*Orhun Kara*

*Dr., TÜBİTAK UEKAE*
*Başuzman Araştırmacı*

# II. Dünya Savaşı'ndan Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme

II. Dünya Savaşı'nda Enigma şifreleme cihazını yaygın olarak kullanan Almanlar, savaş sırasında Enigma şifrelerinin Müttefikler tarafından kırıldığının farkında değildi. Yaklaşık yarım milyon Alman mesajını çözen Müttefikler Atlantik'teki Alman "U-boat" savaşında, Normandiya Çıkarması'nda ve Afrika Çöl Savaşları'nda büyük avantaj elde etti. Öyle ki şifre kırma faaliyetlerinin karargâhı haline gelen Londra yakınlarındaki Bletchley Park için Alman Ordusu BBG evi gibiydi!

**Anahtar Kavramlar**

II. Dünya Savaşı'nda Almanlar Enigma adlı daktilo benzeri şifreleme cihazını yaygın olarak kullandılar. Savaş sonunda ordunun envanterine kayıtlı yaklaşık yüz bin Enigma vardı.

Enigma şifrelerini ilk Polonyalılar kırdı. Ardından İngilizler Bletchley Park'ta Enigma'nın analizi üzerinde çalıştılar. Bletchley Park'ın şifre kırıcıları ülkedeki en yetenekli matematikçilerden, satranç oyuncularından ve bulmaca meraklılarından seçilmişti.

Claude Shannon'ın 1949'da Bell Laboratuvarları'nın teknik dergisinde çıkan "Gizli Sistemlerin Haberleşme Teorisi" adlı makalesi modern simetrik sistemlerin tasarım felsefeleri ve güvenlik modelleri için bir temel oluşturmuştur.

Diffie ve Hellman 1976'da IEEE'nin *Information Theory* dergisinde çıkan "Kriptografide Yeni Yönler" adlı makalelerinde açık bir kanalda iki tarafın nasıl güvenli anahtar paylaşabileceğine dair bir metot önerdiler. Bu makale kriptoloji biliminde çığır açtı.

Rijmen ve Daemen adlı iki Belçikalı kriptoloğun tasarladığı Rijndael adlı algoritma, AES adıyla 1976'da standart olarak kabul edilmiş olan DES adlı algoritmanın yerine standart şifreleme algoritması olarak seçildi.

Bilkent Üniversitesi Matematik Bölümü'nden mezun olan Orhun Kara aynı bölümde yüksek lisans ve doktorasını tamamladı. 2001 ve 2002 yıllarında Fransa'da CNRS'e bağlı IML'de (Institut de Mathématiques de Luminy) Prof. Serge Vladuţ ile çalıştı. Literatürde "reflection attack- yansıtma atağı" olarak bilinen kendine benzeşim atağını buldu. Ayrıca *How to Break Gilbert-Varshamov Bound* adlı kitabın yazarlarındandır. TÜBİTAK UEKAE'de kripto algoritmalarının tasarımı ve analizi üzerinde çalışmaktadır.

Arthur Scherbius adlı bir Alman mühendis XX. yüzyılın başlarında, özellikle bankaların ve iş adamlarının gereksinimleri doğrultusunda ticari gizliliği sağlayacak, pratik, kullanışlı ve güçlü olduğunu düşündüğü rotorlu bir kripto cihazı tasarladı ve cihazına "muamma, bilmece" anlamına gelen Enigma ismini verdi.

Scherbius'un Enigma'sı ilk sürümlerinde hantal olsa da, birkaç sürümden sonra olgunlaştı ve hafifledi. Scherbius, zengin olma hayalleriyle Enigma'ya patent aldı ama iş dünyasından beklediği ilgiyi göremedi. Ticari Enigma İsviçre ordusunda, İspanyol İç Savaşı'nda ve İtalyan donanmasında görev aldı.

Enigma'nın yıldızı asıl Alman donanmasının ilgisiyle parlayacaktı. Almanlar Versay Antlaşması'nın kırgınlığı içinde çoktan yeniden var olma mücadelesine girmişlerdi. Baş döndürücü bir hızla silahlanıyorlardı. Savaş alanında kullanışlı, hafif, ucuz, pratik, anahtar değişimi ve kurulumu kolay bir kripto cihazına ihtiyaçları olacaktı. Enigma tam istedikleri türden bir cihazdı. İlk olarak, o dönemki adı "Kriegsmarine" olan Alman donanması Enigma kullanmaya başladı. Ardından 1930'lu yılların başlarında Alman Gizli Servisi

"Abwehr", Alman Kara Kuvvetleri "Wehrmacht" ve Alman Hava Kuvvetleri "Luftwaffe", kendi birimlerinde gizli haberleşme için Enigma'yı kullanma kararı aldılar. Enigma II. Dünya Savaşı sırasında Alman ordusunun en yaygın kullandığı şifreleme cihazı oldu. Savaş sonunda ordunun envanterinde kayıtlı yaklaşık yüz bin Enigma vardı.

Enigma yaklaşık 10 kg ağırlığında, daktilo benzeri, rotorlu, elektromekanik bir şifreleme cihazıdır. Tuş takımının hemen üst kısmında 26 harften oluşan ışıklı bir pano yer alır. Operatörün her tuşa basımında ışıklı panoda bir harfin ışığı yanar; bu harf, karşılık gelen şifreli karakter olur.

Enigma'daki matematiksel fonksiyonlar 26 elemanlı harf kümesindeki permütasyonlardı. Bu permütasyonlar ticari Enigma'da üç rotor ve bir yansıtıcıyla ifade ediliyordu. Her bir rotorun bir tarafında 26 pin, diğer tarafında 26 levha bulunuyordu. Her bir pin, rotorun öbür yüzündeki levhalardan birine içerden bir kablo ile bağlıydı. Böylece bir pinden geçen elektrik akımı rotorun diğer tarafında bir levhadan çıkıyor ve bu da 26 elemanlı bir alfabede bir permütasyon ifade ediyordu.

Rotorlar, bir rotorun pinleri diğerinin levhalarına temas edecek şekilde bir çubuk ekseninde, dik konumda yan yana yerleştiriliyor ve en soldaki rotorun levhaları da yansıtıcının pinlerine temas ediyordu. Böylece bir rotorun levhasından geçen elektrik akımı bir sonraki rotorun bu levhaya temas eden pinine atlıyordu. Akım bu şekilde yoluna devam ediyor ve üç rotordan da geçtikten sonra yansıtıcıya ulaşıyordu. Yansıtıcının 26 pini vardı ve kablolarla bu pinler içeriden ikişer ikişer birbirlerine bağlanmışlardı. Böylece bir pinden gelen elektrik akımı diğer bir pinden çıkıp, yansıtıcıya temas eden rotorun başka bir levhasına geri dönüyordu. Akım rotorlardan, rotorların iç telleri üzerinde bu sefer ters yönde ve bambaşka bir yol çizerek tekrar geçiyor ve ardından ışıklı panoya ulaşıyordu. Böylece batarya ile panodaki 26 lambadan biri arasında devre tamamlanmış oluyor ve bu lamba yanıyordu.

Tuşa her basıldığında en sağdaki rotor bir harf kayacak şekilde, yani bir turun yirmi altıda biri kadar dönüyor ve böylece içsel permütasyonlar değişmiş oluyordu. En sağdaki rotor bir tur döndüğünde ortadaki bir harflik, ortadaki bir tur döndüğünde en soldaki bir harflik dönüyordu. Bu da oluşan permütasyonlar kümesinin periyodunun son derece yüksek olmasını sağlıyordu. Bir harfi şifreleme için kullanılan bir permütasyon ancak bütün rotorlar birer tam tur döndüğünde, yani 26x26x26=17576 harf şifrelendikten sonra tekrar kullanılıyordu. Böylece

http://www.nationalmuseum.af.mil

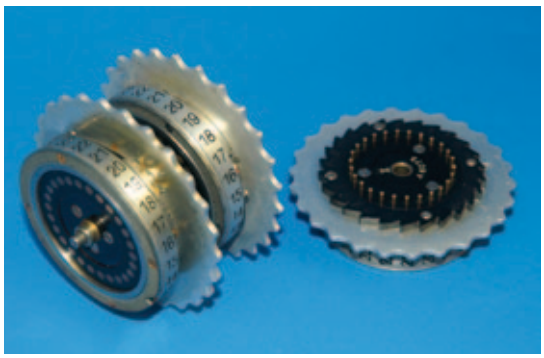
http://www.nationalmuseum.af.mil

Enigma operasyonda. Alman Hava Kuvvetleri askerleri Enigma'nın başında. Bir operatör şifreleme yaparken (şifre çözerken) diğer operatör kaydediyor.

pratikte her harf şifrelenişinde farklı bir permütasyon kullanılmış oluyordu.

Enigma permütasyonların özelliği *involüsyon* olmalarıydı, yani harfler karşılıklı olarak birbirlerine gidiyorlardı. Örneğin A harfi Z'ye gidiyorsa Z harfi de A'ya gidiyordu. Bu durum yansıtıcının da *involüsyon* olması ve yansıtıcıdan sonra rotorların belirlediği permütasyonların ters yönde ve ters sıra ile tekrar uygulanması sayesinde oluyordu. Böylece cihazın aynı kurulumuyla şifre çözme de kolayca gerçeklenebiliyordu.

Alman ordusunda kullanılan Enigma'ya ticari Enigma'lardan farklı olarak bir de "steckerbrett" denilen fişleme tablosu eklenmişti. Hemen tuş takımının ardında yer alan bu tabloda 26 harf oyuğu bulunuyordu. Bir fişin bir ucu bir harfin oyuğuna, diğer ucu da başka bir harfin oyuğuna takıldığında bu iki harf yer değiştirmiş gibi davranıyordu. Örneğin A harfi ile Z harfi bir fiş ile bağlandığında, A harfi Z, Z harfi de A gibi davranıyordu. Operatör A harfine bastığında sanki Z harfine basılmış gibi elektrik akımı rotorlara iletiliyordu. Şifre çözme işleminin de aynı olması açısından, cihazın ürettiği permütas-



wikimedia

Enigma'nın rotorları. Yan yatmış rotorda 26 pin ve öndeki rotorda 26 levha gözükmektedir.

yonları *involüsyon* yapmak gerekiyordu. Bu yüzden akım son olarak ışıklı panoya gelmeden fişleme tablosundan tekrar geçiyordu.

Fişleme tablosunda çiftler halinde hangi harflerin kablolarla birbirlerine bağlanacağı anahtar bilgisiydi ve bu da tek tek deneme yoluyla anahtarı bulmayı pratikte imkânsız kılacak kadar çok kombinasyon sunuyordu. 26 harften 13 çift $26!/(13!\times 2^{13})$ farklı yolla oluşturulabilir ki bu da 13 basamaklı bir sayıdır.

Ticari Enigma'dan farklı başka bir uygulama olarak Almanlar beş rotor bulunduruyor ve üçünü seçerek kullanıyorlardı. Bu da anahtar bilgisinin bir parçasıydı ve sisteme 60 kat karmaşıklık getiriyordu.

Ticari Enigma'yı Polonyalılar ve İngilizler kırdılar. İngilizler şifre kırma faaliyetlerini kurumsal hale getirmek için GC&CS (Government Code and Cipher School - Devlet Kod ve Şifre Okulu) adlı bir yapı oluşturmuştu. GC&CS İspanyol İç Savaşı'nda kullanılan Enigma şifrelerini çözmeyi başarmıştı, ama 1930'lu yıllarda Alman Ordusunun Enigma'sı İngilizler için hâlâ bir muammaydı.

Alman Enigma'sını ilk kıranlar Polonyalılar oldu. Polonyalılar yaklaşan Alman tehlikesini sezmiş olacaklar ki daha 1930'lu yılların başlarında, Varşova yakınlarında en iyi matematikçilerin toplandığı bir şifre kırma okulu kurdular. Bu okulda en başarılı üç matematikçiyi -Marian Rejewski, Henryk Zgalski ve Jerzy Rozicki- Enigma'yı analiz etmek üzere çok gizli bir görevle Biuro Szyfrom'a (Şifre Bürosu) aldılar. Bu üç matematikçinin Biuro Szyfrom'da yoğun çalışmaları kısa sürede meyvelerini verdi ve Polonyalılar Enigma'yı kırmayı başardı.

Hans-Thilo Schmidt adlı bir Alman casusun Fransızlara aktardığı bilgiler Enigma'nın analizinde Polonyalıların oldukça işine yaradı. Ayrıca bir başka gelişme Polonyalıların ekmeğine yağ sürecekti. Alman hükümeti büyük bir hata yaparak bir diplomatik Enigma'yı Berlin'den Varşova'daki büyükelçiliğe sıradan bir kargo gibi gönderdi. Bunu fark eden Polonyalılar Enigma'yı ele geçirdiler ve iki gün boyunca kurcaladılar. Cihazların iç tel sistemlerini inceleyip fotoğraflarını çektiler. Ardından hiçbir şey olmamış gibi paketleyip Alman Büyükelçiliği'ne teslim ettiler. Almanlar durumun farkına varmadı ama Polonyalılar sistemle ilgili her şeyi öğrenmişti. Hatta iki tane kopya Enigma dahi ürettiler.

Biuro Szyfrom'da özellikle Marian Rejewski, Enigma'nın analizinde oldukça başarılı sonuçlar elde etti. Enigma'nın iç sisteminin birçok permütasyonu üretemeyeceğini keşfetmişti. Sonuçta rotorların oluşturduğu permütasyonları olası adaylar arasından eleme yoluyla bulan bir cihaz geliştirdi. Cihaza "bombe" adı verilmişti. Bu, tarihte bilinen ilk kriptoanaliz cihazıydı ve altı Enigma cihazını aynı anda taklit edebiliyordu. Bir rivayete göre, cihazdaki Enigma rotorlarını taklit eden yassı toplar o dönem Polonya'da yaygın olan ve bombe adı verilen tatlılara benzediği için cihaza bombe adı verilmişti. Başka bir rivayete göre ise cihazın ismi bu topların çalışırken, düşen bombaların ıslıkları gibi ses çıkarmalarından geliyordu.

Bombe cihazlarını Polonya'nın radyo fabrikası olan AVA şirketi üretiyordu. 1939 sonbaharında Almanların Polonya'yı işgalinden hemen önce kriptoanaliz faaliyetleri durduruldu ve Biuro Szyfrom lağ-

Visual Photos

Alman donanması tarafından 1942'den sonra kullanılan ve M4 adı verilen dört rotorlu Enigma.

vedildi. Polonyalılar hiçbir kanıt bırakmamak için bütün çalışmaları ve bombeleri yok ettiler. Bu yüzden maalesef günümüze Polonya bombesinden bir örnek, hatta bir fotoğraf dahi kalmamıştır.

Alman işgaliyle birlikte Polonyalı kriptoanalistlerin birçoğu Fransa'ya veya İngiltere'ye kaçtı. Enigma'nın kriptoanalizi artık İngilizlere kalmıştı. İngilizler 1930'lu yıllarda bu konuda Polonyalılardan çok şey öğrendiler. GC&CS, karargâhını 1939'da Londra'dan yaklaşık 90 km uzakta bir banliyö kasabası olan Bletchley'de kurdu. Kriptoanaliz çalışmalarını başlangıçta küçük ve mütevazı bir ekip yapıyordu. İşler büyüdükçe ekip de genişledi. Öyle ki savaşın sonuna doğru yaklaşık 8000 kişilik dev bir kriptoanaliz ordusu harıl harıl Alman şifrelerini çözmekteydi.

Bletchley Park'ta çalışan şifre kırıcılar ülkedeki en yetenekli matematikçilerden, satranç oyuncularından ve bulmaca meraklılarından seçilmişti. Bu isimler arasında özelikle Alan Turing ve Gordon Welchman dikkat çekiyordu. Turing, Polonya bombesi üzerinde yoğun bir çalışmaya daldı ve sonunda kendisi de bir Enigma şifre kırma cihazı geliştirmeyi başardı. Cihazın çalışma ilkesi Polonya bombesinden çok farklı olmasına karşın bu cihaza da bombe ismi verildi.

İngiliz bombeleri bir ton ağırlığında ve üç yatay bataryadan oluşan devasa makinelerdi. Bataryalar, her bir sırası Enigma rotorlarını taklit eden dönen toplardan oluşan üç sıra teşkil ediyordu. En hızlı dönen top Enigma'nın en soldaki rotorunu temsil ediyordu ve saniyede iki tur atıyordu. Bir Enigma aynı hızda çalıştırılmak istense saniyede 52 tuşa basmak gerekecekti! Üstelik bir bombe üzerinde onlarca Enigma simülasyonu aynı anda paralel çalışıyordu.

Bu devasa kriptoanaliz makineleri çok hızlı onlarca Enigma gibi davransa da makinelerin anahtarları tek tek deneyerek bulmaları yıllar alacak bir işlemdi. Bombelerin taramaları aslında Turing'in keşfettiği Enigma'nın bir zayıflığını kullanıyordu ve aday permütasyonlar şaşırtıcı bir hızla eleniyordu.

Bombeler BTM (British Tabulating Machine-İngiliz Tablolama Makinesi) fabrikası tarafından büyük bir gizlilikle üretiliyor ve Bletchley Park'a getiriliyordu. İlk iki bombe 1940'ın Mart ayında göreve başladı. İngilizler savaş sonuna kadar 200'den fazla bombe ürettiler ve bu makinelerle neredeyse yarım milyon Alman mesajını çözmeyi başardılar.

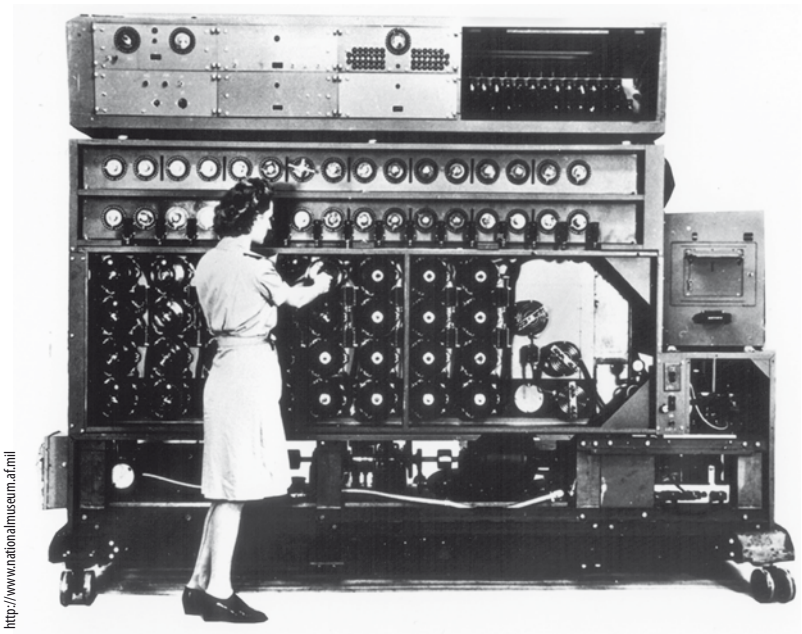
Y istasyonları adı verilen dinleme istasyonlarında toplanan sinyallerden şifreli metinler çıkarılıyor ve Bletchley'e gönderiliyordu. Bletchley'de çözülen metinler sınıflandırılıyor ve kurmaylar tarafından değerlendirmeye alınıyordu. Almanlar günlük anahtar kullanıyorlardı. Genellikle gece yarısı değiştirilen anahtarlar, öğleye doğru Bletchley'de İngilizlerin eline geçmiş oluyordu.

Visual Photos

Enigma'nın rotorları.

İngiliz bombesi "bilinen açık metin atağı" uyguluyordu. Dolayısıyla İngilizlere Y istasyonlarında topladıkları şifreli metinlerin bir kısmına karşılık gelen açık metinler gerekiyordu. Ancak açık metin elde etmek onlar için hiç de zor olmadı. Sabit hava raporları, mesajların belli yerlerinde geçen "cevap bekleniyor", "derhal" gibi tekrar eden sözcükler, kalıplaşmış askeri terimler, mesajların standart başlangıç ve bitiş şekilleri, test mesajları ve içi doldurulan matbu formlar İngilizlere kolayca açık metin sağlıyordu.

Bombe üretmek oldukça pahalıya mal oluyordu. Üstelik 1942 başlarında Alman donanması Enigma'ya bir rotor daha eklemişti. M4 kodlu bu Enigma'lara Bletchley sakinleri "shark" (köpek balığı) adını verdiler. Çözülemeyen "shark" kodları Bletchley'i zor durumda bırakıyordu. İngilizler ABD'den yardım istediler. Amerikalılar da 1942'nin sonlarında bombe üretmeye başladılar. Onların



http://www.nationalmuseum.af.mil

WAVES adı verilen operatörlerce kurulan ABD donanma bombesi. Bu dev makinelerde Turing'in Enigma'ya karşı geliştirdiği atak gerçekleniyordu.

bombesi 2,5 ton ağırlığındaydı ve daha hızlı çalışıyordu. Ürettikleri ilk iki bombeye Âdem ve Havva adını koydular. İlginçtir, projenin başında Joseph Desch adlı bir Alman vardı. Ar-Ge çalışmaları NCML'de (Naval Computing Machine Lab-Donanma Hesaplama Makineleri Labaratuvarı) yapıldı ve bombeler NCR (National Cash Register-Ulusal Kasa) firmasında üretildi (Bir ATM cihazından para çekerken cihazın bir köşesinde NCR yazısı dikkatinizi çekmiş olabilir. NCR aynı zamanda ATM de üretiyor). Amerikalılar savaş sonuna kadar yüzden fazla bombe ürettiler.

Alan Turing ve ekibi M4 Enigma'sının analizleri üzerine yoğun çalışmalarının semeresini görmeye başladı. 1942'nin sonbaharına doğru Bletchley Park'ta artık köpek balığı kodları çözülebiliyordu. ABD bombeleri de köpek balığı kodlarını okuyabiliyordu.

Bletchley Park'ta sadece Enigma kodları çözülmüyordu. Yüksek rütbeli Alman askerlerin ve kurmayların kullandığı Lorenz SZ-40 Schlüsselzuzatz eklenti şifresi tam 12 rotorluydu ve teleyazıcı devreleri için kullanılıyordu. Bletchley'de Lorenz ile gönderilmiş şifrelere "tuna kodu" deniliyordu. Tuna kodları John Tiltman ve William Tutte tarafından analiz edildi ve kırıldı. Sonuçta, Hitler'in haberleşmesi bile dinlenebilir hale geldi. Bletchley'de tuna kodlarını çözmek için Colossus adı verilen ve delikli şerit kâğıtlar yardımıyla programlanabilen dev cihazlar geliştirildi.

Bletchley Park projesinin başında, büyük bir gizlilik içinde yapılan şifre kırma işlemlerine "ultra sır" adını veren dönemin başbakanı Churchill vardı. Bu yüzden projeye "Ultra Projesi" dendi. Bletchley Park'ta olup bitenler o kadar gizli tutuluyordu ki "ultra" bilgileri kullanılırken kaynağın "boniface" (hancı) kod adlı bir casus olduğu söyleniyordu.

Ultra Projesi Atlantik'te, Afrika Çöl Savaşları'nda ve Normandiya Çıkarması'nda Müttefiklere önemli avantajlar sağladı. Birçok tarihçi Bletchley'deki şifre kırıcılar sayesinde savaşın en az iki yıl kısaldığı konusunda hemfikir. Müttefikler Atlantik'teki Alman denizaltılarının yerlerini kolayca saptadılar. Ayrıca, I. Dünya Savaşı'nda efsane olmuş Alman komutan Mareşal Rommel, şifre kırıcıların da etkisiyle Afrika'daki savaşı kaybetmişti. Bletchley Park, Akdeniz'deki Alman mühimmat gemilerinin yerlerini gerçek zamanda saptayabiliyordu. Üstelik Almanların savaş planları anında İngiliz Mareşal Montgomery'in önüne seriliyordu. Öyle ki Hitler'in Rommel'e gönderdiği bazı mesajlar gecikebiliyor ve bu mesajlar Rommel'e ulaşıncaya kadar, çoktan Bletchley Park'ta çözülmüş ve Montgomery'e iletilmiş oluyordu.

Şifre kırıcıların elde ettiği bilgiler Normandiya Çıkarması'nda General Eisenhover'ın -kendi ifadesiyle- işini çok kolaylaştırmış ve birçok askerinin hayatını kurtarmıştı.

Ultra Projesi'nin başarısında Bletchley Park'taki çok geniş ve yetenekli bir kadronun hummalı çalışması ve projenin iyi yönetilmesi kadar, Enigma'daki analitik zayıflıklar ve operatörlerin yaptığı kripto ihlalleri de (kripto güvenliği için uyulması gereken kuralların göz ardı edilmesi) etkili olmuştu. Tarih ders alınacak olaylarla doludur. Bletchley Park buna güzel bir örnektir.

Enigma gerçekten de çağına göre son derece üstün bir şifreleme makinesiydi. Ancak Alman ordusu Enigma'yı kullanmadan önce detaylı test ve analizlerden geçirmedi. Böylece kolayca önlem alınabilecek zayıflıklar gözden kaçmış oldu. Almanlar Enigma'ya aşırı güvendiler ve Enigma trafiğinin dinlenmesinin imkânsız olduğunu düşündüler. Düşmanlarının kriptoanaliz kabiliyetlerini ve hesaplama güçlerini küçümsediler. Ancak bu aşırı güven Almanlara pahalıya mal oldu.

II. Dünya Savaşı'nın bir başka büyük kriptoanaliz projesi de ABD donanmasının yürüttüğü "Magic Projesi"ydi. Japonların diplomatik amaçlı kullandıkları rotorlu bir şifreleme cihazı olan "Purple", ABD kriptoanalistleri tarafından kırıldı. Gerçi Japon ordusu askeri gizli haberleşmelerin diplomatik cihazlarla yapılmamasına özen gösteriyordu ama ABD'li kriptoanalistler İngilizlerin de yardımıyla Purple'la şifrelenmiş iki önemli mesajı açmayı başardılar. Bunlardan biri Berlin'deki Japon büyükelçi-

sinin, Hitler'le görüşmelerini uzun bir rapor halinde, Purple'la Japonya'ya gönderdiği mesajdı. Diğer mesaj ise Pearl Harbor saldırısından önce Japon hükümeti tarafından ABD'deki Japon Büyükelçiliği'ne gönderilen bir dizi acil talimat listesiydi. Bu talimatlardan özellikle iki tanesi dikkat çekiciydi: ABD ile bütün ilişkiler derhal kesilecekti ve ABD karasularındaki bütün Japon gemilerinin acilen ABD karasularını terk etmesi sağlanacaktı.

## II. Dünya Savaşı Sonrasında ve Günümüzde Kriptoloji

II. Dünya Savaşı'nın ardından kriptolojinin artık bir bilim olma yolunda emin adımlarla ilerlediğini görüyoruz. Claude Shannon'ın 1949'da Bell Laboratuarları'nın teknik dergisinde çıkan "Gizli Sistemlerin Haberleşme Teorisi" adlı makalesi modern simetrik sistemlerin tasarım felsefeleri ve güvenlik modelleri için bir temel oluşturmuştur.

1970'li yılların başlarında, içlerinde Feistel ve Coppersmith'in de olduğu IBM mühendisleri tarafından tasarlanan LUCIFER adlı blok şifreleme algoritmasının Shannon'un 1949'da ortaya koyduğu ilkeleri taşıdığını görebiliriz. Bu algoritma daha sonra NSA (National Security Agency-Ulusal Güvenlik Ajansı) tarafından analiz edildi ve bazı değişikliklerden sonra oluşturulan yeni algoritma, 1976'da NBS (National Bureau of Standards-Ulusal Standart Bürosu, daha sonra NIST olarak değişti) tarafından, DES (Data Encryption Standard- Veri Şifreleme Standardı) adıyla ABD'nin standart şifreleme algoritması olarak kabul edildi. DES 64 bit blok uzunluğunda, 56 bit anahtar boyu olan bir blok şifreleme algoritmasıdır.

DES'in standart olarak kabul edildiği yıl bir başka gelişme kriptolojide bambaşka bir ufuk açacaktı. Diffie ve Hellman IEEE'nin (Institute of Electrical and Electronics Engineers- Elektrik ve Elektronik Mühendisliği Enstitüsü) *Information Theory* (Bilgi Teorisi) dergisinde çıkan "Kriptografide Yeni Yönler" adlı makalelerinde, açık bir kanalda iki tarafın nasıl güvenli anahtar paylaşabileceğini anlatıyorlardı. Bu anahtar paylaşım protokolünün güvenliği matematikte ayrık logaritma probleminin çözümünün zorluğuna dayanıyordu. Böylece açık anahtarlı kriptografi doğmuş oldu. Hemen bir yıl sonra Rivest, Shamir ve Adelman açık literatürün ilk ve belki de en çok kullanılan açık anahtarlı şifreleme algoritmasını yayımladılar. Algoritmanın ismini kendi isimlerinin baş harflerinden oluşturmuşlardı: RSA. RSA'nın güvenliği de zor bir matematik problemine dayanır. Bu problem büyük sayıları çarpanlara ayırma problemidir.

1980'li ve 90'lı yıllarda kriptolojinin gelişimi ivme kazandı ve kriptoloji bir bilim olarak olgunlaştı. Sıradan insanların bilgi güvenliği ihtiyaçlarını karşılayan birçok uygulamanın bu yıllarda başladığını ve günümüzde de hızla yaygınlaştığını görüyoruz.

1980'li yılların sonlarında Koblitz ve Miller, şifrelemede ve sayısal imzalamada eliptik eğri üzerindeki ayrık logaritma probleminin kullanılabileceğini önerdiler. Eliptik eğri kriptosunda anahtar boyu diğer asimetrik kriptolarla karşılaştırıldığında son derece kısadır. Buna rağmen kripto camiası ilk yıllarda eliptik eğri kriptosunu şüpheyle karşıladı. Eliptik eğriler oldukça derin matematiksel objelerdi. Bu objeler üzerine kurulan kripto sistemlerin güvenliği hakkında hiç kimsenin tam bir fikri yoktu. Analizler zordu ve derin matematik bilgisi gerektiriyordu. Ancak yıllar ilerledikçe araştırmalar derinleşti. Yaklaşık yirmi yıllık yoğun kriptoanaliz çalışmalarına rağmen, şu ana kadar birkaç özel eliptik eğri dışında eliptik eğrilerin üzerindeki kriptonun zayıflığına dair bir sonuç bulunamadı. Dolayısıyla günümüzde eliptik eğri kriptosuna olan güven oldukça artmıştır.

1980'li yıllarda güvenli olduğuna inanılan DES, 90'lı yılların başında hızla itibar kaybetti. 1991'de Biham ve Shamir (RSA'nın S'si) tarafından yapılan diferansiyel atakla DES yara aldı. Atak pek pratik değildi ve uygulama için çok sayıda seçilmiş açık metin gerekiyordu. Asıl darbe iki yıl sonra Japonya'dan geldi. Mitsuri Matsui doğrusal kriptoanalizi keşfetti ve DES'in doğrusal atakla kırılabileceğini gösterdi. Hatta bir sene sonra pratik bir doğrusal atak düzenleyerek DES'i kırdı. Bu, literatürde DES'e uygulanmış ilk pratik ataktı.

Bütün bu gelişmeler artık DES'in şifreleme algoritması olarak ömrünü tamamladığını ve 2000'li yılların güvenlik ihtiyacını karşılamaktan uzak olduğunu gösteriyordu. NIST (National Institute of Standards and Technology-Ulusal Standartlar ve Teknoloji Enstitüsü) 1997'de yeni bir şifreleme standardı için yarışma başlattı. Yarışma 2001 yılında sonuçlandı. Rijmen ve Daemen adlı iki Belçikalı kriptoloğun tasarladığı Rijndael adlı algoritma AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standardı) adıyla yeni standart şifreleme algoritması olarak seçildi. Günümüzde AES bütün dünyada en yaygın kullanılan şifreleme algoritmalarından biridir.

**Kaynaklar**

Kahn, D., *The Codebreakers: The Story of Secret Writing*, Scribner, 1996.

Menezes, A.J., Oorschot, P.C. ve Vanston, S.A., *Handbook of Applied Cryptography*, CRC, NY, 1997.

http://www.bletchleypark.org.uk

http://www.enigmahistory.org/