılında Mısır'ın Reşit şehri yakınlarında Napolyon'un askerleri tarafından bulunan bir tablet belirgin bir şekilde üç bölüme ayrılmıştır. Üstteki bölüm hiyeroglif olarak, ortadaki bölüm halkın kullandığı Mısır dilinin bir formunda ve alttaki bölüm ise Yunanca yazılmıştır. O zamana kadar antik Mısır hiyerogliflerinin tamamıyla resimlerin ifade ettiği bir dille yazıldığı kabul edilmektedir. Örneğin hiyeroglifte geçen bir kuş resminin, bir kuşu ya da uçmak gibi kuş ile ilgili bir konuya ifade ettiği zannedilmektedir. Rosetta Tableti bu açıdan önemli bir ipucu sağlayacağından üzerinde birçok çalışma yapılmıştır. Fransız bilgin Jean-Francois Champollion, 14 yıllık bir çalışma sonucu 1822 yılında bu yazılı çözülemeyi başarmıştır. Şekil 2.6'de gösterilen tablet, 1801'de Fransızlardan İngilizlere geçmiştir. Şu anda "British Museum"da sergilenmektedir [2-5].



(a)



(b)

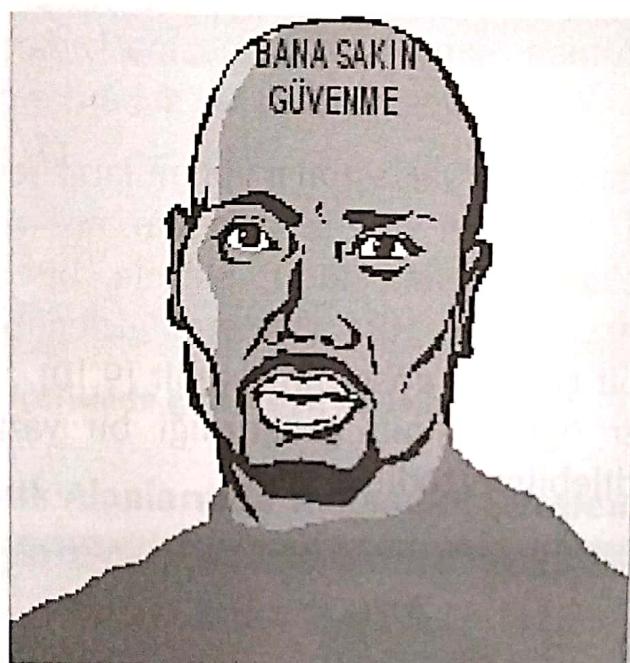
Şekil 2.6. (a) Rosetta (Raşit) yerleşim merkezi (b) Rosetta Tabletı

Bu tip antik yazıtlarda aslında gizli bir bilgi yoktur. Ama çözüleне kadar yapılan uğraşlar, hiyeroglif yazıyı şifreli metin; Yunanca yazıyı da düz metin olarak düşünürsek birer kriptoanaliz çalışması olarak ele alınabilir. Bu tabletin çözülmesi ile hiyerogliflerin çözülmesi çok kolaylaşmıştır.

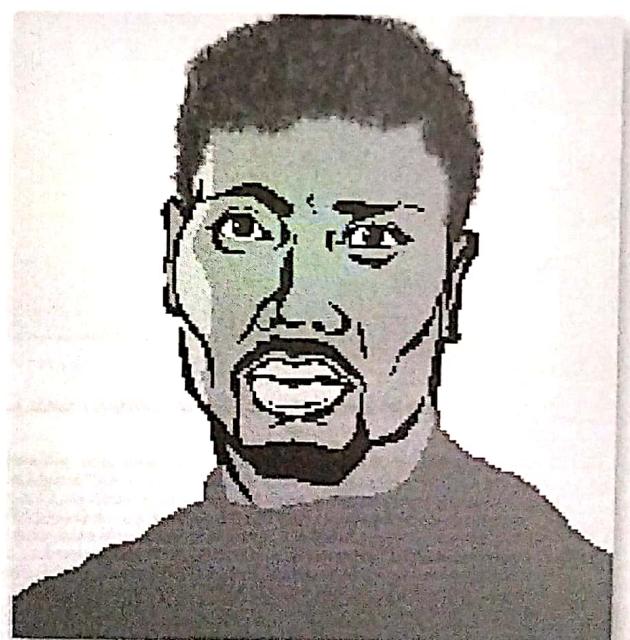
2.2.2 Steganografi

M.Ö. 1500 yıllarında başlayan bu yaklaşım, günümüzde bir bilim dalı olarak gelişmelerini sürdürmektedir. Steganografi, saklı bir mesajın, sadece alması istenen kişi veya kişilerin mesajın varlığından haberdar olduğu şekilde yazılmazı sanatı ve bilimidir. Bir mesaj veya ortam içerisinde “gizlenmesi gereken mesaj” gizlenir. Mesaj anlaşılır fakat varlığı gizlidir. Şifrelemede mesajın varlığı açıktır; anlam gizlidir [6].

Herodot, saçı tıraş edilmiş bir kölenin başına, gönderilmek istenen mesajın dövme ile yazıldığı bir hikâyeden bahsetmektedir. Şekil 2.7'de gösterilmeye çalışıldığı gibi bu yöntemin tek sakıncası, mesajı



(a) Mesajın yazıldığı an

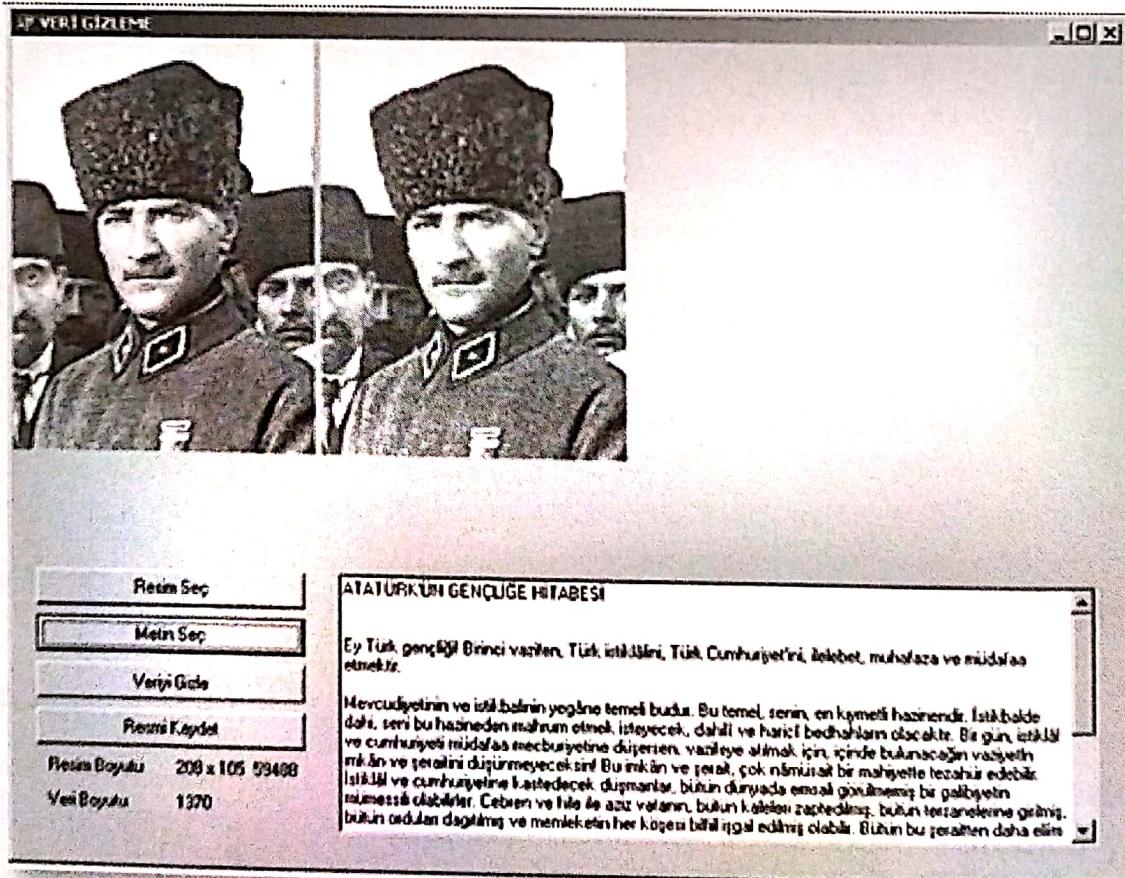


(b) Mesaj gizlenince

Şekil 2.7. Antik Steganografi

(mesajcayı) göndermeden önce saçın tekrar uzamasını beklemektir [7]. Antik Yunan'da tahtanın üzerine yazılı mesajlar balmumu ile kaplama kullanılmamış tablet ("wax tablet") olarak gizleme, avlanan hayvanların karnında mesaj gönderme ve görünmez mürekkeple gizli mesajlar yazma kullanılan yaklaşımlardan bazlılarıdır. Bu mesajları okuyabilmek için kâğıdı ısitmak veya kâğıda kimyasal bir işlem uygulamak gerekmektedir. II. Dünya Savaşında mektuplardaki satırlar arasına gizli mesajlar görünmez mürekkeple yazılmıştır. İngiliz arşivlerinde saklı sırlara göre, Almanlar II. Dünya Savaşı boyunca moda kitaplarını gizli haberleşme aracı olarak kullanmışlardır. Kitaptaki resimlerin içine mors alfabesiyle gizli mesajlar yazılarak, İngiliz yetkililerinin uyguladığı sansür delinerek, çok önemli sırlar yerlerine ulaştırılmıştır. 1942 yılında iki Alman ajanın sorgulamasına kadar İngiliz istihbarat servisi MI5, mors alfabeli mesajlardan hiç haberdar değildi [8].

Günümüzde steganografik yaklaşımlar kullanılarak resim, yazı veya ses formatındaki gizli bilgilerin yine farklı resim, ses veya yazı içerisinde gizlenmesi gerçekleştirilebilmektedir. Mesela, bir Atatürk resminin içine "Atatürk'ün Gençliğe Hitabı" metni gizlenebilmektedir. Şekil 2.8'de buna ait bir çalışma gösterilmektedir [9,10]. Yazarlardan Şeref Sağıroğlu ile bir öğrencisinin geliştirdiği bu yazılım Internet'ten kolaylıkla elde edilebilmektedir.



Şekil 2.8. "Atatürk'ün Gençliğe Hitabı"nın Atatürk'ün resminin içerisinde steganografi ile saklanması

2.2.3 Anlamsız Şifre (Null Cipher)

Antik zamanlarda kullanılan şifreleme yöntemlerinden biridir. Steganografinin en basit şekli olarak düşünülebilir. Düz metin, çok miktarda şifrelenmemiş materyal içinde saklanarak gizlenir [11]. Şekil 2.9'da buna bir örnek verilmiştir. Bu yazı içerisinde sıradan bir hava durumu haberi yer almaktadır. Fakat bu haberdeki her kelimenin baş harfleri "Newt is upset because he thinks he is President." (Newt başkan olduğunu düşündüğünden dolayı üzgün) gizli mesajını içermektedir.

News Eight Weather. Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Şekil 2.9. Bir metin içerisinde gizli mesaj saklama

2.2.4 Din ve Mistik Alanlarında Kullanılan Şifreleme Yaklaşımları

Dinle ilgili birçok alanda şifreleme yaklaşımı yoğun bir şekilde kullanıldığı görülmektedir. Birçok dini mesaj veya konu, şifreli olarak yayılmış ve kullanılmıştır. Atbash, 666 rakamı, Domuz ağılı, Kabala bu tip yaklaşılardan bazılarıdır. Bu yaklaşımların bazıları aşağıda kısaca açıklanmıştır.

Kabala, Yahudilerde, yazılı olarak konulmuş olan Tanrı kanunlarının yanında, ağızdan ağıza geçen din buyruklarının, İbranî felsefesinin ve efsane yazılarının bütünü olarak tanımlanmaktadır. Kabala'nın Yahudilerin Babil'de esaret dönemi sırasında Keldani öğretmenlerinin Yahudi geleneklerine etkileşiminden doğduğu önerilmiştir. Öğreti erken dönemlerinde tamamen sözlü aktarılmaktaydı, bundan dolayı Kabala, İbranice imla olarak QBLH kelimesi QBL "kabul etmek" anlamına geliyor.

2.2.5 Atbash Şifresi

M.Ö. 600–500 yılları arasında geliştirilmiştir. Bu şifreleme yaklaşımında İbranice'de bulunan 22 harf kullanılmaktadır. Bu harfler: Alef, Beit, Gimel, Dalet, Hei, Vav, Zayin, Chet, Tet, Yud, Kaf, Lamed, Mem, Nun, Samech, Ayin, Pei, Tzadik, Kuf, Reish, Shin ve Tav. Atbash

şifresi basit bir şifreleme teknigi gibi gözükse de yıllarca gizliliğini koruyabilmistiir. Bu 22 harfin ilki, sonuncu ile; ikincisi, sondan ikinci ile ve bu yolla devam ederek baştan on birinci harf, sondan on birinci harfi gösterecek şekilde şifrelenmektedir [12,13]. Şekil 2.10'da şifre anahtari iki şekilde gösterilmektedir. Birinci kısımda, bütün harfler tek bir sırada gösterilirken; ikinci kısımda daha pratik bir gösterim yer almaktadir. 22 harf ortadan ikiye bölünüp ikinci kısım ters sırada ikinci sıraya yazılmıştır. Bu şekilde herhangi bir harf altında veya üstünde yer alan harf ile şifrelenir veya şifresi çözülür.

1. Kısım	<table border="1"> <tr><td>A</td><td>B</td><td>G</td><td>D</td><td>H</td><td>V</td><td>Z</td><td>Ch</td><td>T</td><td>Y</td><td>K</td><td>L</td><td>M</td><td>N</td><td>S</td><td>O</td><td>P</td><td>Tz</td><td>Q</td><td>R</td><td>Sh</td><td>Th</td></tr> <tr><td>Th</td><td>Sh</td><td>R</td><td>Q</td><td>Tz</td><td>P</td><td>O</td><td>S</td><td>N</td><td>M</td><td>L</td><td>K</td><td>Y</td><td>T</td><td>Ch</td><td>Z</td><td>V</td><td>H</td><td>D</td><td>G</td><td>B</td><td>A</td></tr> </table>	A	B	G	D	H	V	Z	Ch	T	Y	K	L	M	N	S	O	P	Tz	Q	R	Sh	Th	Th	Sh	R	Q	Tz	P	O	S	N	M	L	K	Y	T	Ch	Z	V	H	D	G	B	A
A	B	G	D	H	V	Z	Ch	T	Y	K	L	M	N	S	O	P	Tz	Q	R	Sh	Th																								
Th	Sh	R	Q	Tz	P	O	S	N	M	L	K	Y	T	Ch	Z	V	H	D	G	B	A																								
2. Kısım	<table border="1"> <tr><td>A</td><td>B</td><td>G</td><td>D</td><td>H</td><td>V</td><td>Z</td><td>Ch</td><td>T</td><td>Y</td><td>K</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Th</td><td>Sh</td><td>R</td><td>Q</td><td>Tz</td><td>P</td><td>O</td><td>S</td><td>N</td><td>M</td><td>L</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>	A	B	G	D	H	V	Z	Ch	T	Y	K												Th	Sh	R	Q	Tz	P	O	S	N	M	L											
A	B	G	D	H	V	Z	Ch	T	Y	K																																			
Th	Sh	R	Q	Tz	P	O	S	N	M	L																																			

Şekil 2.10. Atbash Şifresi Anahtar Tablosu

İncil'de sıkılıkla geçen Shechach kelimesinin Atbash ile çözülmesine bir örnek aşağıda verilmiştir.

"Ve kuzeyin uzak ve yakın, biri biri ile beraber, bütün kralları ve yeryüzünün üzerinde olan bütün krallıkları ve Sheshach kralı bunlardan sonra içmelidir." (Kutsal Yazilar: Jeremiah 25:26).

"Sheshach" (SheSheK) bir kod sözcüktür ve bilinmeyen bir ülke veya yerdir. Atbash kullanılarak şifre çözülür, Sh-Sh-k (İbranice'de sesli harf yoktur) bu yerin B-b-l (Babil) olduğu düşünülmektedir [13].

İncil'de sıkılıkla yer alan ve neyi temsil edildiği bilinmeyen bir kelimeye Atbash şifre çözümü uygulandığında bu kelimenin Babil'i ifade ettiği bulunabilmektedir. Bu şekilde Yahudi inancında kutsal yazıtlarda Atbash şifresi ile Magog olarak adlandırılan ve Nuh'un oğlu (Türk'ün babası) Yasef'in, coğrafi alan olarak Türkiye'yi, kuzey İran'ın bir kısmını, Gürcistan, Ermenistan ve Azerbaycan'ı gösterdiği yerden bahsettiğine inanılmaktadır.

2.2.6 Tevrat'ın Şifresi (The Bible Code)

Tevrat'ın Şifresi adlı kitapta belirtilen, "Tevrat'ta üç bin yıldır saklı olan şifre, Eliyahu Rips adlı İsraili bir matematikçi tarafından çözülmüştür. Rips, kanıtlarını önde gelen bir bilim dergisinde yayımlanmış ve dünyanın en ünlü matematikçileri bunu onaylamıştır.

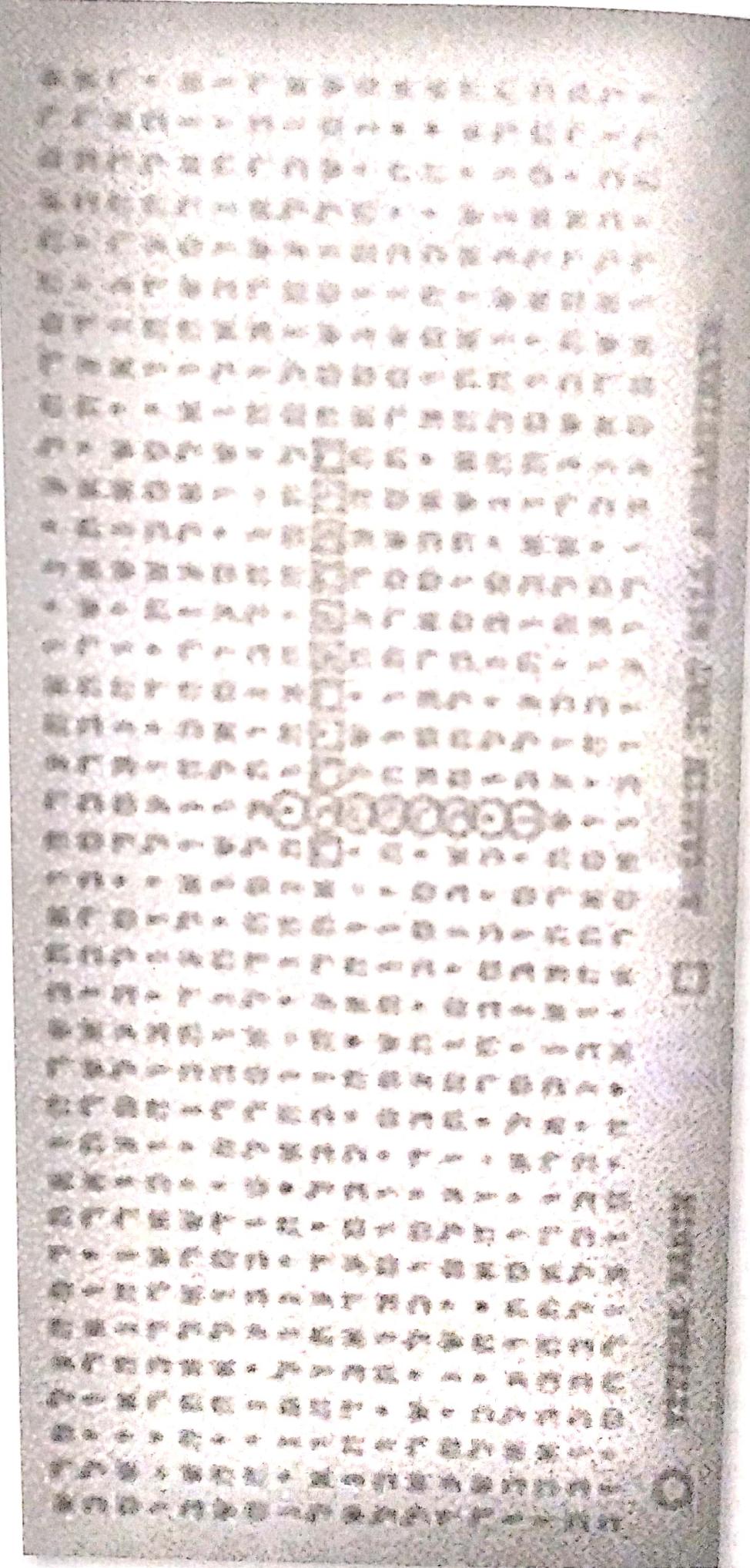


Şekil 2.11. Oslo Anlaşması, 13 Eylül 1993 (İzak Rabin (1922–1995), William Jefferson Clinton (1946) ve Yaser Arafat (1929–2004))

İzak Rabin'in öldürüleceğine dair kehaneti içeren şifreyi ("assassin that will assassinate") bilgisayarda bizzat bulup, Rabin'i uyaran bu kitabı yazan Michael Drosnin, belirttiği tarih ve şekilde suikastın gerçekleştiğini belirtmekte fayda vardır. Bunun üzerine; beş yıllık bir araştırma sürecinde Harvard, Yale ve İbrani üniversitelerinden en üst düzey matematikçilerle görüşmüştür ve bunların tümü Tevrat'ta geleceği haber veren bir şifre olduğunu doğrulamıştır. Kennedy ve Rabin suikastlarından Oklahoma'da Federal Hükümet binasının bombalanmasına, Clinton'ın başkanlığından Netanyahu'nun başbakanlığına, II. Dünya Savaşı'ndan Körfez Savaşı'na, Ay'a ayak basımasından Jüpiter'in bir kuyruklu yıldızla çarşışmasına kadar bütün önemli olaylar, ayrıntılarıyla birlikte tam üç bin yıl önce Tevrat'ta şifrelenmiştir. Tevrat'ın şifresi, gerçek Kiyamet'in nükleer bir dünya savaşı olabileceği konusunda da uyarıcı bulunuyor" açıklama din alanında kullanılan şifrelemenin gelebileceği boyutları göstermektedir.

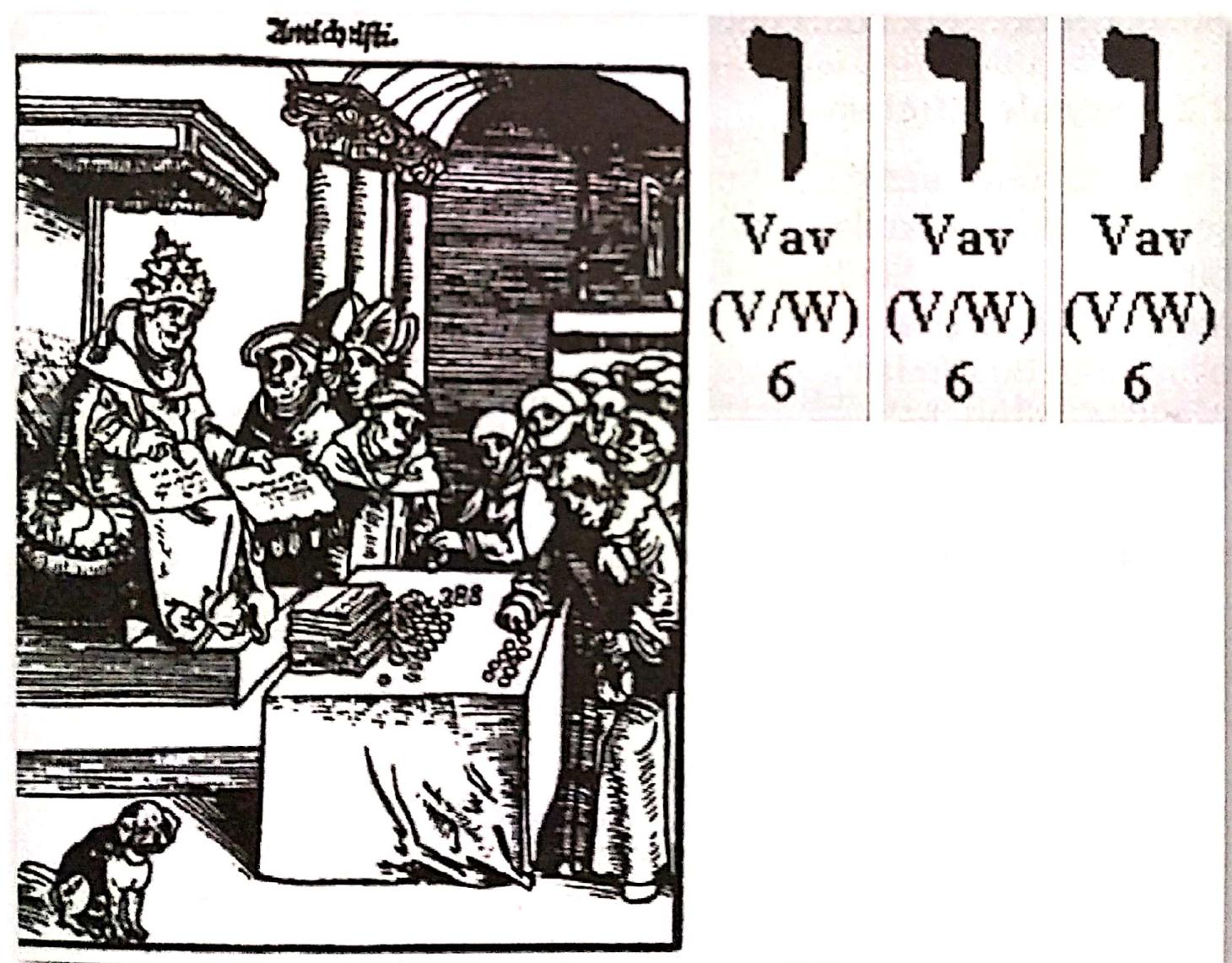
2.2.7 The Number of the Beast (666)

Kriptografi, baskın kültüre veya siyasi yetkililere karşı gelmek için kullanılan dini yazılardaki eski bir gelenektir. Belki de bunların en eski ve ünlülerinden biri Hıristiyan Yeni Ahit kitabında (Vahiyler kitabında) geçen Şeytan'ın Sayısıdır. 666 rakamı tehlikeli bir referansı gizlemenin kriptografik yolu olabilir. Şekil 2.13'de gösterildiği gibi bu rakamın değişik manalar içерdiği söylense de; birçok araştırmacı bunun Roma İmparatorluğunun veya daha muhtemel olarak İmparator Nero'nu ima eden bir kod olduğunu söylemektedir [14, 15].



Şekil 2.12. İsrail Başbakanı İzak Rabin'e yapılan suikastın şifresi "assassin that will assassinate"

“İblisin işaretti” olarak da adlandırılan 666 rakamı antichrist (“sahte Mesih”) olarak İncil’de geçtiği de düşünülmektedir: “İşte hikmet. Ona, “beast” sayısını anlamasına fırsat ver: o bir adamın sayısıdır ve adamın sayısı 666’dır.” (Revelation (Vahiy) 13:18) Antichrist, Hıristiyan dininin dünyanın sonu ile ilgili kehanetlerinden biridir. Bu sayıya İslam dininde Deccal’ın karşılığı da denilebilir.



Şekil 2.13. Antichrist ve 666'nın İbranice WWW (World Wide Web) göstermesi
[16]

2.2.8 Domuz Ağılı Şifresi (Pigpen Cipher)

Bu şifreleme yaklaşımı 18.Y.Y.'da hür masonlar tarafından kayıtların gizli tutulması için kullanılmıştır. Şifre, bir harf yerine başka bir harf yerleştirmek yerine her harf için bir simge kullanmaktadır. Alfabe domuz ağılı şeklinde tasvir edilen bir ızgaralara Şekil 2.14'de gösterildiği gibi yerleştirilerek; o harfe bitişik ızgara öğelerinin oluşturduğu şekil simge olarak kullanılmaktadır.

Bu şifrelemede örnek olarak $A=J$ $R=U$ $Y=\diamond$ $Z=\wedge$ harflerine tablodan dönüşüm yapılmaktadır. Aşağıda MERHABA kelimesine karşılık gelen karakterler ise  karakterleriyle ifade edilmektedir.

A	B	C
D	E	F
G	H	I

J.	K.	L.
M.	N.	O
P.	Q.	R

S
T
U
V

W
X.
Y
ż

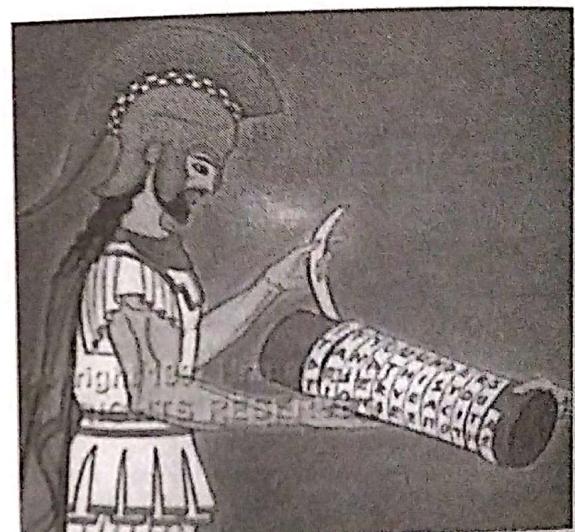
Şekil 2.14. Domuz Ağılı Şifresi

2.2.9 Scytale Şifreleme

Bir başka ünlü antik şifreleme tekniği, M.Ö. 475'de Yunan Sparta şehrinde ilk olarak kullanılan Scytale şifresidir. Düz metin, silindire sarılı bir şeride yazılır. Şerit silindirden çıkarıldığında mesaj anlaşılamaz. Mesajı alan taraf ancak aynı çapta bir silindire şeridi sararak mesajı okuyabilir. Bu şifreleme yöntemi antik Yunan'da Spartalılar tarafından özellikle askeri haberleşmede kullanılmıştır [17]. Şekil 2.15'de bu şifrelemenin bir örneği görülebilir.



(a) Yunanistan – Sparta



(b) Şifrenin çözülmesi

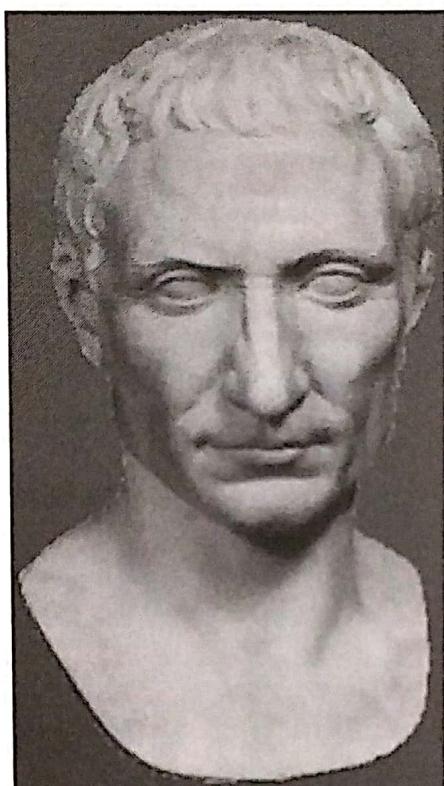
YMSRAAAEAIRLRLYUDD İDAZIINIMM											
=====											
		Y	A	R	D	I					
		M	E	D	İ	N					
		S	A	L	D	I					
		R	I	Y	A	M					
		A	R	U	Z	K					
		A	L	D	I	M					
=====											
YARDIM EDİN SALDIRIYA MARUZ KALDIM											

(c) Şeride yazılan şifre ve çözümü

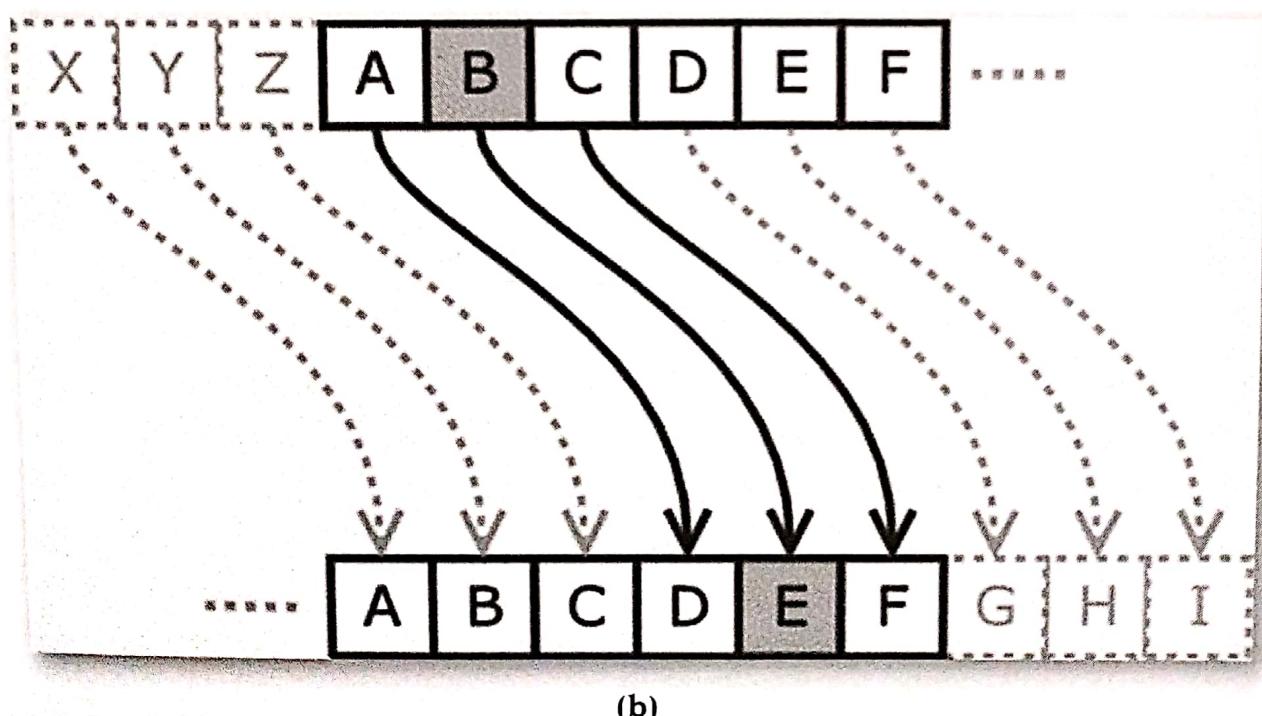
Şekil 2.15. Örnek bir scytale şifresi ve çözümü

2.2.10 Sezar Şifresi

M.Ö. 100-50 yılları arasında Julius Sezar, generallerine göndermek istediği mesajı, gönderdiği ulağa güvenmediğinden mesajın içindeki her harfi, o harfin üç harf sonrası ile değiştiriyordu. Bu kullanım günümüzde birçok şifreleme yönteminin geliştirilmesine ilham kaynağı olmuştur. Bu yöntem günümüzde modüler aritmetik tabanlı şifreleme ve şifre çözme ile gerçekleştirilmektedir [18]. Şekil 2.16'da harflerin nasıl şifrelendiğinin görsel bir anlatımı görülebilir.



(a)



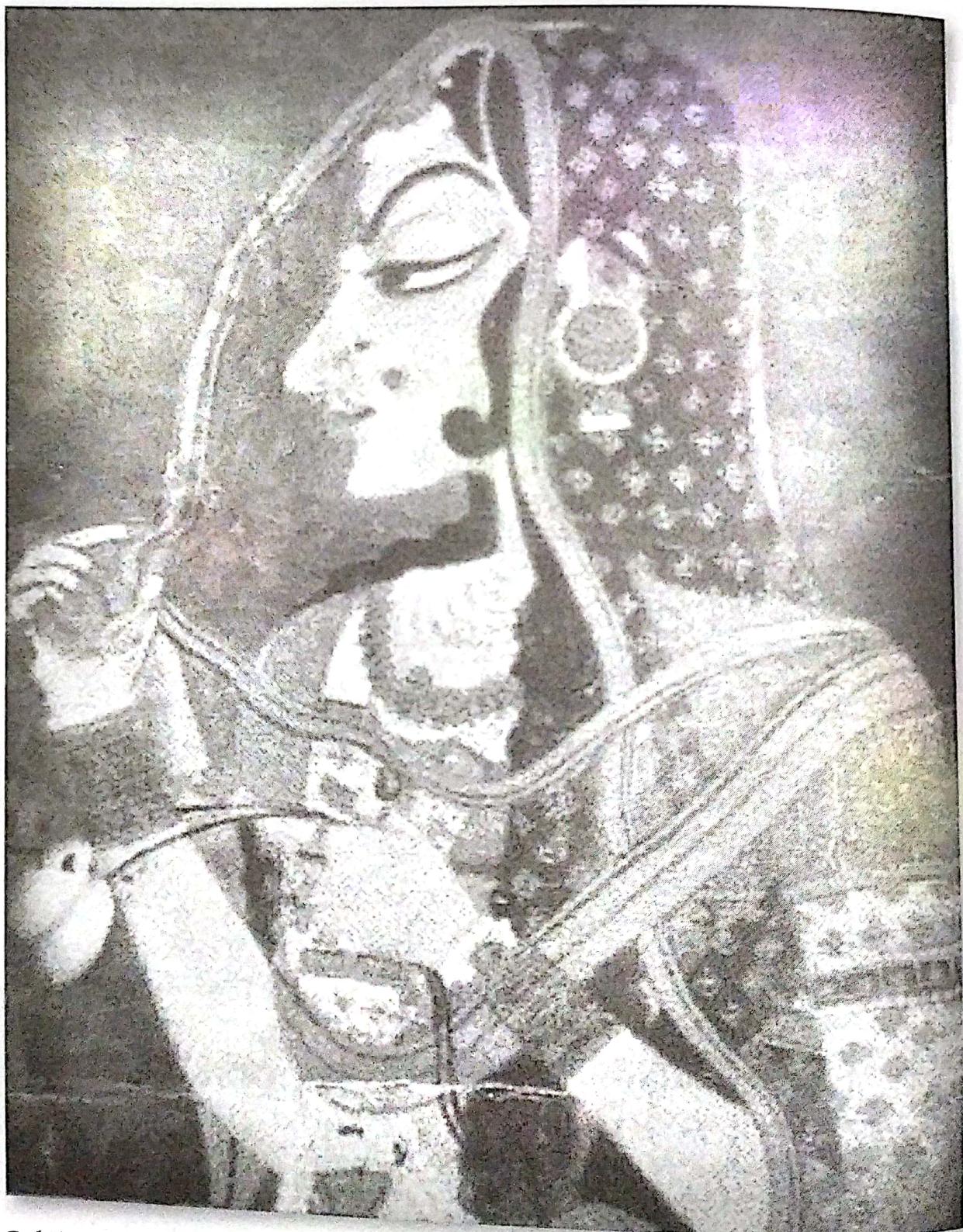
(b)

Şekil 2.16. (a) Julius Sezar (M.Ö. 100 – M.Ö. 44) (b) Sezar Şifresi'nin işlevisi

CamScanner ile tarandı

2.2.11 Kama Sutra

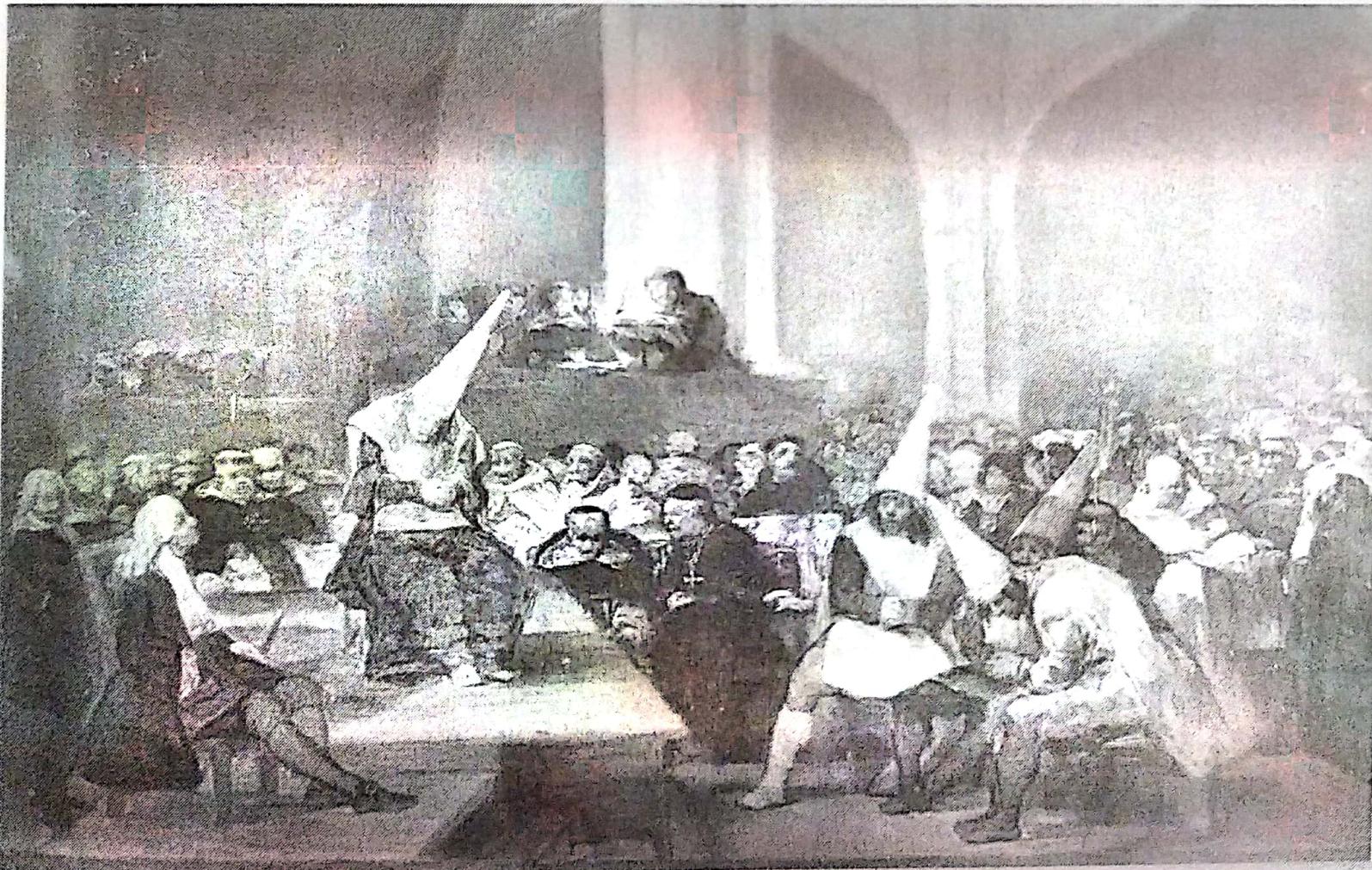
M.S. 0–100 yılları arasında şifreleme konusunda ilginç başka bir örnek Hindistan'da karşımıza çıkmaktadır. Sevgililerin dikkat çekmeden iletişim kurabilmeleri için geliştirilen şifreli teknikte; yazıların şifrelenmesi ve kelimelerin garip şekilde yazılması sanatı, kelimelerin şekillerini değiştirerek konuşma sanatı, kelimelerin başlangıç ve bitişini değiştirerek konuşma, bir kelimenin her hecesine gereksiz harfler koymak (kuşdili, "segenigi segevigliyogorugum") v.s. gibi teknikler bulunmaktadır [7].



Şekil 2.17. Kama Sutra figürü

2.2.12 Avrupa'da Criptografinin Karanlık Çağı

M.S. 500-1400 yılları arasındaki dönemde Avrupa'da yaşanan gerileme sonucu, criptografi hakkındaki pek çok bilgi kara büyüğünü nitelendirildiğinden kaybolmuştur. Bu sırada bazı Müslüman ülkeler criptoloji bilgilerini geliştirmiştir [19].

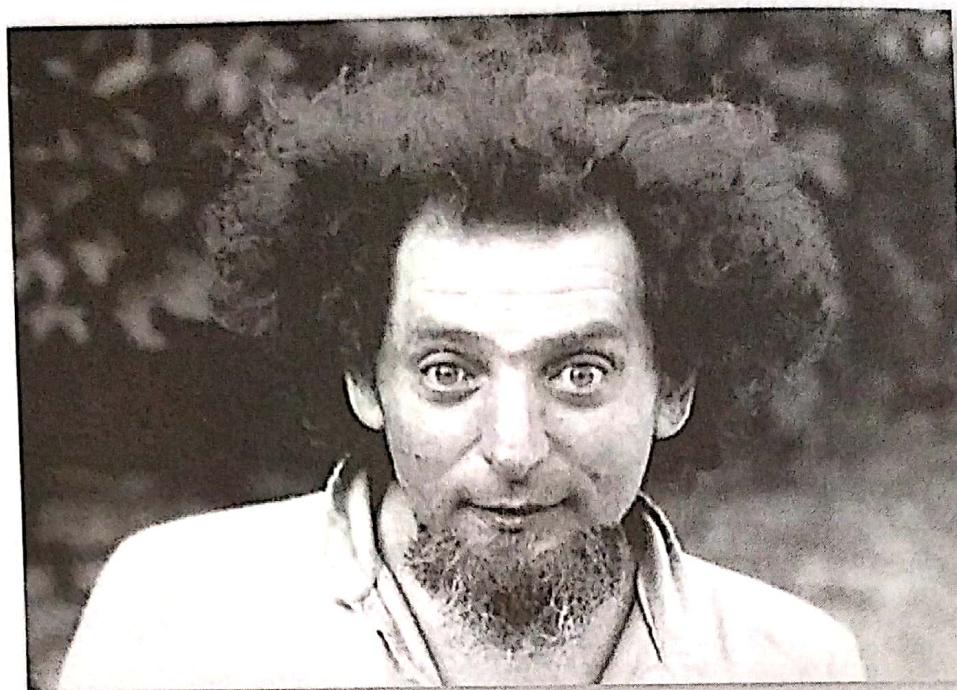


Şekil 2.18. Avrupa'da karanlık çağ

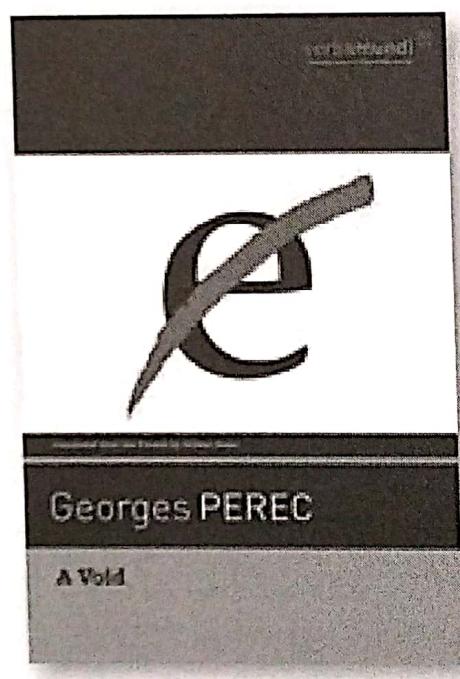
2.2.13 El-Kindi - Frekans Analizi ile Criptoanaliz

M.S. 850'de, harflerin başka harflerle değiştirilmesi prensibine dayanan Sezar şifresi gibi şifreleri (substitution cipher) çözmenin en çok bilinen yolu kullanılan dildeki harflerin frekanslarına göre deneme yapmaktır. Örneğin İngilizce'de "e" , "t" ve "a" harfleri en sık kullanılan harflerdir. Gizli metinde en çok geçen harfi bu harf sayarak sonuca ulaşmak mümkün olabilir. Bu arada bu yaklaşımın her zaman doğru sonuç üretmeyeceğini de belirtmek isteriz. Örneğin , Gadsby adında içinde "e" harfinin geçmediği 50.000 kelimelik, 267 sayfaya sıghan bir roman yazmıştır. İçinde belirli bir harfin hiç geçmediği bu tür yazılar lipogram olarak adlandırılmaktadır [20]. Böyle bir lipogram ünlü Fransız yazar Georgec Perec'in hiç 'e' harfi kullanmadan yazdığı 'La Disparition - Kayboluş' adlı romanıdır ve bu roman yine hiç 'e' harfi kullanmadan Cemal Yardımcı (1961) tarafından Türkçe'ye çevrilmiştir. Yardımcı, çeviri sürecini "Fransızca'da e harfi kullanmamaya karar verdiğinizde kelime hazineniz yüzde 30-40 oranında daralıyor. Türkçe'de ise bu oran

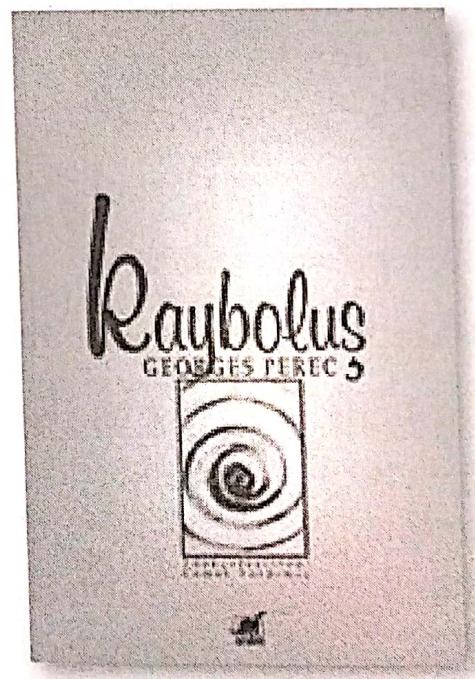
dörte bire iniyor. 'Sen, ben ve -ken' gibi kelime ve ekleri kullanamamak insanı bir hayli zorluyor." şeklinde ifade etmektedir [21].



(a)



(b)



(c)

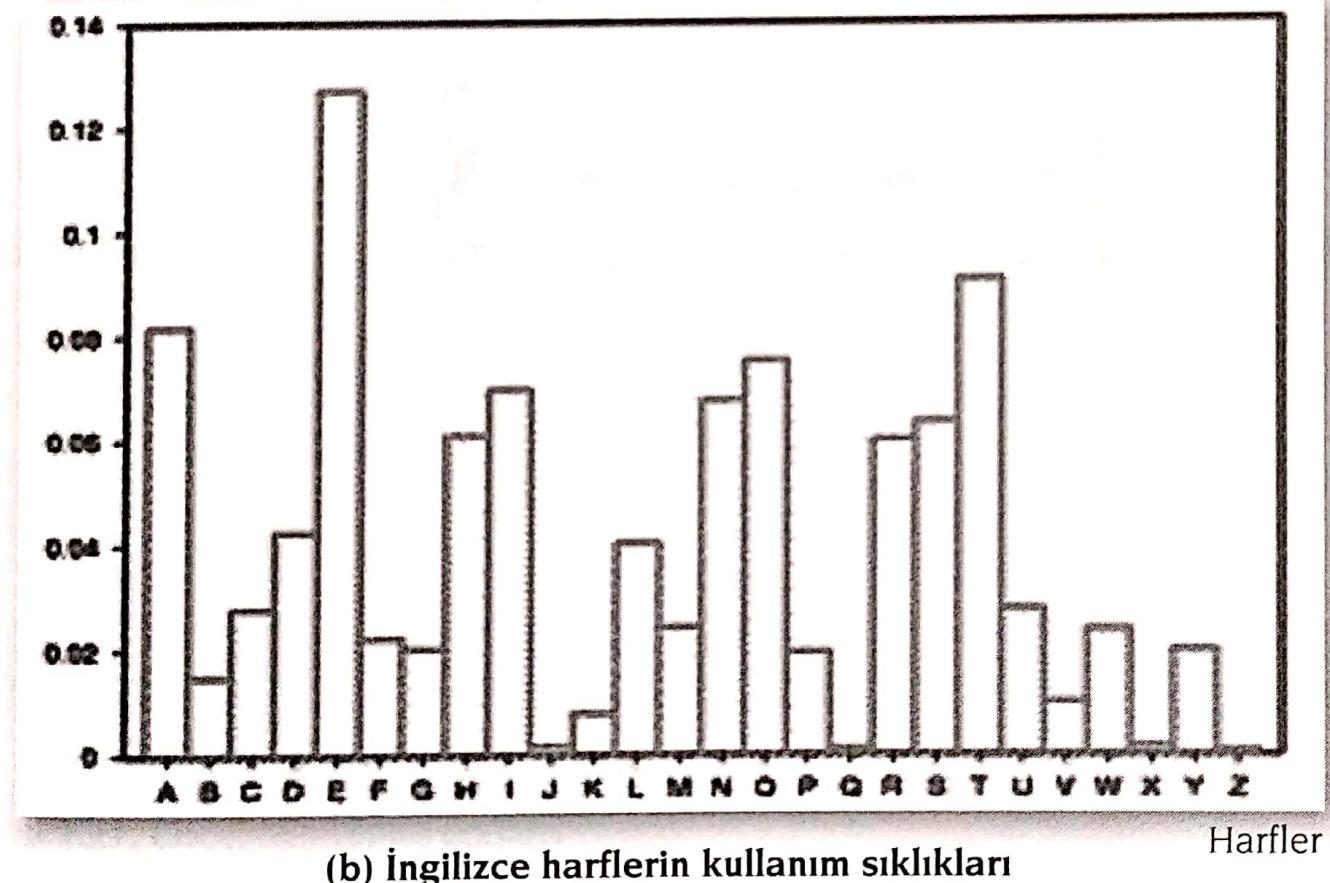
Şekil 2.19. (a) Georges Perec (1936–1982) (b) (c) hiç 'e' harfi kullanmadığı romanı

Frekans analizi yöntemini ilk kez uygulayan kişi "Arapların Filozofu" olarak da bilinen Ebu Yusuf El-Kindi'dir. İstanbul'da Süleymaniye Osmanlı Arşivinde araştırma yapan Prof. Myrayati, El-Kindi'ye ait "Kriptografik Mesajların Şifresinin Çözülmesi Üzerine Bir El Yazması" isminde bir belge bulmuştur. Bu belgede konu ile ilgili çalışma anlatılmıştır. Kur'an'ı Kerim'in metin analizi, frekans analizinin ortaya çıkışmasını sağlamıştır [22-25].



(a) Ebu Yusuf El-Kindi (805–873) [26]

Bağıl Frekans



(b) İngilizce harflerin kullanım sıklıkları

Şekil 2.20. Frekans analizini bulan El-Kindi ve bu analize bir örnek

Güzel Türkçemizde ise en fazla kullanılan ilk 12 harfin sıklıkları ise "e" %12, "a" %11.4, "i" %9, "r" %7.4, "l" %6.9, "n" %6.8, "k" %5.3, "ı" %4.4, "m" %4, "t" %3.9, "s" %3.6 ve "d" %3 olarak belirlenmiştir. Diğer harfler ise bunları izlemektedir.

2.2.14 Ebcet Hesabı

Ebcet hesabı Çizelge 2.1'de görüldüğü gibi Arapça harflere verilen değerlerle kelimelerin şifrelenmesi veya tanımlanmasıdır.

Çizelge 2.1. Ebcet Tablosu

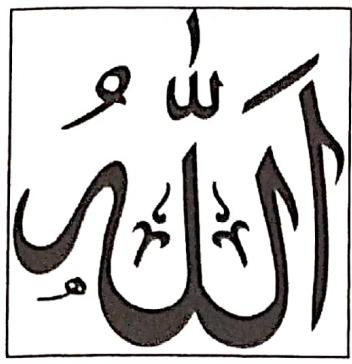
Arap alfabetesinin sıra ve sayısal değerleri

Sıra değeri	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Arapça harfler	ا	ب	ج	د	ه	و	ز	ط	ي	ك	ل	م	ن	ـ
Türkçe okunuşu	elf	be	cim	dal	he	var	ze	ha	vi	ye	kef	lam	mim	nun
Sayısal Değer	1	2	3	4	5	6	7	8	9	10	20	30	40	50

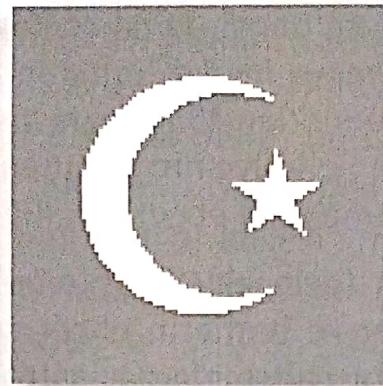
Sıra değeri	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Arapça harfler	س	ق	ص	ف	ع	ر	ت	ش	ر	ق	ص	ف	ع	ـ
Türkçe okunuşu	sin	ayn	fe	sad	kaf	re	şin	lo	se	hi	zel	dad	zi	şayn
Sayısal Değer	60	70	80	90	100	200	300	400	500	600	700	800	900	1000

Bu hesap özellikle Osmanlı zamanında, isimler arasında ilişki kurmak, tarih düşme, mimari gibi bilimsel alanlarda kullanılmıştır [27-31].

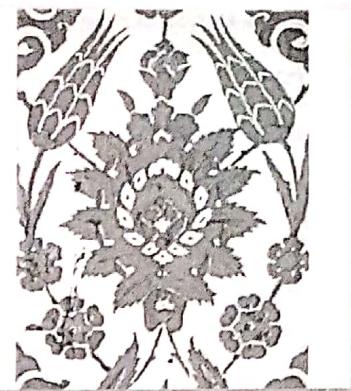
İsimler arasında ilişki kurmada; Allah, Hilâl ve Lale kelimelerinin ebcet hesabına göre karşılığı 66'dır. Bundan dolayı Osmanlı zamanında hilâl ve laleye daha özel bir ilgi gösterilmiştir. Tarih düşme; önemli olayların tarihini, rakam olarak belirtmek veya akılda tutmak yerine bir dizi kelimenin ebcet hesabına göre karşılığı bu tarih olacak şekilde yazılmasıdır. Şair Fuzuli, Kanûnî Sultan Süleyman'ın Bağdat'ı fetih tarihi olan 941 hicri yılı için "Geldi burç-i evliyaya padişah-ı namdar"



(a) Arapça Allah yazısı



(b) Hilâl



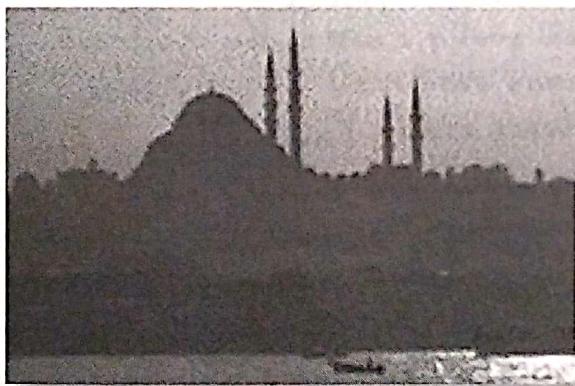
(c) Lale



(d) Türkiye ayırmacı



(e) Abdülmecid (1823–1961)



(f) Süleymaniye – İstanbul



(g) Selimiye - Edirne

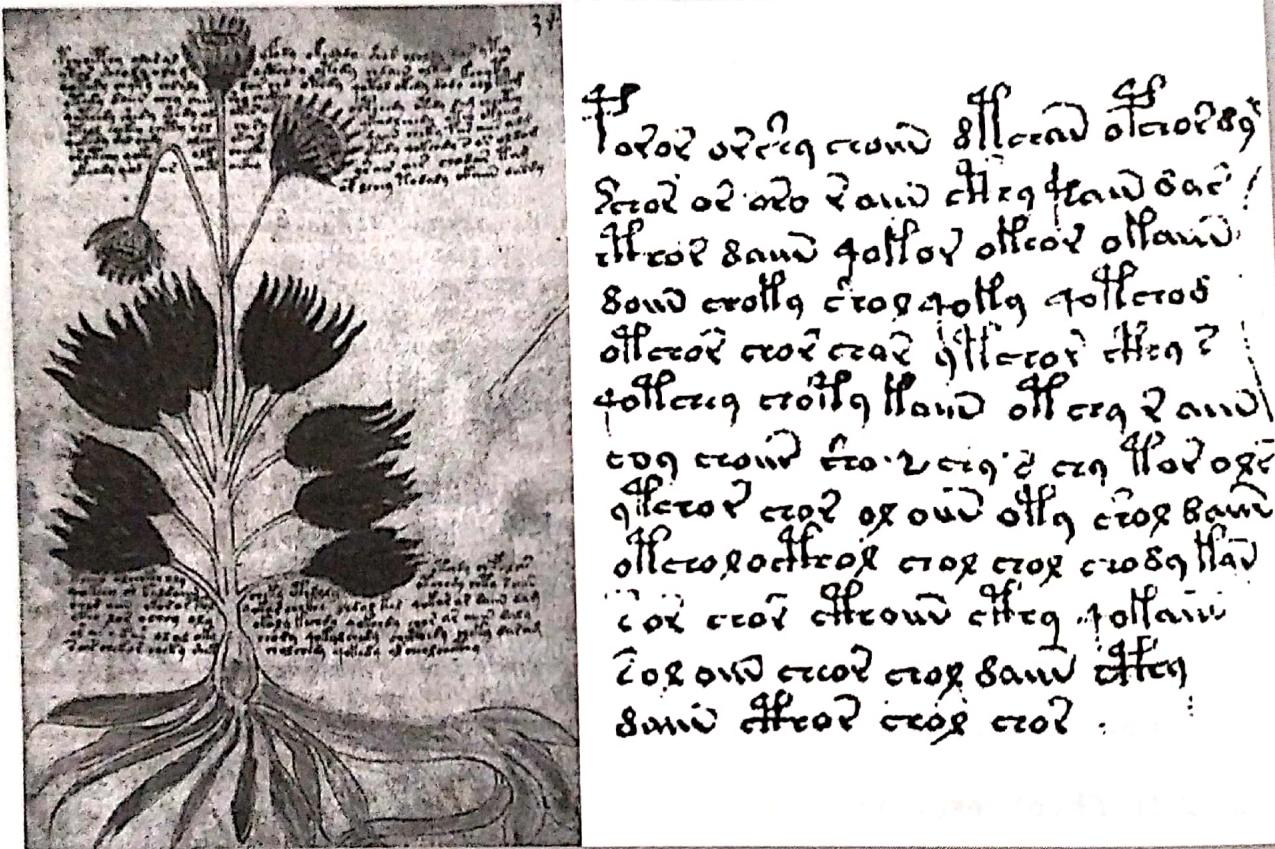
Şekil 2.21. Ebcet hesabının etkileri

mîrsasını tarih düşmüştür. Yine Sultan Abdülmecit'in sultanata geçişinde "Bir iki iki delik (1255 hicri) Abdülmecid oldu Melik" mîrsası ile tarih düşmüşlerdir. Aynı şekilde doğum tarihi yeni doğan bir çocuğa verilecek ismin seçilmesinde bir yöntem olarak kullanılmıştır. Mesela, Hicri 1311'de doğan çocuğa "Ömer Rıza" adı verilebilir. Mimari gibi bilimsel alanlarda; özellikle Mimar Sinan, eserlerinde kullandığı boyutların düzenlenmesinde ebcet hesabını kullanmıştır. Temel İslam kavramlarının ebcet hesabı karşılığının, mimari boyutları seçerken kullanılması ile ilgili bir kaç örnek verirsek: Süleymaniye'de zeminden kubbe üzengi seviyesi 45, kubbe alemi 66 arşın yüksekliktedir. Ebcet'e

göre "Âdem" 45, "Allah" kelimesi de 66 etmektedir. Yine Selimiye'de kubbeyi taşıyan sekiz ayağın merkezlerinden geçen dairenin çapı 45 arşındır. Kubbe kenarı zeminden 45, minare alemi buradan itibaren 66 arşındır. Süleymaniye ve Selimiye'nin görünen siluetleri 92 arşındır ki, bu da "Muhammed" kelimesinin ebcet karşılığıdır.

Ebcet hesabı ayrıca cifr (gelecekte muhtemel olacak işlerden haber verme, sembolik şekiller ve harflerin ebcet sayı karşılıkları üzerinde yorum yapma), vefk gibi çalışmalarda, astrolojide, define aramada da kullanılmıştır. Ömer Çelakıl'ın Kur'an'da Gizlenen Tarihler isimli kitabının günümüzde çok tartışılmışının sebebi Kur'an'ı Kerim'de gelecekte olan birçok olayın şifreli olarak belirtildiğinin örneklerle açıklanmasıdır.

2.2.15 Voynich Yazmaları



Şekil 2.22. Voynich yazmaları kitabından örnek sayfa ve yazı metni

Bir başka ilginç ve çözülemeyen şifreleme yaklaşımı olan Voynich yazmalarının, belirlenemeyen bir alfabe ve anlaşılmaz bir dilde, anonim bir yazar tarafından 1450'li yıllarda yazıldığı tahmin edilmektedir. Bu yazmalar, bilinmeyen içerikte, şekilli, gizemli bir kitaptır. 240 sayfadan oluşan bu kitap Yale Üniversitesi kitaplığında bulunmaktadır [32,33]. Bu kitap Amerikan kitap satıcısı Wilfrid M. Voynich tarafından 1912'de elde edildiğinden bu adı almıştır. Beş bölümden oluşan kitapta Şekil 8'de bir örneği görülen botanik bölümünde dünyada hiç bulunmayan

bitkilerin resmi bulunmaktadır. Kitabın varlığının bilinmesiyle birçok amatör ve profesyonel kriptograflar (II. Dünya Savaşının en üst Amerikan ve İngiliz kod çözücüleri de dahil) bu konuda yoğun çalışmalar yapmışlar fakat tek bir kelimenin bile şifresini çözememişlerdir. Bu yüzden tarihi kriptolojinin “kutsal kâsesi” (holy grail) olarak görülmekteyse de azımsanamayacak ağırlıkta bir görüş ise bu yazımı rasgele sırada simgelerden oluşmuş ayrıntılı bir “muziplikten” başka bir şey olmadığını ileri sürmektedir. Bu konuda ileri sürülen teoriler: Harf tabanlı şifre, kod kitabı şifresi, steganografi, (her sözcüğün ikinci harfi, her satırdaki harf sayısı), egzotik doğal dil, çok dilli bir lisan, yapay dil, şaka olarak ifade edilmektedir.

2.2.16 Çok Alfabeli Şifreleme (Polyalphabetic Cipher)

1467 yılında Leon Battista Alberti tarafından bulunan çok alfabeli şifreleme, birden fazla alfabe kullanılarak yer değiştirme (substitution) yöntemine dayanmaktadır. Bu tip şifrelemenin en bilinen türü daha sonra hatalı olarak Blaise de Vigenere'ye atfedilen ve bu isim ile anılan Vigenere şifresidir. Vigenere şifresi 1553 yılında Giovan Batista Belaso tarafından bulunmuştur. Şifre bir anahtar sözcüğe göre farklı dizilerde Sezar şifresini kullanmaktadır. Anlaşılması ve gerçekleştirilmesi oldukça kolay olduğundan özellikle şifreleme ile ilgili eğitimlerde sıkılıkla yer almaktadır.

Örneğin düz bir metin: SALDIRI ŞAFAKTA; anahtar sözcük LİMON olarak alınırsa Çizelge 2.2'deki tablodan yararlanılarak şifreli metin aşağıdaki gibi elde edilir:

Düz metin:	S A L D I R I	Ş A F A K T A
Anahtar:	L İ M O N L İ	M O N L İ M O
Şifreli metin:	F İ A S V E S	Ğ O Ş L U H O

2.2.17 Amerikan Criptografi

1917'de criptoanaliz terimini ortaya atan Amerikan criptoanalizinin babası William Frederic Friedman, Amerikan hükümeti için criptoanaliz çalışmalarını başlatmıştır. Bu sırada Amerika'nın I. Dünya Savaşına katılması ile ele geçen bütün kodlar Friedman tarafından 1930'a kadar her defasında başarı ile çözülebilmiştir [19,34].

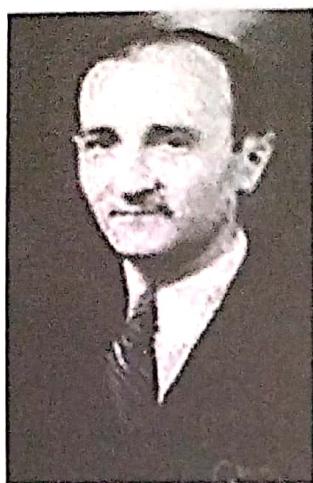
Girdi / Anahtar	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z							
A	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z							
B	B	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z							
C	C	C	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A								
Ç	Ç	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A								
D	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C								
E	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	D								
F	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	D	E								
G	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	D	E	F								
H	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	G							
I	I	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	G	H							
J	I	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	G	H	I						
K	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	G	H	I	I	J						
L	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K							
M	M	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K							
N	N	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L							
O	O	O	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M						
Ö	Ö	Ö	Ö	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N					
P	P	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö						
R	R	R	R	S	S	S	S	T	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	P		
S	S	S	S	S	S	S	S	S	T	Ş	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	P	
Ş	Ş	Ş	Ş	Ş	Ş	Ş	Ş	Ş	Ş	T	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P		
T	T	T	T	T	T	T	T	T	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	Ş		
U	U	U	U	U	U	U	U	U	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	Ş			
Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	Ş			
Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	Ü	V	Y	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	Ş		
V	V	V	V	V	V	V	V	V	V	Y	Z	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	R	S		
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Z	Z	A	B	C	C	D	E	F	G	Ğ	H	I	I	J	K	L	M	N	O	Ö	P	R	S	
Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

Çizelge 2.2. Vigenere karesi uyarlaması (“tabula recta”)

1917'de AT&T için çalışan Gilbert S. Vernam, tek kullanımlık bir şifre olan ve “one-time pad” adında tamamıyla rastsal ve asla tekrar etmeyen bir anahtarı kullanan pratik çok alfabeli bir şifre makinesi icat etmiştir. Güvenilir olduğu ispat edilebilen bu teknik, çözülemeyen tek şifreleme tekniğidir [34,35]. Bu makine, Amerikan hükümetine I. Dünya Savaşı'nda kullanılması için önerildiyse de bunun reddedilmesi ilginçtir. 1920'de makine, ticari olarak pazarlanmaya başlanmıştır.

2.2.18 Enigma'nın Esrarı

Kriptografi tarihinin belki de en önemli konusu Enigma makinesidir. Enigma, hem şifreleme hem de şifre çözme için kullanılan elektromekanik bir şifre makinesidir. Arthur Scherbius tarafından 1919'da geliştि-



(a) William Frederic Friedman
(1891–1969)



(b) Gilbert S. Vernam
(1890–1960)

Şekil 2.23. Amerikan kriptografisinin öncüleri

rılmıştır. Alman Silahlı Kuvvetleri tarafından kullanılmıştır. Kullanımı kolay olması ve “kırılamayacağının düşünülmesi” yaygın kullanımını sağlamıştır. Fakat şifre kırılmıştır ve kimi tarihçilere göre bu, II. Dünya Savaşının bir yıl erken bitmesini sağlamıştır [36-38].

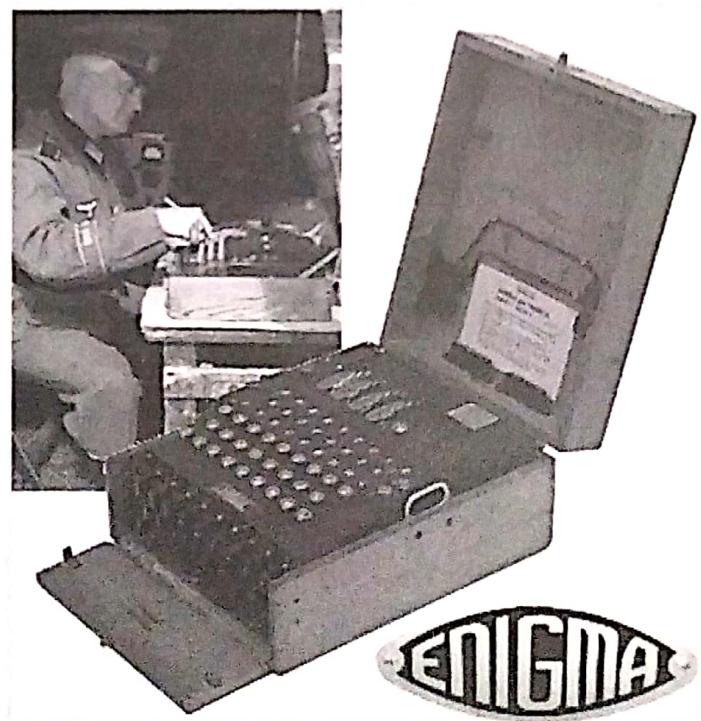
İlk olarak Polonyalılar diplomatik bir bavulda korunmamış bir Enigma makinesini ele geçirmişlerdir ve bunu İngilizler ile paylaşmışlardır. Ayrıca Almanların şifresini çözmek için kod ve şifreleme okulu açmışlardır. İngiliz matematikçiler, kriptograflar, satranç, briçoyuncuları ve bulmaca fanatikleri ve Alan Turing (Şekil 2.25) beraber çalışarak bu şifreleme yaklaşımını anlamaya ve kırmaya çalışmışlardır.

Enigma şifresinin çözülmesinde ilk başlarda iki veri bulunmaktadır:

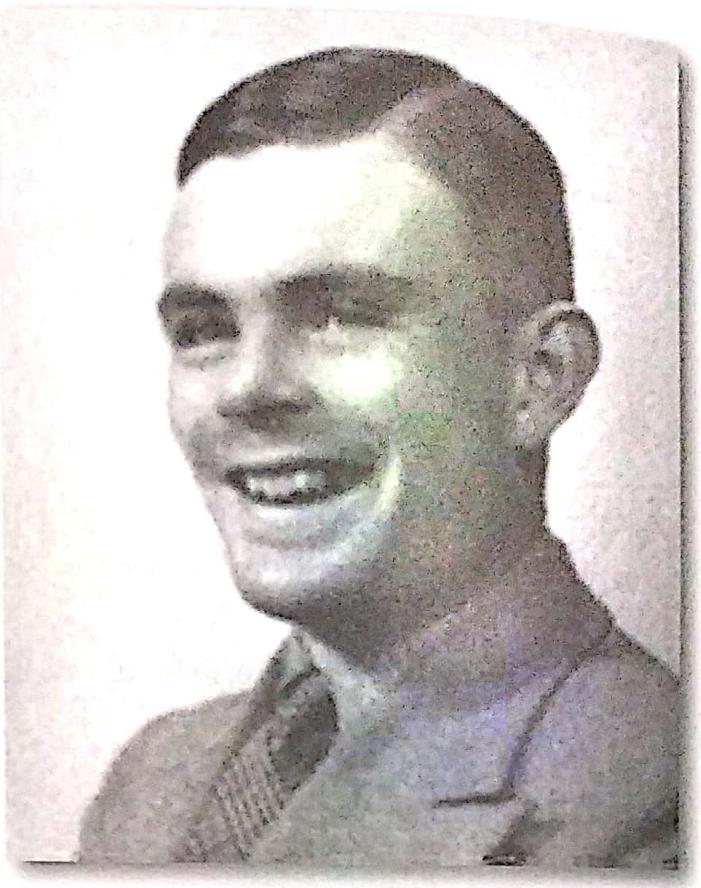
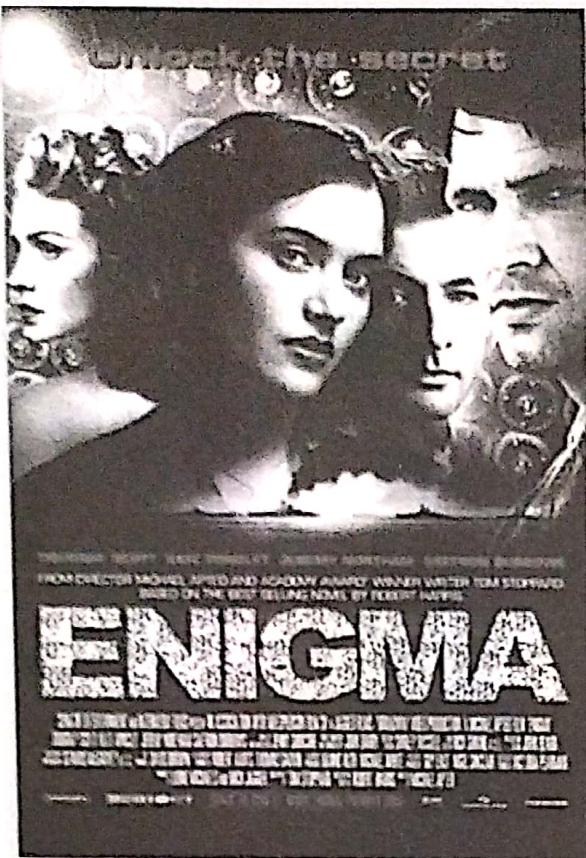
- Veri 1: Hiç bir harf kendisi olarak şifrelenmemiyordu.
- Veri 2: Yaygın Alman ifadeleri: “Heil Hitler”, “Lütfen cevap verin”

Bunların dışında bu süreç içinde Alman operatörlerinin yardımları da olmuştur:

- Test mesajı göndermesi istenen bir alman operatörü sadece T tuşuna defalarca basılmış bir mesaj gönderdi. İngiliz analizci tek bir T harfi olmayan bu uzun mesajı alıcı istasyonlarından ele geçirmiştir.



Şekil 2.24. Enigma



Şekil 2.25. ENIGMA film afisi ve Alan Turing (1912–1954)

- Coğu operatör mesaj kodları için kendi veya kız arkadaşlarının isimlerinin baş harfleri hep aynı ayarları kullanıyordu.
- Her gün gönderilen Hava Durumu mesajları gibi mesajlarda önemli ipuçları sağlanmıştır.

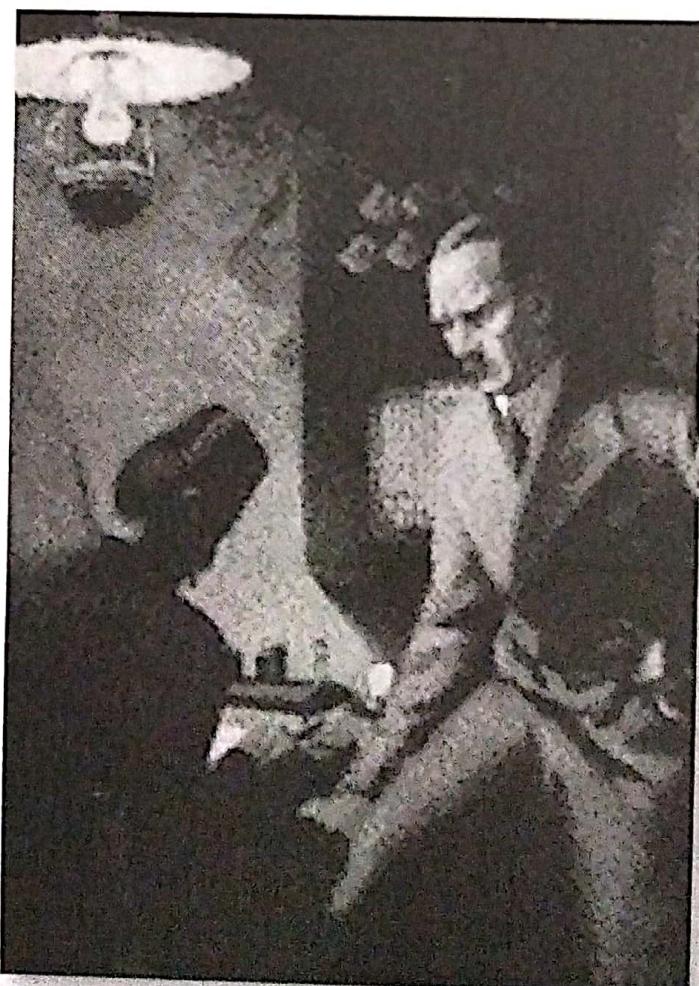
Mayıs 1941'de İngilizler, ele geçirdikleri bir gemide Enigma makinesini, kod kitabı, işletim el kitabı ve şifrenin kırılmasına yarayacak diğer bilgileri ele geçirmeleriyle Enigma şifreleri çözülmüştür. Enigma şifresinin çözüldüğü, 1991 yılına kadar tüm dünyadan saklanmıştır. Bu bilginin elli yıl sırr olarak saklanması "Hiç bir kriptoanalist, hiç bir kriptograf'ın kendi şifresinin çözüldüğünden haberi olmasını istemez." ilkesinin en göze çarpan örneklerinden biridir.

Bu konuda şifreleme tarihinde üzerinde çok düşüntü yapılmış tarihi bir olayın ayrıntıları Şekil 2.26'de verilmiştir [39-45]. 15 Kasım 1940'da 500 kadar alman savaş uçağı İngiliz Coventry şehrini bombaladı. Saldırının kod adı "Ay Işığı Sonatı" (Ludwig van Beethoven [40]) idi ve saldırısı Enigma makineleri kullanılarak şifrelenmişti. Yüzlerce ölü ile beraber şehrin üçte ikisi yıkıldı. Birçok kaynakta İngiliz başbakanı Churchill'in bu saldırından yapılan şifre çözme çalışmaları ile daha önceden haberı olduğu; fakat şehri boşaltmanın bu çalışmaları deşifre edeceği ve ilateride daha önemli bilgilerin elde edilememesine sebep olacağından şehri kendi kaderine bıraktığı belirtilmektedir [39-43].

2.3 ÜLKEMİZDE ŞİFRELEME TARİHİ

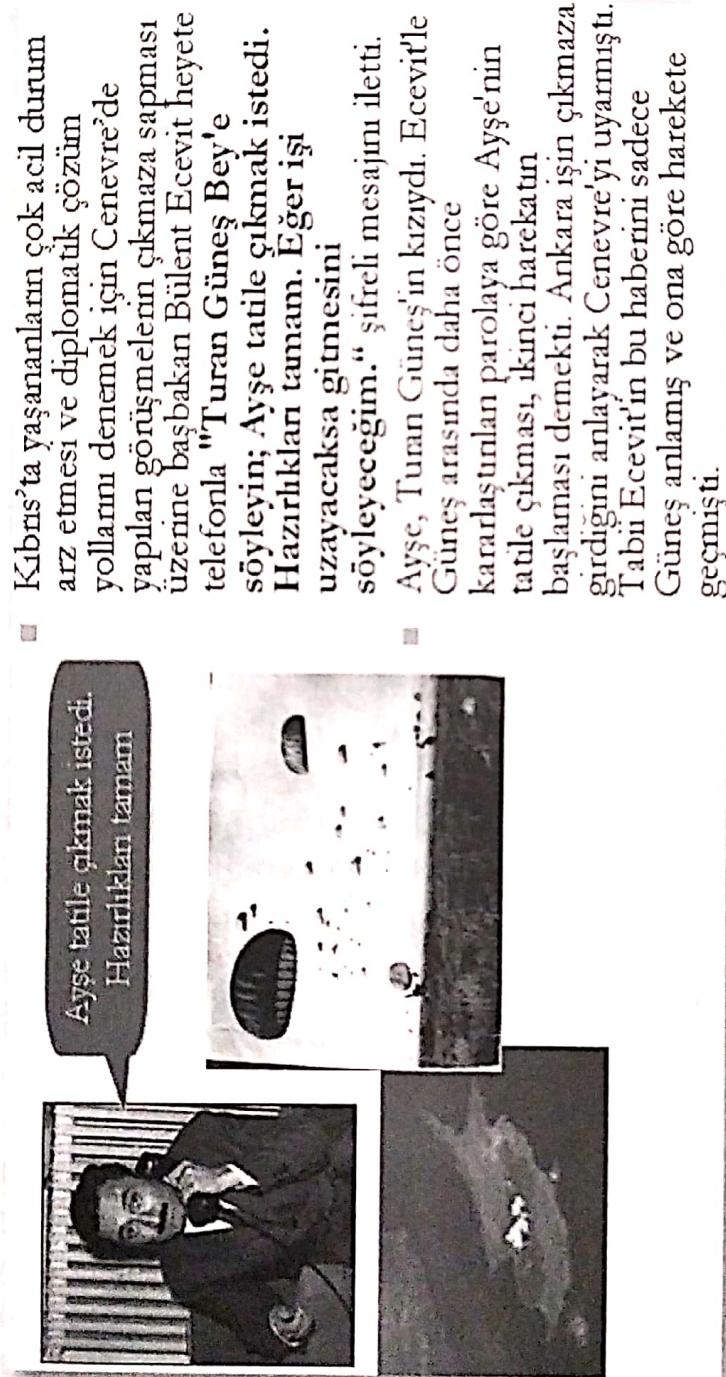
Ülkemizde şifreleme konusu ile ilgili pek fazla kaynak bulunmamaktadır. Bu konudaki araştırmaların yetersiz olduğunu görmekteyiz. Bununla birlikte özellikle 1. Dünya Savaşı, Kurtuluş Savaşı ve Kıbrıs Barış Harekâtında gizli haberleşmeye yönelik uygulamaların olduğu bilinmektedir [65]. Son yıllara kadar kriptoloji ile ilgili çalışmalar yurtdışı kaynaklı olarak karşımıza çıksa da bu konunun öneminin fark edilmesi ile modern kriptografide birçok özgün çalışmalara başlanmış ve bu konuda birçok başarı kazanılmıştır.

Osmanlı zamanında haberleşmede kripto kullanılmaktaysa da tek kelime Osmanlıca bilmeyen Vatikan papazlarının bu şifreleri altı saatte kırabildikleri belirtilmiştir [66]. Osmanlı döneminde Selçuklular zamanında da kullanılan Siyakat yazısı Türkler tarafından bulunan şifreli yazıya bir örnektir. Bu yazı genellikle tapu-tahrir defterlerinde ve Osmanlı iktisadı ile ilgili belgelerde kullanılmaktadır. Yazanın dışında şifresinin çözülmesinin zor olduğu bu yazı türünün, 1900'lu yıllarda bile, var olan belgeleri okuyabilecek personel istihdamında zorluklar çekildiği belirtilmektedir [67]. Günümüzde de arşivlerimizde bulunan Siyakat ile yazılmış belgeleri okuyabilen tarihçi ya da araştırmacı sayısı yok denecek kadar azdır [68].



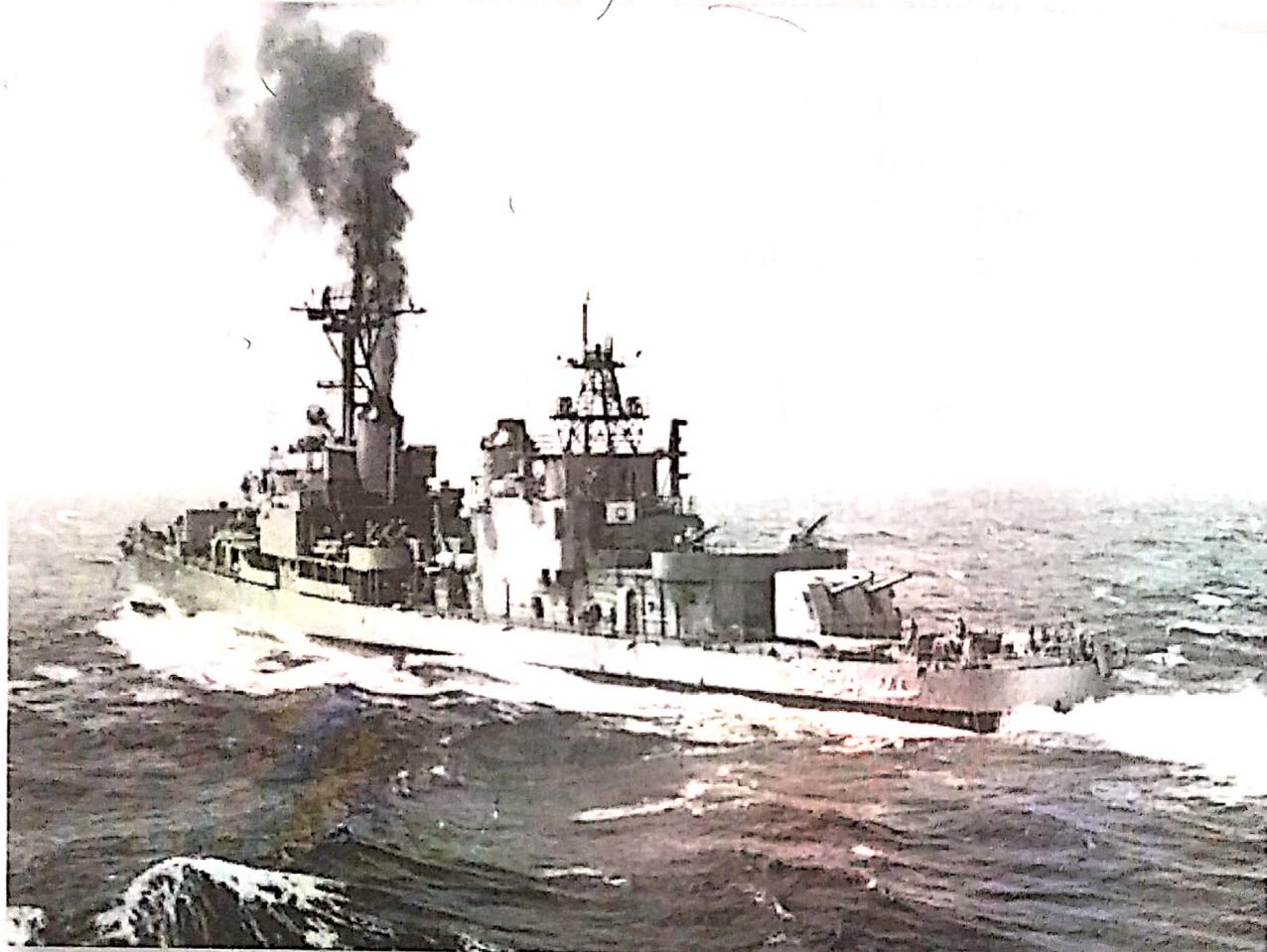
Şekil 2.35. Atatürk telgraf başında [69]

Özellikle kurtuluş savaşında şifreli telgrafların önemi çok fazladır. Savaş zamanında, şifrelerin değiştirilme aralığı sıklaştırılmıştır. Gerçek bir şifre savaşı olarak da adlandırılan II. Dünya Savaşında Türkiye'nin savaşa girip girmeyeceğini anlamak için büyük çaba sarf eden İngilizler, Almanlar ve Ruslar büyük bir dikkatle Türk gizli iletilerini takip etmişlerdir ve tüm bu devletlerin dışişleri, Türk gizli yazışmalarını düzenli olarak deşifre etmişlerdir. II. Dünya Savaşında yaşanan bu gelişmeler şifreleme ve deşifre birimlerini yeniden oluşturulmasına neden olmuştur. Soğuk savaş dönemi ise istihbaratçılar ve şifreciler arasında yaşanan savaşı en üst noktaya getirmiştir [70]. Ülkemizde 1974 Kıbrıs Barış Harekâtı sırasında kullanılan şifreleme ile ilgili yaşanan bir olay Şekil 2.36'da verilmektedir.



Şekil 2.36. Kıbrıs Barış Harekâtında (1974) yaşanan bir şifreleme örneği [71-74]

Ülkemizde şifreleme konusu ile ilişkili olarak tarihi ve trajik bir olaydan bahsetmek, öz eleştiri ve tarihten dersler çıkarmak açısından faydalı olur düşüncesindeyiz. 21 Temmuz 1974'de Kıbrıs Barış Harekâti sırasında Kocatepe Muhibimizin bir parola anlaşmazlığı ve diğer işleyiş hataları sebebi ile kendi savaş uçaklarımız tarafından bombalanmış ve batırılmıştır.



Şekil 2.37. Kocatepe Muhibi

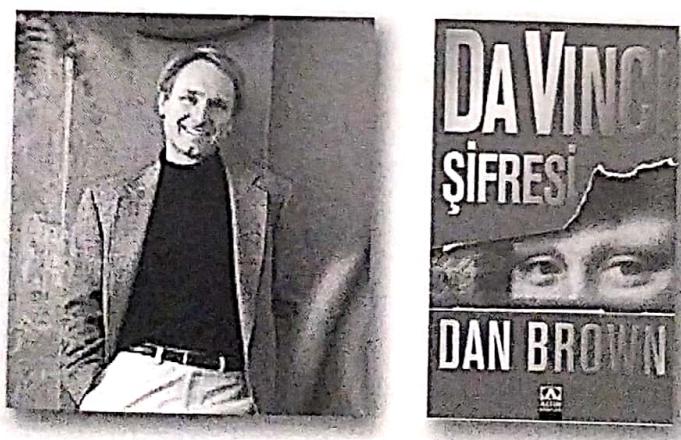
53 askerimizin şehit olduğu bu elim olayda, bölgedeki Yunan gemilerini batırma emri alan savaş uçağı pilotlarının, bölgede Türk unsurlarının bulunmadığı bilgisi ve muhibi Türk bayrağı çekmiş bir Yunan gemisi olduğu düşüncesi ile bombalamaya başlamıştır. Bunun üzerine gemiden telsizle yapılan "Biz Türk gemisiyiz, saldırmayın" mesajına, konuşan kişilerin "çok iyi" Türkçe bilen Yunanlılar olduğu kanısıyla pilotlar gemiden parola sormuş; parolanın verilmemesi üzerine Kocatepe ağır hasar alarak ikiye bölünmüş ve batmıştır [75]. Aslında her askeri harekât için dost zayıatı diye bir bölüm bulunmaktadır. Her ordu buna benzer hadiseler yaşayabilir. Günümüz modern Deniz Kuvvetlerimizin bu konuda gerekli çalışmaları yerine getirdiğini ve Amerika'da indirme, çıkışma, atma planları ve koordinasyonu açısından ders olarak verilen Kıbrıs Barış Harekâtındaki bu olaydan da gerekli dersleri çıkardığını biliyoruz [76].

Ülkemizde 1980'li yıllara kadar askeri alanda bile kullanılan kripto makineleri yurtdışından satın alınmıştır [77]. Edinilen acı tecrübeler ışığında milli savunma sanayinin gelişmesi ile kripto sistemlerinde "milli algoritmanın" kullanılması gerekliliği kabul görmüş ve gerekli adımlar atılmıştır.



Şekil 2.38. Şifreleme ile ilgili popüler konular (kitaplar, gazete başlıklarları) [78 -82]

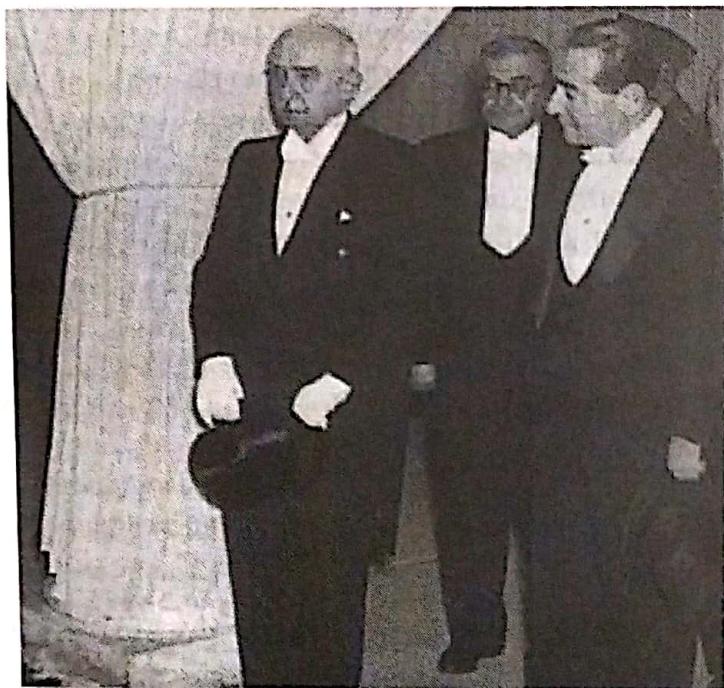
Her ne kadar günümüzde şifreleme ile ilgili çok değişik konular gazete, dergi, televizyon ve gazete başlıklarında gündemde olmasına rağmen (Şekil 2.38); ülkemizde de bu konudaki bilimsel çalışmaların sayısının artacağı değerlendirilmektedir. Bugünlerde 44 ayrı dilde 25 milyondan fazla satan ve en çok satan kitap rekoru kıran Dan Brown'ın "Da Vinci Şifresi" (Bkz. Şekil 2.39), ülkemizde de çok okunan kitaplar arasına girmesi şifreleme konusunda toplumsal duyarlılığın ve merakın bir ölçüsü olarak değerlendirilmektedir [83].



Şekil 2.39. Dan Brown (1964) ve ünlü kitabı "Da Vinci Şifresi"

Türkiye'de özellikle iletişim alanında kullanılan telefonlar ile ilgili bilgi güvenliği açısından ele alınan husus, şu günlerde de gündemde sıkça yer alan "telefonların dinlenmesi" ya da yazılı ve görsel basında dile getirildiği şekliyle "telekulak" konusudur.

Başbakanlık'ın kamuya açtığı Yassıada belgeleri, Türkiye'nin demokrasiye geçtiği gün telekulakla tanıştığını ortaya koymaktadır [84]. Demokrat Partinin (DP) 1950 yılında işbaşına geldiğinde, o zaman haberleşme altyapısını sağlayan PTT içinde özel bir dinleme birimi oluşturulduğu, 56 yıl sonra kamuoyu ile paylaşılmıştır. Kime bağlı olarak oluşturulduğu konusunda bilgi verilmese de; cumhurbaşkanı, başbakan ve bakanların konuşmalarının dinlenilmiş ve kayıt altına alınmış olması çok hayret vericidir. İşin daha ilginci de Başbakan Adnan Menderes'in bir yandan dinlenirken; diğer yandan da CHP'yi dinletmiş olmasıdır.



Şekil 2.40. CHP başkanı İsmet İnönü (1884–1973) ve DP başkanı, başbakan Adnan Menderes (1899–1961) bir kabul töreninde

Başbakanlık Devlet Arşivleri Genel Müdürlüğü arşivinde bulunan telekulakla ilgili dosyada, 29 Nisan–3 Mayıs 1959 tarihleri arasında dinlemesi yapılan telefonlardan kimlerle ve ne kadar konuşulduğuna dair bir liste, Yassıada Soruşturma Kurulu'nun talebi üzerine Ankara Telefon Müdürlüğü tarafından mahkemeye teslim edilmiştir.

Telekulak konusu son yıllarda özellikle yaygın cep telefonu kullanımı ve özel hayatı müdahale başlıklarıyla tartışılmaktadır. 2005 Temmuz ayında çıkarılan telefon dinlemeye ilişkin 5397 sayılı yasayla; MİT, polis ve jandarma tarafından yapılan telefon dinleme işlemlerinin tek merkez üzerinden yürütülmesi ve denetlenmesine ilişkin düzenleme yapılarak

bu konu üzerindeki belirsizlik ve tartışmaların önüne geçilmeye çalışılmıştır. Yasa uyarınca Telekomünikasyon Kurumu bünyesinde TİB (Telekomünikasyon İletişim Başkanlığı) adı altında yeni bir kurum oluşturulmuş; bu merkezin denetimi altında yürütülecek olan adli ve istihbarat amaçlı dinleme işlemleri hâkimden izin alınması şartına bağlanmıştır.

Telekomünikasyon İletişim Başkanlığı, 2559 sayılı Polis Vazife ve Salahiyyet Kanunu, 2803 sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunu ile 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nda değişiklik yapan 23.07.2005 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren 5397 sayılı yasa ile Telekomünikasyon Kurumu bünyesinde kurulmuştur.

Başkanlığın çalışma usul ve esaslarıyla ilgili olarak, Başbakanlıkça çıkartılan "Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik" de 10.11.2005 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

10 Ağustos 2006 tarihinde Telekomünikasyon Kurul Başkanı Dr. Tayfun Acarer ve Telekomünikasyon İletişim Başkanı Fethi Şimşek'in yapmış olduğu basın toplantısında (Bkz. Şekil 2.41), "Telekomünikasyon İletişim Başkanlığının istihbarat toplayan, topladığı bilgileri değerlendiren ve ilgili makamlara sunan bir istihbarat kurum veya kuruluşu olmadığı" vurgulanmış; "kuruluş yasasında da belirtildiği üzere; telekomünikasyon yoluyla yapılan iletişimini tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına ilişkin ilgili kurum faaliyetlerinin hâkim kararları çerçevesinde yürütülmesini sağlayan Telekomünikasyon kurumu bünyesinde bir birim" olduğu ifade edilmiştir [85].



Şekil 2.41. Telekomünikasyon Kurul Başkanı Dr. Tayfun Acarer (1956) ve Telekomünikasyon İletişim Başkanı Fethi Şimşek (1956)