kriptolojinin dönüm noktası

Enigma

Süleyman Sevinç

TÜBİTAK
POPÜLER BİLİM KİTAPLARI

Enigma

kriptolojinin dönüm noktası

Süleyman Sevinç

TÜBİTAK

POPÜLER BİLİM KİTAPLARI

TÜBİTAK Popüler Bilim Kitapları 311

Enigma - Kriptolojinin Dönüm Noktası
Süleyman Sevinç

TÜBİTAK Popüler Bilim Kitapları'nın seçimi ve değerlendirilmesi TÜBİTAK Popüler Bilim Kitapları Yayın Kurulu tarafından yapılmaktadır.

ISBN 978 - 975 - 403 - 504 - 9

1. Basım Ağustos 2009 (5000 adet)

Yayın Yönetmeni: Adnan Bahadır
Yayıma Hazırlayan: Mustafa M. Dağlı
Kapak Tasarımı: Ayşe Taydaş
Sayfa Düzeni: Fatma Onay
Basım İzleme: Yılmaz Özben

TÜBİTAK
Popüler Bilim Kitapları
Atatürk Bulvarı No: 221 Kavaklıdere 06100 Ankara
Tel: (312) 467 72 11 Faks: (312) 427 09 84
e-posta: kitap@tubitak.gov.tr
İnternet: kitap.tubitak.gov.tr

Sistem Ofset Basım Yayın Sanayi ve Ticaret Ltd. Şti.
Strazburg Caddesi No: 7/A Sıhhiye 06430 Ankara
Tel: (312) 229 18 81 Faks: (312) 229 63 97

Enigma

kriptolojinin dönüm noktası

Süleyman Sevinç

TÜBİTAK POPÜLER BİLİM KİTAPLARI

İçindekiler

Teşekkür

Bu kitabı yazmalı mıydım? Daha da doğrusu bu kitabı derlemeli miydim? Bu çalışma iyi bir nedene veya bir kişiye faydalı olabilir miydi? İyi birşeylerin gelişmesine katkıda bulunabilir miydi?

Bu düşünceler arasında gidip gelirken Homer [1] ve Herodot'u [2] hatırladım. O kitapların ve çevirilerinin kendi yaşamımı ve gelişimimi nasıl etkilediklerine baktım. Homer ve Herodot birilerini kendi yaşam süreleri sona erdikten binlerce yıl sonra bu kadar etkileyebileceklerini düşünmüşler miydi?

Enigma ve Enigma'nın şifrelerinin kırılması çalışmaları benim üzerimde Evliya Çelebi'nin Gemlik'e doğru denizi görmesi gibi bir etki yarattı. Bu etkiyi paylaşmak istedim. Bu çalışmayı yaparken fark ettim ki bir bilgiyi aktarmak binlerce yumurtayı sırtında taşımak gibi hassas bir iş. Mesajı taşırken açmak, anlaşılır hale getirmek ve sunmak; bunu yaparken de nesnelliğini tutarak, abartmadan yapmak. Türkçeye bu çalışmayı kazandırdığım için huzurluyum; umarım okuyanlar da öyle hissederler.

Bu çalışmanın oluşması ve şekillenmesi aşamasında pek çok insanın katkıları oldu; çoğu benim

konu hakkında uzun konuşmalarıma tahammül etmek durumunda kaldılar. Bazıları bunun da çok ötesine giderek eserin ortaya çıkması için destek ve yardım sağladılar.

Değerli arkadaşım Rıza Öcalır, çalışma süresince hem bir editör hem de bir teknik ressam gibi katkıda bulundu. Kendisine minnettarım. Sayın Prof. Dr. Gündüz Gedikoğlu, sayın Prof. Dr. Ahmet Çakır, sayın Prof. Dr. Yavuz Gündüzalp, sayın Prof. Dr. Ali Okatan, sayın Dr. Kürşat Özdilli ve diğer Haliç Üniversitesi personeline akademik çalışmalarımda göstermiş oldukları destekler için teşekkürlerimi sunarım.

Kitabın düzenlenmesi ve okunabilir hale getirilmesinde büyük katkılar sağlamış olan TÜBİTAK Popüler Bilim Kitapları yayın ekibine teşekkürlerimi sunarım. TÜBİTAK ve yayın ekibinin destekleri olmaksızın, bu kitapın dosyalarım arasında bir not olarak kalması kuvvetle muhtemeldi.

Av. Zafer Sevinç ve Tatiana Shibelkina'ya, bana verdikleri sonsuz destekten dolayı teşekkür ederim. Sevgili annem, Neslihan Sevinç ve sevgili babam Mustafa Sevinç'e yorulmadan verdikleri her türlü destek için çok teşekkür ederim.

Prof. Dr. Süleyman Sevinç

Enigma: Yasak Elma

Enigma, 1928-1945 yılları arasında, Alman ordularının birimleri arasında güvenli iletişimi sağlayan daktiloya benzer elektronik bir sisteme verilmiş isimdir (Şekil 1). Sistem, denizaltılar, gemiler, kara birlikleri, demiryolları, vs. gibi binlerce noktada kullanılmıştır. Güvenli olarak gönderilmesi gerekli olan bir ileti Enigma kullanılarak önce şifreleniyor, sonra da şifrelenmiş mesaj, alıcısına radyo, telgraf veya kurye aracılığı ile ulaştırılıyordu. İletinin alıcısı da yine Enigma makinesini kullanarak mesajı deşifreliyor, yani kodlanmamış düz metin haline getiriyordu. Aynı makinenin daha güvenli modelleri Hitler'in ve ordu komutan-

Şekil 1 3 Rotorlu Enigma Makinesi (Resim, www.ilord.com sitesinin sahibi olan Bob Lord'un izniyle kitapta kullanılmıştır)

larının haberleşmelerini sağlamak üzere de kullanılmıştır [3, 28].

Almanlar Birinci Dünya Savaşı'ndan, savaşta iletişim ve koordinasyonun değerini iyice kavrayarak çıkmışlardı. Birinci Dünya Savaşı'nda Avrupa, Atlantik ve Afrika'ya dağılmış birliklerin birbirleri ile olan iletişimleri genel olarak telgraf, radyo ve postalar yolu ile sağlanıyordu. Bu mesajların önemli kısmı şifresizdi veya kırılması oldukça kolay yöntem-

lerle şifrelenmişti. Düşman, Almanların planladıkları hareketleri daha Alman kuvvetleri hazırlıklarını bitiremeden haber alıyordu. Gönderilen mesajlardan Alman gemilerinin yerleri de kolayca belirlenebiliyordu. Sonuçta Almanya mağlup olmuş, aşağılanmış ve kendini Avrupa'dan dışlanmış hissetmişti. Bunu hazmedemeyen Almanlar, daha savaş bitmeden, ikincisine hazırlanmaya başlamışlardı bile.

Almanya ikinci savaşı doğru yapmaya kararlıydı. Almanya birincisinden aldığı dersle, ikinci savaşta ordusu, deniz ve hava kuvvetlerini evrensel ve güvenli bir iletişim sistemine geçirmek zorunluluğunu hissediyordu. Dünya savaşları geniş coğrafyalara yayılmış değişik niteliklere sahip kuvvetlerin beraber operasyon yapmalarını gerektiriyordu. İletişim sistemi hızlı ve güvenilir olmalıydı. Bu nedenlerle, Almanlar İkinci Dünya Savaşı için yürüttükleri özel çalışmaların içinde U-Boat denizaltılarının geliştirilmesi, havadan füze tabanlı bombalama sistemlerinin geliştirilmesi ve nükleer bombaların geliştirilmesi yanmda, en üst düzeyde gizli olan bir çalışmaya daha başlamışlardı. Bu çalışmanın amacı Alman ordusunun birimleri ve komuta kademesi arasındaki iletişim güvenliğinin tam olarak sağlanmasıydı.

Alman ordusu 1918 yılında tam da aradığı çözümü buldu. Bu; kitabımıza konu olan Enigma makinesi idi ve bir Alman mühendis olan A. Scherbius tarafından patent edilmişti. Enigma, ordu tarafın-

dan satın alma yoluyla edinildi. Enigma, elektronik olarak çalışan bir şifreleme makinesiydi. Bu makine elektronik olduğu için şifreleme işlemi ve deşifreleme işlemini otomatik olarak yapabiliyordu. Hızlıydı. Şifreleme otomatik olarak yapıldığı için insan hataları sıfıra indirilebilirdi. Makine yaklaşık 12 kg ağırlığındaydı ve 4.2V'luk bir pille çalışıyordu. Kolayca taşınabilir ve cephede bile sorunsuzca kullanılabilirdi. Ayrıca sistemin şifreleri önceki yöntemlerle kıyaslanmayacak kadar da güvenliydi.

Alman ordusu 1918 yılından sonra da Enigma'yı kendi kullanımları için daha da geliştirmeye devam etti. Yapılan ilavelerle sistem o kadar güvenli bir hale getirildi ki düz deneme / yanılma mantığıyla yapılacak bir teşebbüsle tek bir Enigma mesajını kırmak bile binlerce yıllık bir zaman gerektiriyordu. Alman ordusunun şifreleme makinelerine olan güveni tamdı.

Birinci Dünya Savaşı'nın sonunda Avrupa'da pek kimse yeni bir savaş çıkabileceğini düşünmüyordu. Oysa Polonya Almanya'nın niyetlerinden şüpheleniyordu. Alman komuta kademelerinin ve birliklerinin niyetlerini anlayabilmek için Polonyalılar bir iletişim dinleme istihbarat bürosu kurmuşlardı [4]. Bu büro, diğer görevlerin yanında, Alman birlikleri arasındaki mesajları elektronik yollarla ele geçiriyor ve böylece Alman hareketlerini yakından gözlemleyebiliyordu. En azından 1928 yılına kadar.

Alman ordusu Enigma'yı edindiği 1918 yılından beri teknik olarak Enigma'yı daha da mükemmelleştirme çalışmalarının yanında, böyle bir makinenin ordunun tüm birimleri tarafından kullanılmasını sağlayacak personelin yetiştirilmesi, eğitimi ve prosedürlerin oluşturulması konularında da yoğun çalışmalar yapıyordu. Ordunun tüm birimleri için yeterli makine, yedek parça üretilmesi işlemleri tamamlandı. 1928 yılında Enigma'yı devreye almak için her şey hazırdı.

Polonya istihbarat bürosu için 1928 iyi bir yıl değildi. Enigma'nın devreye alınması ile Alman mesaj trafiği birden şekil değiştirmişti. Gönderilen mesajların görünürde bir anlamı yoktu. Polonyalılar kısa sürede, yeni bir şifreleme sisteminin kullanıldığını anladılar. Ancak Polonya 1932 yılına kadar tek bir Enigma mesajını dahi deşifre edemediler.

Polonya 1939 yılına kadar Enigma hakkında, daha sonraki çalışmalarda İngilizler için oldukça önemli olacak olan bilgiler topladı. Enigma'nın iç bağlantıları çözüldü, hatta bir kopyası bile üretildi [4,5]. Fransızların da sağladığı bilgilerle Polonyalılar pek çok Enigma mesajının şifrelerini kırdılar. Hatta şifre kırıcısı olarak kullanılmak üzere elektronik bir makine dahi ürettiler. Ancak 1939'da Polonya'nın Almanya tarafından işgali bu çalışmaları durdurdu. İstihbarat bürosu Fransa'ya firar etti. Eldeki bilgiler Fransa ve İngiltere ile paylaşıldı. 1939'da Enigma şifrelerini kırma bayrağı İngilte-

re'ye teslim edildi. Enigma şifrelerinin kırılması ile ilgili olarak, kitabımızın da teknik olarak incelemeye aldığı kısım işte bu kısımdır. Yani 1939 ile 1945 yılları arasında İngiltere'de gerçekleştirilen şifre kırma çabaları diyebiliriz.

Gerçekten de Almanlar sonuçta, deneme yanılma yoluyla, kırılması imkânsız olan bir şifreleme teknolojisi geliştirdiler. Buna rağmen İngilizler yeterli sayıda Enigma mesajını çözmeyi başardılar. Enigma'nın çözümlenmesi çalışmalarının savaşın kaderi üzerinde en etkin faktörlerden birisi olduğu konusunda genel bir kanı mevcuttur [6]. Her halükârda çalışma tüm yönleri ile işbirliği ve insan iradesinin neler başarabileceğinin örnekleri ile doludur.

Enigma, zamanının en yaygın kullanılan şifreleme sistemi oldu. Savaş boyunca Almanlar yüz binden fazla Enigma ürettiler. Enigma'ya benim ilgim ise iki açıdan gerçekleşti. Birincisi, Enigma'nın ilk yaygın kullanılan elektronik şifreleme makinesi olması ve benim bu teknolojiye daha yakından bakmak istememdir. İkincisi ise Enigma etrafında gerçekleştirilen inanılmaz bir insan işbirliği ve çalışmasıdır. Bir aşamada Enigma şifrelerini kırabilmek için 12,000 İngilizin görev aldığı bilinmektedir. Alan Turing önderliğinde gerçekleştirilmiş bu çalışma muhteşem bir entellektüel enerjinin tek bir amaç için yoğunlaşmasının eşsiz bir örneğidir. İngilizler bilim adamları ve mühendislerine güvendiler, onlara sorumluluk verdiler ve bunun karşılığını aldılar.

Enigma üzerinde Türkçe bir kaynak oluşturmak istememin başlıca nedeni, konuyu objektif olarak ele alan bir katkıyı Türkçeye aktarmak istememdir. Şifreleme, istihbarat ve mühendislik alanlarında çalışanlar, sadece hobi olarak bu alanlara ilgi duyanlara, bilgisayarın temeli olarak adlandırılan bir cihazı merak edenlere veya sadece eğlenceli bir kitap okumak isteyen herkese yönelik olarak hazırladım bu kitabı. Buna rağmen teknik detayların kaybolmamasına özen gösterdim. Enigma'nın tarihsel tarafını da uzmanlık alanım dışında olduğu için tarihçilere bıraktım.

Kitaptaki örnekler Geoff Sullinav M3 Enigma (yazılım) simülatörleri kullanılarak gerçekleştirilmiştir [7].

Enigma projesi savaştan sonra elli yıldan fazla devlet sırrı olarak muamele gördü. Enigma şifrelerini kırmak üzere tasarlanmış hiçbir bilgi kamuoyuna duyurulmadı. Belki de bunda savaş sonrası İngiliz, Amerikan, Rus ve diğer milletlerin Enigma'ya benzer şifreleme cihazları oluşturmalarının etkisi vardır [8,9].

Enigma tarihin akışını değiştirmiş olan bir şifreleme makinesidir. Enigma'nın tasarımcısı Scherbius makinesinin gerçek başarısını göremedi; 1928 yılında bir araba kazası sonucu yaşamını yitirdi. Savaş boyunca iki yüz bin ile dört yüz bin arasında Alman Enigma mesajı deşifre edildi. Enigma mesajlarının kırılmasındaki bu başarının Atlantik'teki

Alman U-Boat denizaltılarının egemenliğine son verdiği ve savaşın kazanılmasında en önemli faktörlerden birisi olduğu konusunda genel bir kanı mevcuttur. Ne yazık ki projenin lideri Alan Turing'in katkılarının tanınması (askeri gizlilik nedeni ile!) onun yaşam süresince mümkün olamadı. Turing savaştan yedi yıl sonra İngiltere'de homoseksüellik suçundan tutuklandı. Kendisine iki yıl hapis ya da cinsel isteklerini bastıracak kimyasal hormon tedavisinden geçmesi cezası verildi. Bir süre hormon tedavisi gören Turing bu hormonların etkisi ile vücudunda oluşan değişiklikler nedeniyle, bunalıma girdi. 1954 yılında içine siyanür enjekte ettiği bir elmadan yiyerek intihar etti. Oldukça ironik olarak, Turing intiharını gerçekleştirmek için, içinde yaşadığı toplumun yaşamın başlangıcı inanışının simgesi olan elma ile intihar etmeyi seçmişti.

Faydah olacağı umudu ile...

Süleyman Sevinç
10 Şubat 2008
Ataşehir

I. Bölüm

Ayşe Tatile Çıksın

1974 yılının Ağustos ayının ortalarında dönemin dışişleri bakanı Turan Güneş, Kıbrıs'ın üç garantör ülkesinden birisi olan Yunanistan ile Kıbrıs konusunda bir uzlaşmaya varabilmek ve diğer garantör ülke olan İngiltere'nin desteğini alabilmek için Cenevre'deydi. Ancak bir uzlaşmadan ve İngiltere'nin desteğinden ümit kesilmişti. Şimdi, zaman geçirmeden ve haber Yunanistan'a sızıp gerekli tedbirler almamadan ikinci Kıbrıs askeri harekâtının başlaması gerekiyordu. Üstelik o sıralar Akdeniz'de bulunan Amerikan 6. Filosu da potansiyel bir tehlikeydi. Amerika'daki güçlü Yunan lobisi, Amerikan Başkanı'm müdahaleye ikna ede-

bilirdi. Bakanın, durumu Ankara'ya hızla iletmesi gerekiyordu. Bakan, zamanın başbakanı Bülent Ecevit ile bir telefon görüşmesinde[10] *Ayşe Tatile Çıksın* diyerek harekâtın acil başlaması gerektiğini Ankara'ya iletti. Gereklilikler hızla tamamlandı. Kısa bir süre sonra da Türk Silahlı Kuvvetleri Kıbrıs'a çıktı. Harekât hızla gerçekleştirildi. Yunanistan, ABD ve İngiltere; fiilen çıkarmaya müdahil olmadı ya da olacak zaman bulamadı.

"Ayşe Tatile Çıksın" türünden şifreleme şekli, bir cümlenin dildeki standart anlamının bir başka anlam yerine kullanılmasıdır (metafor). Örneğin "Büyük Beyaz Göründü" cümlesi de gerçekte radarda düşman gemilerinin göründüğü anlamında kullanılabilir. Bu şekilde kodlamalarla gerçekleştirilecek şifreleme sisteminde kullanılan metaforların sayıları artıkça bir şifreleme anahtar kitabına ihtiyaç olacağı açıktır. Şifreleme anahtar kitapçığında her bir metafor ve onun gerçek anlamının ne olabileceği açıklanmalıdır.

Bu durumda şifre anahtarlarını içeren kitapçığın dağıtımında ve kullanımında, güvenliğe ihtiyaç olacaktır. Şifre kitapçığı yöntemi, ilk kimler tarafından kullanıldığı bilinemese de, oldukça eski bir yöntemdir. Metaforik şifrelemeye ilaveten, şifre kitaplarını doğrudan şifreleme yaklaşımları içinde kullanabiliriz. Bu yöntemde şifre kitapçığı olarak herhangi bir kitap kullanılabilir. Örneğin şu anda okuduğunuz kitap seçtiğimiz şifre kitabı olsun.

Şifreleme için yapılması gereken önce düz metin mesajın yazılmasıdır. Ondan sonra bu mesajın her kelimesi şifre kitapçığında aranarak bulunur. Her kelimenin şifre kitapçığında kaçıncı sayfada olduğu, bulunduğu satır numarası ve soldan sağa olarak satırda kaçmcı kelime olduğu not edilir. Şifreleme işlemi için düz metindeki her kelime yerine elde edilen bu üç rakam (sayfa no, satır no, kelime no) virgüllerle ayrılmış olarak yazılır. Böylece şifreli metinde kelimeler yerine, birbirinden virgüllerle ayrılmış rakamlar görülür.

Bu türden şifrelemenin güvenliği şifre kitabı ele geçirildiğinde tamamen ortadan kalkmaktadır. Bu nedenle de artık yaygm olarak kullanılmamaktadır.

Anlamsal kodlama ile şifreleme, bilinen tarihte en geniş anlamını İkinci Dünya Savaşı'nda bulmuştur. Amerikan ordusu, yeryüzünde pek az kişinin bildiği Navajo kızılderililerin dillerini biraz da modern zamanlara uygun şekilde genişleterek şifreleme aracı olarak kullanmıştır [11]. Bu örnekte Navajo dili yeterli sayıda kişiye öğretilerek veya anadili Navajo olan yeterli sayıda kişi temin edilerek, bu kişiler çeşitli lokasyonlara dağıtılmış ve bu dilde iletişim sağlanarak hassas konularda iletişim güvenliği sağlanmıştır.

Bu yöntemlerden hiçbirisinin bir ordunun tüm birliklerinin güvenli bir şekilde iletişmesinde yeterli olmadığı ortadadır. Bugünkü askeri ya da sivil organizasyonların potansiyel olarak on binlerce

ünite olan büyüklükleri göz önüne alındığında, seçilecek yöntemin otomasyonunun mümkün olması ve insan hatalarını kompanze edebilecek matematiksel bir şifreleme güvenliğine de sahip olması gerekmekte olduğu açıkça görülebilir.

"Ayşe Tatile Çıksın" tarihe en ünlü Türk şifresi olarak böylece geçti. Oysa şifrelemeye Türkler olarak ilgimizin en az 1567 yılına kadar gittiği anlaşılmaktadır [12]. Bu yayında, şifrelemeye ulusal olarak ilk sistematik yaklaşımımız olarak tanımlayabileceğimiz ve Milli Emniyet Hizmeti tarafından 1928 yılında basılmış olan *Cryptographie* adlı bir yayımdan bahsedilmektedir. Bu yayımda Milli Emniyet Hizmeti tarafından değişik şifreleme yöntemlerinin tanıtıldığı ifade edilmektedir.

Şifreleme

Şifrelemenin tarihinin MÖ 200 yıllarına kadar gittiği anlaşılmaktadır [13]. Yunanlı matematikçi Polybius'a atfedilen yöntem her harfe bir rakam atanarak şifrelenmiş metnin ortaya çıkarılmasına dayanıyordu. Örneğin "ve" düz metni, v harfine 16, e harfine 75'in atandığını varsayarak "16 75" şeklinde kodlanabiliyordu. Ünlü Romalı lider Jülius Ceasar'ın da benzer bir "yerine koyma" yaklaşımı kullandığı rapor edilmektedir [14]. Buna göre Ceasar, yazdığı gizli metinleri generallerine şifreleyerek ulaştırıyordu. Kullanılan yöntem bugün hâlâ Ceasar Yöntemi olarak bilinmektedir ve oldukça

basittir. Buna göre "ve" düz metni, her harfin kendisinden 3 harf sonra gelen harfle yer değiştirmesi sonucu, "ağ" şeklini alıyordu. Yani "ve" düz metnine karşılık gelen şifreli metin "ağ" oluyordu. Bu şekilde bir harfin yerine bir başka harfin konmasıyla elde edilen şifreleme yöntemlerinden tarihsel açıdan önemli olanlarının bir özeti Stallings [18] Bölüm 2'de bulunabilir.

Takip eden iki bin yıl boyunca bilindiği kadarıyla şifrelemede pek fazla bir ilerleme olmadı. Kullanılan yöntemler basitti; genel olarak düz metindeki harfin yerine başka bir harfin veya o harf için seçilen bir sayının konması suretiyle şifreli metin elde ediliyordu. Ancak bu şekilde kodlanan şifreli metinler, elde edildikleri düz metinlerin istatistiksel özelliklerini de beraberlerinde taşımaktaydılar. Yukarıdaki örnekte "v" yerine "a" harfi konulduğunda, eğer düz metin içerisinde "v" harfinin kullanılma sıklığı yüzde bir (%1) ise, şifreli metinde de "a" harfine rastlanma olasılığı yüzde bir olmak durumunda idi (Türkçe harflerin kullanım sıklığı için bkz [30]).

Böylece bir dilde, örneğin Türkçe, harflerin kullanım sıklığı bilgisine sahip olan birisi, şifreli metindeki "a" harflerinin yaklaşık yüzde bir olduğunu sayma yolu ile belirleyerek "a" harfinin muhtemelen "v" harfi yerine kullanıldığını tahmin edebilmesi mümkün idi. Özellikle Birinci Dünya Savaşı sıralarında kullanılan "harf-yerine-harf" koyma şifreleme

yöntemleri sözünü ettiğimiz istatistiksel özelliklerin şifreli metne yansıması olasılığının azaltılması için tasarlanmışlardı. Bunun için kullanılan yöntemlerden bazıları harflerin tek tek şifrelenmesi yerine ikişerli veya üçerli gruplar halinde şifrelenmesi idi. Örneğin "SAKLAN" düz metninde "SAK", "BDR" ile yer değiştirirse ve "LAN" üçlüsü, "FMG" ile yer değiştirirse sonuçta ortaya çıkan şifreli metin "BDRFMG" olur. Görüldüğü gibi düz metindeki ilk "A" harfi "D" ile ikinci "A" harfi ise "M" ile kodlanmış olduğundan şifreli metinle düz metin arasındaki istatistiksel ilişki daha az görünür hale getirilmiştir. Kitabımızın konusu Enigma makinesi de şifrelerinin çözülmesini engellemek amacı ile bir gölgeleme yöntemi kullanmıştır. Buna göre, ileride detaylı olarak göreceğimiz gibi Enigma rotorlarının her dönüşü şifrelemede kullanılan "harf-yerine-harf" koyma alfabesinin değişmesini sağlıyor ve böylece şifrelerini daha güvenli hale getiriyordu. İlave olarak, uzun şifreli metinlerin, şifreleme alfabesini değiştirerek saklanan düz metin ve şifreli-metin arasındaki istatistiksel ilişkinin ortaya çıkmasına neden olabileceğinden dolayı Enigma metinlerinin 250 karakter uzunluğunu aşması Alman şifreleme uzmanları tarafından yasaklanmıştı.

Daha kompleks şifreleme yöntemleri hem matematiğin hem de elektronik bilgisayarların keşfedilmesi ile gerçekleşti. Elektronik bileşenlerdeki ilerlemenin sonucu olan veri şifreleme standartı

(DES) [29] ve benzeri şifreleme yöntemlerine, önemli olmaları nedeniyle ileride kısaca değinilecektir. Elektronik bilgisayarların yaygın kullanımları ise hem matematiksel hem de gerçeklenebilirlik açısından daha karmaşık ve çözülmesi güç şifreleme yöntemlerinin gelişmelerine yol verdi. Özellikle Fransız matematikçi Fermat(1601-1665) İsviçreli matematikçi Euler(1707-1783) tarafından yapılan çalışmalar ve Galois'nın (1811-1832) grup teorisi bu alandaki çalışmaların matematik alt yapısını oluşturdu.

Bin beş yüz yıldır Çinliler tarafından bilinen bir teorem olan ve "Çinli Kalan Teoremi (ÇKT)*" adıyla anılan bir teorem bugünün en önemli bazı şifreleme yöntemlerinin dayanağını teşkil etmektedir. Öte yandan Fermat "Fermat'm Küçük Teoremi (FKT)" adıyla bilinen ama sonuçları açısından oldukça büyük olan bir eşitlik önerdi. FKT, herhangi bir sayının bir asal** sayıya bölünmesi ile elde edi-

* ÇKT, en basit haliyle, iki asal (dipnot **) sayının çarpımından daha küçük olan tüm sayıların bu iki asal sayıya bölünmeleri halinde kalanların çifti olarak ifade edilmesi demektir. Örneğin 3 ve 5 asal sayılardır. Bu durumda 15'ten küçük tüm rakamlar 3 ve 5'e bölündüğünde farklı kalanlar verir. Örneğin 8 rakamı 3 ile bölündüğünde 2 kalanı verir, 5 ile bölündüğünde ise 3 kalanı verir. Böylece 8 rakamını 3 ve 5 asal sayılarına göre ifade edersek (2, 3) şeklinde ifade etmek mümkündür. 15'ten küçük başka hiçbir sayı bize bu iki kalanı vermez. Örneğin 9 için (0, 4), 10 için (1, 0), 11 için (2, 1) vs elde edilir. Çinlilerin bu yöntemle ordularındaki askerlerin sayılarını inanılmaz kısa sürelerde hesapladıkları söylenir.

** Asal sayı kendisi ve bir rakamı dışında hiçbir sayıya tam olarak bölünmesi mümkün olmayan sayılara verilen addır. 1,2,3,5,7,11,.. en küçük asal sayılardır.

len kalanının, yine aynı asal sayıya göre üstünün alınıp sonra yine o asal sayıya bölünmesi sonucunda ortaya çıkan kalanla aynı olduğunu ispatladı. Karmaşık görünen bu ifade aslında oldukça net ve kolaydır. *Örneğin 24 sayısını alalım.* Seçtiğimiz asal sayı da 5 olsun. 24 sayısı 5'e bölündüğünde kalan 4 olacaktır. Şimdi 4'ün 5'e göre üssünü alırsak (4 x 4 x 4 x 4 x 4 = 1024 olur), 1024'ün 5'e bölünmesi ve kalanının alınması bize başladığımız kalanı yani 4'ü verecektir.

Euler, Fermat'ın bu sonucunu genelledi (Euler Totient Fonksiyonu ETF)*. Euler ETF'ye ilave olarak modüler aritmetik (kalanlar aritmetiği) adıyla anılan ve sayılar teorisinin bir parçası olan alanda yaptığı çalışmalarla da kriptolojinin matematik alt yapısının oluşmasında önemli katkılarda bulundu.

Ancak bugün uygulanan ileri kriptolojinin mümkün olabilmesi için 20 yaşında bir düelloda yaşamını yitiren Galois'nın grup teorisini kurgulamasına ihtiyaç vardı [15,16]. Galois'nın çalışmaları, yaşamı süresince kabul görmemiş olsa da, matematiğin pek çok alanına ışık tutacak derinlik ve genişlikteydi. Galois'nın Grup Teorisi günümüzde en yaygın

* Euler Totient Fonksiyonu olarak bilinen bu sonuç, Fermat'ın sonucunu herhangi bir asal olmayan sayıyı da içine alacak şekilde genişletti. Buna göre herhangi bir sayı seçilebilir, bu sayıdan küçük ve bu sayı ile ortak böleni olmayan sayıların (göreceli asalların) adedi (ETF) belirlenerek Fermat'ın sonucunda kullanılan asal sayı yerine bu adedin kullanılması ve kalan hesaplanmasında da seçilmiş olan tamsayının alınması ile Fermat'ın sonucu genellenir.

kullanılan ve en güvenli olarak bilinen şifreleme yöntemlerinin kalbinde yatmaktadır.

Fermat ve Euler'in elde ettikleri matematik sonuçlara dayanan ilk şifreleme yöntemlerinin ortaya çıkışı dijital bilgisayarların yaygın kullanıma girmesi ile gerçekleşti [17, 18, 19]. Daha önceki dönemlerde şifrelemenin gizliliği, büyük ölçüde şifreleme yönteminin (algoritmasının) gizliliğine dayanıyordu. Böylece yöntemi keşfeden herkes potansiyel olarak şifreleri çözebilirdi. Fermat ve Euler'in elde ettiği sonuçlar ve sayı teorisinde [20] gerçekleştirilen diğer ilerlemeler ve dijital bilgisayarların yaygınlaşması ile kırılması bilinen matematiksel yaklaşımlarla pratik olarak mümkün olmayan şifreleme yöntemleri oluşturuldu [17, 18, 19, 20, 21, 22]. Modern yöntemlerde şifreleme, yöntemin gizliliğine değil, şifreleme anahtarının gizliliğine dayanmaktadır. Öyle ki şifreleme yöntemi genel olarak bilinse bile, kullanılan anahtarların sık değiştirilmesi ve tahmin edilmesinin güçlüğü ile günümüz şifreleme yöntemleri güvenliklerini neredeyse kırılamayacak şekilde sağlayabilmektedirler.

Bugünün şifreleme sistemleri dijital bilgisayarların kendilerine verdiği hesaplama gücünü etkin olarak kullanmaktadır. Genel yaklaşım, düz metinin önce bir sayıya çevrilmesi sonra da bu sayının matematiksel yöntemlerle manipüle edilerek ki genellikle bu şifrelenecek sayının bir anahtar vasıtası ile karıştırılması (scramble edilmesi) veya modüle

edilmesi demektir, alıcıya gönderilmesi ve alıcının da yine aynı yöntemle şifrelenmiş sayıyı önce orijinal haline getirmesi ve sonra da bundan düz metni elde etmesi ile sonlanır. Sonraki bölümde banka makinelerinde kullandığınız 4 haneli anahtarların şifrelenmesi konusunu inceleyeceğiz.

Böylece asal sayıların bazı özellikleri, matematikteki ilerlemelerle ortaya çıkan karmaşık şifreleme algoritmaları, elektronik bilgisayarların hesaplama gücü birleştirilerek kusursuz ve çözülmesi pratik olarak imkânsız olan şifreleme yöntemleri ortaya çıktı.* Tüm matematik alt yapının hazır olmasına rağmen, elektronik biliminin son yüzyılda gelişmesi sonucu modern şifreleme yaklaşımların türemesi ancak bin dokuz yüzlü yılların ortasından sonra mümkün olabildi.

Enigma, matematik alt yapı bakımından Ceasar şifreleme yönteminin izlerini taşımasına rağmen, elektronik açıdan şifrelemede bir dönüm noktası olmuştur. Enigma şifreleme işlemini elektronik olarak gerçekleştirmektedir. Daktiloya benzeyen yapısı ile Enigma şifreleme işleminin kendisi gerçekleştirilirken insanı aradan tamamen çıkarmıştır. Böylece insana bağlı şifreleme hataları en aza indirgenmiş, şifreleme kişisel bir maharet olmaktan, tekrarlanabilir, rutin ve elektronik bir işlem haline

* Çözülmesi pratik olarak imkânsız derken, çözümün teorik olarak mümkün olduğunu ancak çözümün elde edilmesi için gerekli olan işlem sayı ve süresinin pratik bir zamanda gerçekleştirilemeyecek olmasını kast ediyoruz.

getirilmiştir. Bu da Enigma'yı yaygın bir şekilde kullanılabilir bir hale getirmiştir. Elektroniğin gücü Enigma'nın şifreleme uzayını o zamanın hayal gücünün çok ötesinde genişletmiştir. Öyle ki, sadece deneme-yanılma yöntemi ile bir Enigma mesajının çözülmesi pratik açıdan imkânsızdır.

Enigma şifrelemenin elektronik alt yapı ile gerçekleştirilmesini sağlayan bir makine idi. Buna ilaveten, Alan Turing'in Enigma mesajlarını kırma çalışmalarının ilk modern bilgisayarların oluşmasında katkıda bulunduğu söylenir.* Hem matematik hem de elektronik açıdan gerçekten ilerlemiş kriptolojik sistemler 1970'li [21] yıllarda ortaya çıkmıştır.

Enigma'nın keşfedildiği tarihte elektronik bilgisayarlar mevcut değildi. Elektronik olmayan şifreleme yöntemleri çok sayıda noktanın birbiri ile güvenli şekilde iletişmesi için yeterli yöntemler değillerdir. Manüel yöntemler, çok sayıda noktanın birbiri ile iletişiminde lojistik sorunlara ve insan hatalarına karşı duyarlıdırlar. Birinci Dünya Savaşı'nda orduların kıtalar ve okyanuslara dağılmış binlerce merkezden birbirleri ile iletişim ve koordinasyonlarında ciddi sorunlar yaşanmıştı. Almanlar savaşın bitiminde ordularını evrensel ve güvenli bir iletişim yöntemine taşımaya kararlıydılar ve bu ko-

* Bunun nedeni modern bilgisayar kavramının oluşmasma Turing'in yaptığı katkılardır. Enigma ile elektroniğe yakınlaşan Turing'in matematik ile elektronik arasındaki bağlantıyı yapmış olabileceği düşünülmektedir.

nudaki arayışlarını neredeyse savaş bitmeden başlatmışlardı.

Binlerce noktanın birbiri ile iletişebilmesi için, iletilerin şifrelenmesi (düz metinden şifreli metine geçilmesi) ve deşifrelenmesi (tekrardan düz metin haline getirilmesi) kolaylaştırılmalıydı. İnsan hatalarının minimuma indirilmesi elektronik bir yöntem ile mümkün olabilirdi. Şifrelerin başkaları tarafından kırılması tercihen imkânsız veya çok zor olmalıydı. Tüm bunlar elektronik ve matematikte ciddi ilerlemeler gerektiren beklentilerdi. Ama Almanların aradığı çözüm yine bir Alman olan Arthur Scherbius tarafından 1918 yılında patentlenmiş ve hazır bir şekilde Alman ordusunun talebini bekliyordu.

Alman ordusunun Enigma'nın varlığını keşfetmesi fazla bir zaman almadı. Enigma'nın ordunun ihtiyaçlarına olan uygunluğu aşikârdı. Enigma tamamen elektronik bir makineydi. Kolayca taşınabilir ve cephede rahatlıkla kullanılabilirdi. Sadece deneme-yanılma yolu ile Enigma'nın şifrelerini kırmak pratik olarak imkânsızdı. Enigma her özelliği ile Alman ordusunun tam da aradığı çözümdü. Bu amaçla Alman Ordusu Enigma'yı sahiplenmek için Arthur Scherbius ile bir anlaşma yaptı.

Banka Şifrelerinizi Korumak

Ülkemizde pek çoğumuz bir ya da daha fazla banka kartı kullanmaktayız. Her birisi için bir şif-

remizin (anahtar) olması da oldukça yaygın bir durum. Üstelik internet ve telefon bankacılığı ve kullandığımız diğer internet hizmetlerinin de (örn. E-posta) tanıtıcı anahtarlarının olduğunu düşünürsek ortada bir hatırlama sorunu olması oldukça doğal. Kart emniyetini sağlamanın yanında, gerektiğinde bu tanıtıcı anahtarları hatırlamak ama aynı zamanda bu tanıtıcı anahtarların da güvenliğini sağlamak yasal olarak omuzlarımıza konmuş bir gereklilik. Bu tanıtıcı anahtarları herhangi bir şekilde yazmanın da oldukça riskli olduğu ortada. Çünkü, bu bilgi başkalarının eline geçerse sizin hesabınızı haberiniz bile olmadan boşaltmaları mümkün. Peki ama biz bu tanıtıcı anahtarları şifreleyerek yazsak nasıl olur? Böylece anahtara izinsiz ulaşan birisinin bu anahtarı deşifre etmeden kullanması mümkün olmaz.

Örneğin ATM kartınızın tanıtıcı anahtarı (şifresi) 4137 olsun. Bu rakamı yazarken sağa iki kaydırarak yazalım. Yani 3741 şeklinde yazalım. Kendimiz okurken de sola iki kaydırarak okuyalım. Böylece 4137 elde ederiz. Şimdi şifreli metni ele geçiren bir saldırgan bundan bir yarar sağlayamaz. Ancak eğer saldırgan kullandığımız yöntemi biliyorsa durum değişebilir. Saldırgan en fazla 4 denemede şifremizi kıracaktır.

Şifreleme yöntemimizi biraz daha değiştirelim. Düz metindeki her bir rakamın yerine o rakamı 9 rakamından çıkardığımızda elde ettiğimiz rakamı

koyalım. Yani 4137 anahtarını şifreli hali 5862 olur. Kendimiz bu anahtarı deşifre ederken yine aynı algoritmayı uygulayarak, yani her bir rakamın 9 ile olan farkını alarak orijinal anahtara geçebiliriz. Yani 4137. Harika!

Ancak bu durumda da yöntemimizi bilen saldırgan ilk denemesinde şifremizi kıracaktır.

Yöntemimizi istediğimiz kadar sofistike hale getirebiliriz. Saldırganın matematik anlayışını zorlayacak ve sonuçta çözümünü imkânsız kılacak matematik araçlar geliştirebiliriz. Şimdiye kadar her rakamın yerine kolayca hesaplanabilen bir başka rakam koyarak şifreleme çalışmamızı yaptık. Şimdi 4137'yi tüm rakamlarının birlikte ifade ettiği dört bin yüz otuz yedi sayısı olarak düşünelim. Kullanabileceğimiz şifreleme yöntemini de bu bakış açısı ile geliştirelim.

Kullanacağımız yöntemin kolayca hesaplanabilir olması gerektiğini düşünerek şifrelemede yalnızca toplama ve çıkarma işlemini kullanalım. Öncelikle 4137 sayısının üzerine seçeceğimiz herhangi bir rakamı ekleyelim. Seçilen rakam 63 olsun. Bunu 4137 ile toplayınca 4200 elde ederiz. Saldırganın işini daha da zorlaştırmak için bu sayıyı da 9999 sayısından çıkaralım. Kalan 5799 sayısı şifrelenmiş metnimiz olur. Bunu da bir kenara yazalım. Şimdi ATM makinesine gidince orijinal rakamı bulmak için ilk yapmamız gereken 9999'dan 5799 rakamını çıkarmaktır. Kalan 4200 olacaktır. Buradan da da-

ha önce seçtiğimiz 63 rakamını çıkarırsak orijinal anahtara ulaşmış oluruz. Burada 63 rakamı yerine TC kimlik numaranızın veya ehliyetinizin son iki ya da üç rakamını kullanarak hatırlama işleminizi kolaylaştırabilirsiniz.

Burada kullandığımız 63 sayısı ya da TC kimlik numaranızın son üç rakamına şifre anahtarı diyebiliriz. Artık saldırgan algoritmamızı bilse bile bu anahtarı bilmeden şifremizi kolayca kıramaz. Bu ilave bir emniyet getirir ama bu emniyet anahtarın tahmin edilebilirliği ile sınırlıdır. Burada orijinal anahtara **a** diyelim. Seçilen şifre anahtarına **p** diyelim, **y** de şifreli metnimiz olsun. Örneğin a = 4137, p = 63, y = 5799. Bu durumda;

9999 – (a + p) = 5700 yani a + p = 4200 olur. p seçilirken 3 rakam genişliğini aşmaması öngörüldüğünden p'nin en küçük değeri 0, en büyük değeri de 999 olabilir; buradan da muhtemel a ve p çözüm çiftlerinin sayısının 1000 olacağı anlaşılır. Banka sistemlerinin arka arkaya en fazla 3 yanlış denemeye izin verdiğini varsayarsak, saldırganın a'yı tahmin edebilmesi olasılığı 0.003 (binde üç - % 0,3) olur.

Pek Çok Nokta Arasında İletişimin Sağlanmasında Şifreleme

Yukarıda belirlenen metodların pek çoğu kıtalararası dağılmış olan bir ordunun şifreleme ihtiyaçlarını karşılayacak kadar sofistike değillerdir. Ön-

celikle yapılan hesaplamalar basit olmasına rağmen insan tarafından yapılmaları gerektiği için insan hatalarına duyarlıdırlar. İnsanlar hiç hata yapmasalar bile, seçilen şifrelerin sık sık değiştirilmeleri gerekmektedir. Aksi halde şifreyi bir kez ele geçiren herkes sonsuza dek tüm iletileri deşifre edebilir. Ayrıca kullanılan yöntemlerin daha da güçlendirilerek kırılması zor bir hale getirilmeleri gerekir. Buradaki varsayım ne kadar gizli tutulursa tutulsun, şifreleme algoritmasının muhakkak sonunda sızacağı ve herkes tarafından da bilineceğidir.

Yaygm olarak kullanılacak herhangi bir şifreleme yönteminin sağlaması gereken üç şarttan birincisi, kullanım kolaylığı olmasıdır. Şifreleme sistemi on binlerce noktada kullanılacağından kullanımı kolayca öğrenilebilmeli ve özel bir yetenek gerektirmemelidir. İkinci şart, yöntemin insan hatalarına yol açmayacak şekilde tasarlanmasıdır. İnsan hataları son derece ileri şifreleme yöntemlerini bile etkisiz hale getirebilir. Üçüncüsü ise şifreleme sisteminin kırılmasının ya çok zor ya da imkânsız olmasının sağlanmasıdır. Kolayca kırılabilecek şifreleme yöntemleri verinin güvenliğine doğal olarak zarar verecektir.

Enigma, yukarıdaki üç şartı da sağlamaktaydı. Elektronik yöntemlerle şifreleme gerçekleştirdiği için insan hataları azaltılabilirdi. Enigma etrafında Alman ordusu tarafından oluşturulan sistem günlük şifrelerin dağıtımı ve değişimini garanti ediyor-

du. Enigma'nın kriptolojik (şifreleme) sistemi, matematiksel olarak rastgele denemelerle kırılamayacak kadar güçlü bir karmaşıklık arz ediyordu. On kiloyu biraz aşan ağırlığı ile Enigma taşınabilirdi. Savaş ortamı için ideal olan bu makine; Nazilerin gizlilik için önde gelen çözümü olacak ve onların olağanüstü güvenini kazanacaktı. Ancak bu güven Nazilerin savaşı kaybetmelerinin de en önde gelen nedenlerinden birisi olacaktı [6].

II. Bölüm

Enigma

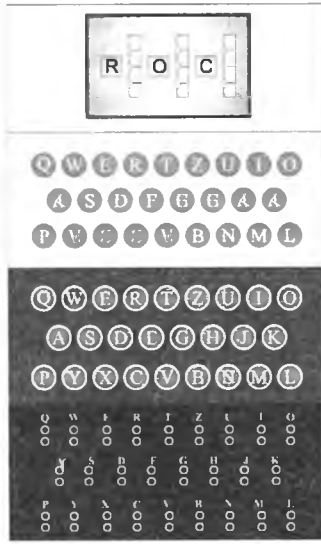
Enigma 12 kg ağırlığında daktiloya benzer bir cihaz şeklinde tasarlanmıştı ve dört bölümden oluşmaktaydı (Şekil 1 ve Şekil 2). Cihazın operatöre bakan ön yüzünde bir önbağlantı panosu (Steckerbrett veya Plugboard), operatöre yakın üst yüzünde klavye, klavyenin hemen üst kısmında lambalar ve lambaların üst tarafında ise rotorlar yer almaktaydı. Bunlardan klavye, düz veya şifrelenmiş metni girmeye yarıyordu. Klavyenin organizasyonu ile aynı şekilde dizilmiş olan lambalar düz metne ait harfler girildiğinde kısa bir süre için yanıp sönmek suretiyle şifrelenmiş harfleri gösteriyor, şifreli harfler girildiğinde ise

yanıp sönen lamba düz metin karşılıkları gösteriyordu.

Enigma normal olarak iki operatör tarafından kullanılıyordu. Bir operatör klavyeden metinleri girerken, diğer operatör ise yanıp sönen lambaları not alıyordu. Şifrelenen metinler telgraf, radyo veya kurye vasıtasıyla alıcısına ulaştırılıyordu. Enigma'nm şifreleme ve deşifreleme işlemi tamamen simetrik olarak tasarlanmıştı. Düz metni girince şifrelenmiş metin üretiliyor, gerekli ayarlamalar yapıldıktan sonra ise şifrelenmiş metnin girilmesi halinde düz metin çıkıyordu.

Şifreleme için düz metinde bulunan harflerin karşılığı olan klavye tuşlarına basılıyor, her harfin şifrelenmiş karşılığı olan lamba kısa bir süre yanıyordu. Elektronik olarak bu klavyenin basılan tuşu ile yanan lamba arasında bir kısa devre oluşturmuş olmaya karşı geliyordu. İkinci operatörün görevi yanan lambaları not almaktı. Şifrelenmiş metin ortaya çıkınca ileti gönderiliyordu. Şifrelenmiş bir metin ele ulaştığında ise Enigma makinesinde o gün için gerekli ayarlamalar yapılıyor ve düz metin girer gibi şifreli metin giriliyor ve yanıp sönen lambaların not edilmesi vasıtasıyla düz metin elde ediliyordu.

Enigma temelde bir "yerine koyma" şifreleme sistemiydi. Önceki bölümde Ceasar şifrelemesinden bahsetmiştik. Ceasar şifrelemesi alfabedeki her harfin yerine üç pozisyon ilerideki harfin konulma-



Şekil 2 Enigma modülleri ve bağlantıları

sı işlemiydi. Enigma Ceasar şifresinden farklı olduğu iki nokta; Enigma'da yerine koyma işleminin daha karmaşık ve elektronik olmasıdır. Yerine koyma işlemi, Enigma'da seri halde takılan rotorlarla sağlanmakta ve her harfin yerine konacak olan harf rotor [23] bağlantıları ile seçilmektedir.

Örneğin Rotor I olarak adlandırılan ve 1930'da kullanıma giren rotorun "yerine koyma" bağlantıları;

ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ

Burada Rotor I in A->E, B->K, C->M, vs (üst satır giriş harfi, alt satır çıkış harfi) şeklinde girişine uygulanan harfin yerine yukarıdaki tabloda gösterilen şekilde çıkış harfini koymaktaydı.

Enigma'da rotorlar bu bağlantıları elektriksel olarak gerçekleştiriyordu. Her rotorun giriş uçları ile çıkış uçlarını birbirine kablolar ile bağlanmaktaydı (Şekil 3). Şekil 3'te rotorun görüntüsü, şekli sadeleştirmek için biraz değiştirilmiştir. Buna göre dış dairedeki harfler rotorun giriş yönünü, iç dairedeki harfler rotorun çıkış yönünü göstermektedir. Gerçek rotorda giriş ve çıkış harf sıralamaları aynı olduğu halde, şekilde giriş yönündeki A'nın altına E, B'nin altına K, ... yerleştirilmiştir. Bu A girişinin çıkışa E olarak, B girişinin K olarak, vs yansıtıldığını göstermek için yapılmıştır. Böylece karmaşık bağlantı çizgileri daha basit olarak ifade edilebilmiştir. Gerçek rotorda çıkıştaki E, girişteki E harfinin tam karşısına düşmektedir. A'nın E'ye bağlanması ise iki harfin birbirine kısa devre edilmesi ile gerçekleştirilmektedir.

Enigma 3 veya 4 rotorlu modeller olarak üretilmiştir. Biz burada sadece 3 rotorlu Enigma ile ilgileneceğiz. 3 rotorlu Enigma'da, rotorlar arası elektriksel giriş çıkış bağlantıları birbirlerine sürten esnek fırça tellerle veya alttan bir yayla beslenmiş ucu yuvarlak bir yuvaya oturabilen bağlantı türleri ile yapılmıştı. Bu bağlantı türü rotorların birbirinden bağımsız olarak dönebilmelerini sağlamak içindi.

Şekil 3 Enigma rotor elektrik bağlantıları

Şekil 4 Rotorun dönüşü ve testere diş

Klavyedeki her tuş bakır bir kablo ile ilk rotorun girişine bağlanmıştı. Bu bağlantı A->A, B->B, vs. şeklindeydi ancak klavye tuşlarına her dokunuşta rotor pozisyonu bir kez ilerletildiğinden, klavyeden sürekli olarak A'ya basılması halinde bile çıkışta farklı farklı harfler okunmaktaydı (Şekil 4).

Bu durumda yukarıdaki örnekte belirtilen Rotor I'in girişine V harfini uyguladığımızda, önce bir pozisyon dönerek

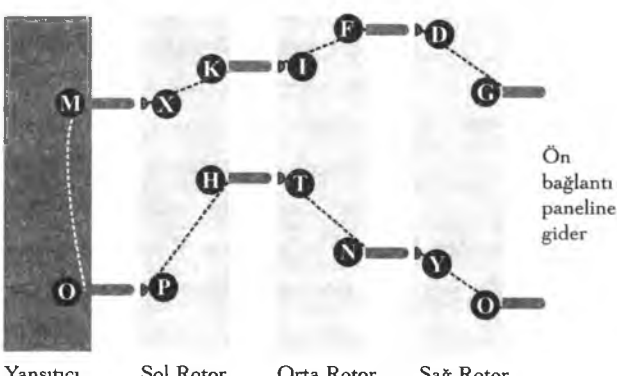
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KMFLGDQVZNTOWYHXUSPAIBRCJE

Durumuna geliyor ve arkasından **B** harfini şifre olarak üretiyordu. Şimdi E harfini girince bir dönüş daha Rotorun durumunu,

ABCDEFGHIJKLMNOPQRSTUVWXYZ
MFLGDQVZNTOWYHXUSPAIBRCJEK

şekline getiriyor ve ardından E'ye karşılık D harfini üretiyordu. Böylece yukarıdaki durumda başlayan Rotor VE düz metnini BD olarak çıkışına gönderiyordu. Rotorun çıkışından gelen elektrik sinyalleri bir düzenek vasıtası ile karşı gelen harflere ait lambaları yakıyordu. Bu son durumda önce B sonra da D lambaları kısa bir süre için yanıp sönüyordu.

Klavye tuşlarının temel görevi önce rotoru bir pozisyon ilerletmek ve ardından 4V'luk bir pil kul-

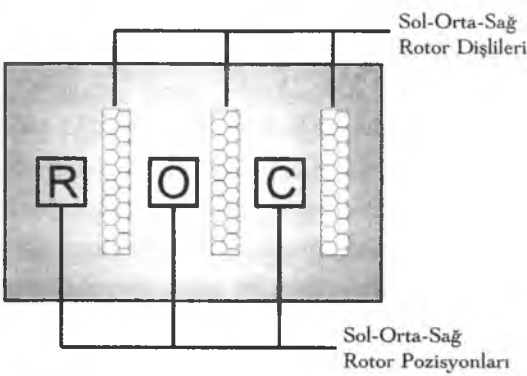


Şekil 5 Klavye ve ön-panelden rotorlara bağlantı.

lanarak basılan tuşu birinci rotorun karşı gelen girişine kısa devre etmekti (Şekil 5).

Enigma'nm pek çok modelinde arka arkaya bağlanmış 3 rotor bulunmaktaydı. Bazı modellerde savaşın sonuna doğru rotor sayısı dörde çıkarılmıştır.

Arka arkaya seri bağlanan motorlar birbirlerinin dönmesini de tetikliyordu. Birinci rotor tam bir dönüş yaptığında ikinci rotorun tek bir dönüşünü tetikliyordu (bir takometre düzeneğinin çalıştığı gibi). Birinci rotorun hangi pozisyonda ikinci rotorun dönüşünü tetikleyeceği, değiştirilebilir şekilde ayarlanmıştı. Bu da üzerinde çentik bulunan bir halkanın uygun noktaya ayarlanmasıyla gerçekleştiriliyordu. Örneğin Rotor I, Q pozisyonunda orta rotorun dönüşünü tetiklemek üzere ayarlanmıştı. Çentik pozisyonları değiştirilebilir olmasına rağmen, savaş boyunca sabit bırakılmışlardır.



Şekil 6 Pencere pozisyonu

Enigma'nın rotor bölümünün üstünde küçük bir pencere bırakılmıştı. Bu pencere rotorların en üstünde yer alan harfleri gösteriyordu (Şekil 6). Buradan görünen harflere pencere pozisyonu diyeceğiz.

Pencere pozisyonu, rotorların her biri döndükçe değişiyordu. En hızlı değişen pozisyon en sağdaki rotora ait olan pozisyondu. Sağ rotorun her 26 dönüşü orta rotorda tek bir dönüşe neden oluyordu. Sol rotorda, orta rotora bağlı olarak, orta rotorun her bir turu için tek bir dönüş yapıyordu. Örneğin; AAA,AAB,AAC,....,AAY,AAZ,ABA,.... Pencere pozisyonu operatör tarafından da, her rotorun pencereden dışarı taşan kısmı vasıtası ile manuel olarak değiştirilebiliyordu.

Böylece üç-rotorlu bir Enigma'da, her rotorda 26 değişik pozisyon olduğu için 26 x 26 x 26 yani 17,576 değişik pencere pozisyonu bulunmaktaydı.*

Her pencere pozisyonunda klavyedeki tuşların şifreli karşılıkları değişiyordu. Örneğin pencere pozisyonu AAA iken, A->K, B->F, ... olabiliyor, pencere pozisyonu AAB iken A->S, B->O, ... olabiliyordu. Enigma'nın simetrik yapısı bir harfin kendine şifrelenmesini yasaklıyordu. Yani her pencere pozisyonu için alfabenin 13 çifti birbirine bağlanıyordu. Her pozisyondaki bu harf çiftlemelerinden

* Enigma'nın rotorlarının dönüşü için kulandığı çentik mekanizmazı nedeniyle bu *17,576* mümkün pozisyondan *sadece 16,900 tanesi* kullanılabilmekteydi. Bunun nedeni orta rotorun çentik pozisyonunda kalamamasıydı (Bkz. Referans 28).

doğal olarak pencere pozisyonlarının sayısı kadar olabilir. Bu da belirli bir rotor seti ve sırası için yukarıda da görüldüğü gibi 17,576'dır.

Aslında teorik olarak 26 harfin bu şekilde birbirine kodlanabilmesi olasılığı çok daha fazladır. Ancak Enigma pratik nedenlerle sadece 5 rotora* sahipti ve kullanım için her gün bu rotorlardan sadece üç tanesi seçiliyordu. Çok daha fazla sayıda rotorun imal edilmesi mümkün olsa da savaş şartlarında taşınabilirlik önemliydi. Bu nedenle rotor sayısının sınırlı tutulması gerekmişti.

Üç rotorun arka arkaya (cascade) bağlanabilmesi Enigma'nın kriptolojik gücünü artırabilmek içindi. Böylece şifreli metinde ortaya çıkması olası düzenliliklerin (patterns) en aza indirilmesi planlanmıştı.

En soldaki rotorun sol tarafında sabit bir yansıtıcı (Umkehrwalze) bulunmaktaydı. Bu yansıtıcının görevi en soldaki rotorun çıkışını tekrardan kendisine (ama bu sefer çıkışından girişine doğru) uygulamaktı. Burada önemli olan nokta yansıtıcının 13 bağlantısının hiçbirisinin bir harfi kendisine, örneğin A -> A, bağlamasına izin verememesidir. Yansıtıcının bu şekilde tasarlanması sonucu klavyeden belli bir harfe basıldığında, (örn. V) Enigma'nın bu harfi şifrelediği, örneğin B, harfine üzerinden elektrik akımının geçebileceği bir elektrik devresi yaratması ve bu devrenin B ile işaretli

* Bu sayı savaşın ilerleyen yıllarında artarak 8'e ulaşmıştır.

lambaya kadar uzanarak B lambasının yanmasına olanak sağlamasıydı. Yani B ile V birbirine kısa devre ile bağlanmıştı. Böylece aynı pencere pozisyonunda B harfi girildiğinde de V harfi ile işaretli lambanın yanması sağlanmıştı. Bu da Enigma'nın şifreleme ve deşifrelemesinin tamamen simetrik olmasını sağlıyor, aynı pencere pozisyonunda düz metin harfi girilirse şifreli harf lambasının, şifreli harf girilirse düz metin lambasını yanması sağlanıyordu.

Şifreleme ve deşifreleme işlemi için belli bir pencere pozisyonu başlangıç pozisyonu olarak seçilmeliydi. Şifrelemenin başladığı bu pencere pozisyonu aslında mesaj anahtarı olarak düşünülmüştü. Deşifreleme için de Enigma'nın pencere pozisyonunun şifrelemede kullanılan mesaj anahtarına aynen ayarlanması gerekiyordu. Bu pozisyonda düz metnin harfleri şifreli metnin harfleri ile kısa devre olduğundan, düz metnin girilmesi şifreli metni üretiyor; şifreli metnin girilmesi ise düz metni üretiyordu.

Rotorların el ile kolayca takılıp çıkarılabilmesi sağlanmıştı. Enigma üç rotor alabilmesine karşın bu üç rotorun içinden seçilebileceği 5 tane rotor mevcuttu. Böylece Enigma'ya takılacak üç rotorun var olan 5 rotorun içinden seçilmesini gerektiriyordu. Şifreleme ve deşifreleme işleminin başarılı olması için gönderen ve alan makinelerde aynı rotorların aynı sırayla takılı olması gereki-

yordu. 5 rotorun içinden herhangi üç rotorun seçilmesi ve seçilen üç rotorun mümkün sıralamaları hesaplandığında 60 değişik olasılığın olduğu görülür. Bu da Enigma'nın karmaşıklığını artırıcı bir etkendi. Daha çok rotor, çözülmesi daha zor şifre demekti ancak savaş koşullarında operatörlerin yanında taşıyabilecekleri rotor sayısı da sınırlı olmalıydı. Bu nedenle Enigma rotorlarının sayısı hep sınırlı kaldı.

Şu ana kadar gözlemlerimizden şifreleme işlemi için;

1. Enigma rotorlarından üç tanesinin seçilmesi
2. Çentik (Notch) pozisyonlarının her bir rotor için ayarlanması
3. Bu rotorların belirlenen sırada cihaza takılması
4. Pencereden görülecek harflerin her bir rotor için el ile ayarlanması
5. Şifrelenecek metnin yazılarak, yanan sönen lambaların not edilmesi
6. Şifreli mesajın alıcıya iletilmesi

Deşifreleme işlemi için ise ilk 4 adımın aynı şekilde uygulanması gerekmekteydi. 5. adım ise şifrelenmiş metnin Enigma'ya klavye vasıtası ile girilmesiydi. Yanan sönen lambaların not edilmesi düz metni vermekteydi.

Alman ordusu Enigma gibi bir şifreleme makinesinin kullanılmasının bazı prosedürlere bağlanması-

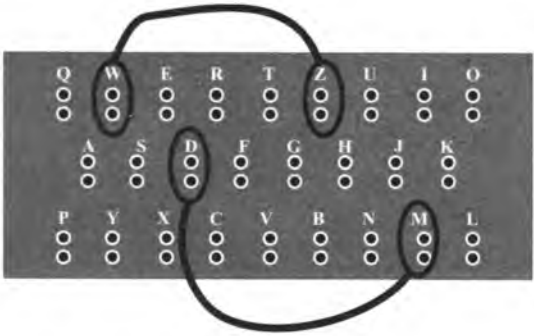
nın gerekliliğini biliyordu. Her gün için seçilmiş olan rotorlar, rotorların sıraları, günün pencere pozisyonu, çentik pozisyonları bültenler halinde basılıyor ve aylık olarak birliklere gizlice dağıtılıyordu. Değişiklikler günün belirli bir saatinde (örn. sabah 5) gerçekleştiriliyor ve uygulamaya geçiliyordu. Bu işlem her gün tekrarlanıyordu.

Ön-Bağlantı Paneli

Ön bağlantı paneli Enigma'yı kırılması daha zor bir hale getirmek için gerçekleştirilmişti (Bkz Ek 1). Ön bağlantı her harfin Enigma rotor sistemine girmeden önce bir başka harfe bağlanabilecek şekildeki bir düzenekten ibaretti (Şekil 7). Bunun için 10 adet kablo sağlanmıştı (26 harf için en fazla 13 adet kablo kullanılabilirdi).

Örneğin ön-bağlantı paneli ile W harfinin Z harfine bağlandığını varsayalım. Operatör W harfine basınca ön bağlantı paneli sağ rotora Z harfini bağlıyordu. Enigma rotorları bu pozisyonda Z harfini D harfine dönüştürsün varsayalım. Bu sefer de D harfi sağ rotor çıkışından ön-bağlantı paneline bağlanıyor, buradan da ön-bağlantı paneline eklenmiş olan kablo vasıtası ile M'ye aktarılıyor ve sonuç olarak yanan lamba M oluyordu.

Ön-bağlantı paneli Enigma'nın ürettiği şifrelerin kırılması işleminin sadece rastgele kombinasyonlar seçilerek yapılabilmesini pratik olarak imkânsız bir hale getirmiştir.



Şekil 7 Ön-bağlantı paneli

Şifreleme ve deşifreleme işlemleri için alıcı ve gönderici makinelerin aynı ön bağlantıları gerçekleştirmesi gerkmekteydi. Bu nedenle, aylık Enigma bültenlerinde hergün için geçerli olan ön-bağlantı listesi de yer almaktaydı. Böylece Enigma operatörleri hergün ilk iş olarak günün ön bağlantılarını gerçekleştirmek, belirlenen rotorları seçmek ve belirlenen sırada Enigma'ya takmak, çentik pozisyonlarının doğru olduğundan emin olmak (gerçekte çentik pozisyonlarının her rotor için sabit tutulduğu anlaşılmaktadır) durumundaydılar.

Enigma Kullanım Prosedürleri

Alman ordusu Enigma için bir kullanım prosedürü geliştirmişti [25]. Aylık listeler halinde, her gün için ön-bağlantılar, seçilecek rotor numaraları, rotor sıralaması ve bir de günlük anahtar anlamına gelen pencere pozisyonu gizlice tüm birliklere ulaş-

tırılıyordu. Tüm bu ayarların aynı şekilde yapıldığı Enigmalar birbirleri ile konuşabiliyorlardı.

Almanlar bu günlük değişkenleri kullanarak birden fazla Enigma ağı oluşturmuşlardı. Her ağ için farklı günlük ayarlar farklı noktalara ulaştırılıyordu. Ordu komutanları ve Hitler arasında da özel bir ağ oluşturulmuştu. Böylece daha duyarlı iletişim ağlarının günlük ayarları daha sınırlı sayıda iletişim noktalarına daha güvenli bir şekilde ulaştırılıyordu.

Deniz Kuvvetleri kendine özgü ve daha güvenli prosedürler kullanıyordu. Savaşın sonuna doğru Deniz Kuvvetleri 4 rotorlu Enigma'ya geçişi ve rotor havuzunda bulunan rotor sayısının da 8'e çıkarılmasını gerçekleştirdi. Kullanım prosedürleri de Deniz Kuvvetleri'nde daha farklı ve genel olarak insan hatalarını daha aza indirecek şekilde planlanmıştı*.

Tipik bir Enigma mesajı şöyleydi**.

SSM 27/03/2008 08:12 121 52 WSG
DBSC ALXJ NCBK QEAZ UELZ GRQF
WVTL XVOY VSVP BGQH QKEU SLVM
ENGC

* Konumuz Enigma'nın tarihsel boyutu olmadığı için kullanılan bu prosedürlerin detaylarına girmiyoruz. Deniz Kuvvetleri günlük anahtarlara ilave olarak her mesaj için seçilen mesaj anahtarlarının belirlenmesinde insan hatalarını azaltacak ve mesaj anahtarlarının daha tesadüfi seçilmiş olmalarını sağlayacak detaylı prosedürler geliştirmişti

** Mesaj Geoff Sullivan, The M3 Enigma Simulator, kullanılarak üretilmiştir. Mesaj anahtarı GYQ, rotor bağlantıları B IV II V, ringstellung KFA. Ön-bağlantı kablosu kullanılmamıştır.

Mesajda baş kısımda şifrelenmemiş bölümler yer almaktadır. Bunlar sırayla gönderen istasyonun kodu, mesaj tarihi ve zamanı, sıra numarası ve mesaj uzunluğudur. WSG mesaj anahtarının günlük anahtar kullanılarak kodlanmış şeklidir. Burada günlük anahtar olarak JWV alınmıştır. Bu pozisyonda mesaj anahtarı olarak kullanılan GYQ kodlandığında WSG elde edilmiştir. Şifreli mesaj kısmı ise dörtlük harf grupları şeklinde aralarında birer boşluk olacak şekilde yerleştirilmiştir.

Yukarıdaki Enigma mesajının orijinal düz metin karşılığı şudur;

ISTA NBUL XBOG AZIN DAXH AVAX
LODO SXGU NESL IXRU ZGAR XHAF IFXX

Bu mesaj düz metin olarak yazıldığında ISTANBUL BOGAZINDA HAVA LODOS GUNESLI RUZGAR HAFIF şeklinde olduğu görülür.

Enigma operatörleri bir eğitimden geçerek mesaj anahtarı seçimi ve diğer kullanım prosedürleri hakkında eğitiliyorlardı. Örneğin aynı anahtarı iki kez üst üste seçmemeleri, ABC (harf sırası), QWE (klavye sırası), AAA (aynı harfin tekrarı) gibi anahtarların seçilmemesi gerekiyordu. Ancak öyle anlaşılıyor ki bazı operatörler bu uyarıların tersine davranıyorlardı. Bunlar da Alman mesajlarını çözmeye uğraşan İngilizlerin işlerini kolaylaştırıyordu [24].

Alman Enigma kullanım prosedürlerinde yer alıyor mu tam olarak bilemiyorum ancak Almanların bazı mesajları, yanlışlıkla da olsa iki farklı anahtarla göndermeleri, mesajların başında ve sonunda standart hitaplar, örneğin Heil Hitler, kullanmaları, her gün belirli saatlerde belirli mesajları göndermeleri, örneğin hava raporları, bazı operatörlerin kız arkadaşlarına sürekli ve tahmin edilebilir mesajlar göndermeleri Alman Enigma şifrelerinin kırılmasını kolaylaştırmıştır. Aslında daha sonra göreceğimiz gibi, mesaj içeriğinin bir bölümünün tahmin edilebilmesi Alman mesajlarının çözümlenmesinin ana yöntemi haline gelmiştir.

III. Bölüm

Şifrelerin Kırılmasına Doğru

Enigma şifreleri müttefik güçlerin ilgi alanına girmekteydi. Bunu anlamak mümkündü. Çünkü, şifrelerin çözülmesi demek, müttefikler için Almanların ne düşündüklerini ve ne yapacaklarını anlamak demekti. 1939 yılına kadar Enigma şifrelerinin kırılmasında gerçekten yol almış tek ulus Polonya idi. 1939'da Polonya'nın Almanya tarafından işgali Polonyalıların çalışmalarını müttefiklerle paylaşmalarını sağladı.

1928 ve 1939 arasında Polonyalıların gerçekleştirdikleri çalışmaların sonucu olarak Enigma'nın rotor bağlantıları ortaya çıkarılmıştı [5].

Daha önceki bölümde not edildiği gibi Enigma'nm toplam 17,576 başlangıç pozisyonu bulunmaktaydı. Enigma operatörleri şifreleme işlemi için, hergün değiştirilmek üzere 5 değişik rotordan üçünü, belirlenen bir sırada makinelerine takıyorlardı. Bu da 60 değişik kombinasyon anlamına geliyordu (5 x 4 x 3).

Polonyalılar başlangıçta günlük şifrelerin, mesajın baş kısmında bulunan mesaj şifrelerini kodlamakta kullanıldığını fark ettiler. Her mesaj için Enigma operatörü keyfi bir anahtar seçiyor ve bu anahtarı günlük anahtarı kullanarak iki kez kodluyor ve bu kodları da yine mesajın baş kısmına yerleştiriyordu. Mesajın devamı ise keyfi olarak seçilmiş olan bu mesaj anahtarı ile kodlanan şifreli metni içeriyordu.

Polonyalıların yaklaşımı keyfi olarak her mesaj için seçilen mesaj anahtarlarından günlük anahtarı çözmek ve buradan da o günün tüm mesajlarını çözmek olmuştu. Mesaj anahtarının keyfi seçilmesi ve iki kez tekrarlanması Polonyahların işlerini kolaylaştırıyordu. Enigma mesaj anahtarı seçme prosedürü Alman ordusu tarafından dikkatle dökümante edilmişti. 3 harfli tüm mesaj anahtarı kombinasyonların yer aldığı bir kitap bile basılmış ve operatörlere dağıtılmıştı. Ancak bazı Enigma operatörleri keyfi olarak belirledikleri mesajları seçerken pek dikkatli davranmıyordu. AAA veya QWE gibi klavyede yan yana olan ya da alfabede yan ya-

na olan harflerin seçilmesi, operatörün kız arkadaşının veya kendisinin isminin ilk üç harfini seçmesi vb. gibi.

Polonyalıların Enigma operatörlerinin bu açıklarından da yararlanarak 1939 öncesi önemli miktarda Alman mesajını çözdükleri anlaşılmaktadır [4]. Hatta mesaj anahtarı ve günlük anahtar çözme işleminde kullanılmak üzere Bomba diye adlandırılan bir makine dahi üretilmişti. Bu makine otomatik olarak günlük anahtar ve mesaj anahtarı kombinasyonlarını karşılaştırarak aramak ve uygun durumları belirlemek üzere tasarlanmıştı. Ancak Bomba tamamlandıktan kısa bir süre sonra Polonya işgal edildi ve Bomba gerçekten kullanıma alınamadı.

Savaş başladıktan sonra Almanların bazı prosedürleri zaman zaman değiştirdiği de anlaşılmaktadır. Örneğin mesaj güvenliğini tehlikeye sokan mesaj şifre anahtarının günlük anahtarla iki kez kodlanması pratiği ortadan kaldırılmış, bunun yerine mesaj anahtarı sadece bir kez kodlanmıştır.

İngilizlerin Çalışmaları

1939 sonrası Polonyalılar ellerindeki bilgileri İngiliz ve Fransızlarla paylaştılar. Polonyalılar Fransızlarla beraber yürüttükleri şifre kırma çalışmalarını bir süre daha yürüttüler. İngilizler, Polonyalılardan Enigma hakkında tüm bilgileri aldıktan sonra, kendi bağımsız çalışmalarını başlat-

tılar. Çalışmalar, sonradan bilgisayar mühendisliği alanının kurucularından olarak anılacak matematik profesörü Alan Turing liderliğinde yürütülmekteydi.

Polonyalıların önceki çalışmaları hakkında çok detaylı bilgiler elimde olmadığından daha sonra Fransızlarla birlikte olan çalışmaları da dahil olmak üzere, Enigma şifrelerini kırmak konusunda ne kadar ileri gittiklerini tahmin edemiyorum. İngilizlerin çalışmaları hakkında ise daha fazla bilgi bulunmaktadır [3,24,26].

Aslında çıplak Enigma mesajlarını (ön-bağlantı paneli olmaksızın oluşturulan mesajlar) kırmak zor değildi. Müttefikler Enigma ve rotorlarını ele geçirmişlerdi. Herhangi bir Enigma mesajı mümkün olan 17,576 anahtardan herhangi birisiyle şifrelenmek durumundaydı. Dolayısıyla elinde 17,576 Enigma olan herhangi birisi bu mesajları çözebilirdi. Yapılması gereken her bir Enigma'nın farklı bir şifre anahtarı için başlangıç durumuna getirilerek şifreli metnin girilmesi, ortaya çıkan düz metinlerden anlamlı olanın seçilmesi idi. Bu işlem mümkün olan 60 rotor sıralaması için tekrarlandığında denenmemiş şifre anahtarı kalmayacak ve mesajlar çözümlenebilecekti.Yeterli hızda elektronik bir makinenin tasarlanabilmesi halinde ise, örneğin Bombe [3,26], bu kırma işlemi tüm mümkün şifreleri birer birer deneyerek de (deneme-yanılma) yapılabilirdi.

Ancak Almanlar boş durmuyorlardı. 1940 yılının Nisan ayında Steckerbrett'i (Ön-bağlantı Panosu) devreye aldılar. Böylece Enigma şifrelerinin tüm olasılıklarının denenmesi yolu ile çözülmesinin önü sonsuza dek tıkanmış oldu. Ön bağlantı panelinin devreye alınması ile birlikte toplam denenmesi gereken kombinasyon sayısı elektronik makinelerin bile deneyebileceği boyutların çok ötesine ulaştı. Her olasılığın denemesi ve böylece tek bir mesajın deşifrelenerek sonuca varılması için binlerce yıl çalışmak gerekiyordu. Açıkçası deneme-yanılma bir seçenek olmaktan tamamen çıkmıştı.

Günlük anahtarla mesaj anahtarı arasında bir ilişki kurarak şifrelerin çözülmesinin de Almanlar tarafından küçük prosedür değişiklikleri ile önü tıkandı. Öncelikle, mesaj şifresinin iki kez tekrarlanması işlemine son verildi.

Düz Metin Saldırıları

Müttefiklerin elinde yeteri kadar şifreli Enigma mesajı ve çözülmüş halleri mevcuttu. Bu bilgiler standart casusluk faaliyetleri ile elde edilmekteydi [4]. Prosedürler Enigma mesajlarının 250 karakteri aşmasını yasaklıyordu. Bunun nedeni aynı harfin mümkün olduğunca değişik harflere şifrelenmesi idi. Öylece şifreli metnin içinde benzer tekrarların oluşması olasılığı azaltılmış harf-kullanım-sıklığı bilgisinin mümkün olduğunca karartılması amaç-

lanmıştı. Tekrarlar olmayınca çözüm daha da zorlaşıyordu.

Ancak Almanlar Enigma operasyonu ile ilgili olarak titiz prosedürler oluşturmalarına rağmen, sahadaki operatörler mesaj içeriklerinde düz metin karşılıklarında pek çok tekrarlara yer vermekteydiler. Mesajlarda "Heil Hitler" gibi terimler sıkça yer almaktaydı [24]. Her mesajın başında kime gönderildiği ve kimden gönderildiği yazılıyordu. Hergün aynı saatte aynı istasyonlardan hava raporları gönderiliyordu. Buna benzer mesaj analizleri bazı mesajların bir kısmını tahmin edilebilir kılıyordu. İngilizler mesajların düz metin karşılıklarında tahmin edilen bu kısımlara kısaca "crib" demişlerdir. Alan Turing bu crib'lerden, şifrelerin bazı koşullar altında kolayca çözülebileceğini farketmiş ve bunu gerçekleştirecek prosedürleri tanımlamıştır[24]. Turing bu işlemleri otomatik olarak yapacak bir de elektronik makine tasarlamıştır [3,26].

Turing, belki de Polonyalıların kendi şifre kırma makineleri için seçtiği isimden esinlenerek, makinesine Bombe adını vermiştir. Bu makine elektronik olarak çalışan ve mesaj içeriklerinin bir kısmının tahmin edilerek geri kalan kısmının belirlenmesini sağlayan bir makine idi. Bir gün için yeteri kadar mesaj üzerinde çalışıldığında ve deşifreleme gerçekleştiğinde o gün için ön-bağlantılar, rotorlar ve sıralamaları ile günlük anahtarın çözülebilmesi mümkün olabiliyordu.

Turing'le birlikte çalışan Gordon Welchman Turing'in tasarladığı makineyi daha da geliştirecek "diagonal board" (kısaca: örümcek) denen bir eklenti ile daha etkin hale getirmiştir.

Turing'in Enigma şifrelerini kırma yaklaşımını bir örnekle anlamaya çalışalım. Doğal olarak örneğimizi de Türkçe olarak ele alalım. Hepimizin bildiği gibi resmi yazışmalarımızın pek çoğu birbirine benzer şekilde biter; SAYGILARIMLA ARZ EDERİM, DURUMU BİLGİLERİNİZE ARZ EDERİM veya ARZ EDERİM ibareleri pek çok askeri ya da sivil mesajın sonunda yer almaktadır.

Turing'in yaklaşımı Alman mesajlarının da tahmin edilebilir başlangıç ve bitişleri olduğu varsayımına dayanıyordu. Ayrıca İngilizler başka vasıtalarla ele geçirdikleri veya bir şekilde çözülmüş olan Alman mesajlarına da sahiptiler. Ayrıca bazı Alman iletişim noktalarından hergün benzer mesajlar, örneğin belli bir noktadaki hava durumu, gönderilebiliyordu. Sonuç olarak Turing, mesajın belli bir kısmı tahmin edilebilirse, Enigma'nın çalışma şeklini göz önüne alınarak imkânsız olan pek çok olasılığın bertaraf edilebileceği ve geriye kalan mümkün çözüm uzayında yapılacak bir deneme-yanılma aramasıyla sonuca gidilebileceğini düşündü.

Turing ve ekibi, Bletchley Park denen eski bir malikanede çalışmalarını sürdürmekteydiler. İngiltere'nin çeşitli noktalarına dağıtılmış olan yüz kadar operatör sürekli olarak Alman mesajlarını dinlemek-

te ve şifreli mesajları kaydetmekteydiler. Bu mesajlar hızla Bletchley Park'a iletilmekte orada da her mesajın anlaşılması için bir çalışma başlatılmaktaydı. Bletchley Park'm çalışma şeklinin analizini tarihçilere bırakalım ve örnek bir mesaj üzerinden Turing sisteminin nasıl çalıştığını anlamaya çalışalım.

Şifreli bir Enigma mesajı ulaştığında, yapılması gereken ilk şey bu mesajın içeriğinde olabilecek bir kısmı tahmin etmek idi. İçerikte olabileceği düşünülen bu kısma "crib" adı verildiğini belirtmiştik. Mesaj için bir crib belirlendiğinde, bu crib'in mesajın hangi noktasına karşı geldiğini de tahmin etmek gerekiyordu. Bunun için şifreli metin üste, crib alta konuyor ve Enigma kurallarına aykırı olmayacak şekilde crib için bir başlangıç pozisyonu belirleniyordu. Crib'i yerleştirirken kullanılan ana kural Enigma'nın hiçbir harfi kendi kendine şifrelemeyeceği gerçeği idi. Eğer crib ve şifreli metnin alt alta gelen harflerinden herhangi birisi aynı ise, crib'in pozisyonu bir kaydırılıyor ve bu durum tekrardan kontrol ediliyordu.

Crib için şifreli metnin altında potansiyel olarak doğru olabilecek uygun bir yer bulunduğunda, crib'in başlangıç pozisyonundan başlanarak her pozisyon numaralanıyordu.

Şimdi durumu daha iyi anlayabilmek için, çözmeye çalıştığımız şifreli mesajın şifrelenme anına geri döndüğümüzü düşünelim. Elimizdeki crib'in ilk harfini Enigma klavyesi ile girdiğimizde, Enig-

ma pencere pozisyonu birinci pozisyonuna ilerletecek ve crib'in ilk harfine karşı gelen şifreyi uygun lambayı yakmak suretiyle üretecektir. Crib'in ikinci harfini Enigma klavyesi vasıtası ile girdiğimizde Enigma pencere pozisyonu ikinci durumuna ilerleyecek ve bir sonraki şifreli harf de üretilecektir.

Enigma pozisyonları bu şekilde düşünüldüğünde, her bir Enigma pozisyonunun bir şifrelenmiş bir de düz metin olmak üzere iki harfi birbirine bağladığını düşünebiliriz. Böylece ortaya çıkan durumu, biraz sonra örnekte göreceğimiz gibi, bir graf şeklinde ifade etmek mümkündür. Bu şekilde bir crib ve bir şifreli metin kullanılarak oluşturulmuş olan graflara Bletchley Park ekibince "menu" denmekteydi.

Şimdi örnek bir Enigma şifreli mesajı seçelim ve yine örnek olarak kullanacağımız SAYGILARIMLA ARZ EDERİM ifadesini "crib" olarak alalım. Öncelikle crib'deki boşluklar yerine X harfi koyalım. Bunun nedeni Alman mesaj göndericilerinin boşluk yerine X harfi kullanmalarıdır.

Bu çalışmalarımız sırasında şu iki gözlemimizi not edelim. Enigma, herhangi bir pozisyonda iki harfi birbirine kısa devre ederek kodlama işlemini gerçekleştirdiğinden dolayı, herhangi bir pencere pozisyonunda bir harfi kendi kendine kodlayamaz. Örneğin, A->A mümkün değildir. Almanlar boşluklar için genel olarak X harfini kullanırlar, rakamlar içinse yazılı karşılıklarını kullanırlardı, örneğin, bir rakamı için EIN.

Örnek mesajımız; SALDIRIYA HAZIRIZ SAYGILARIMLA ARZ EDERİM olsun. Bu mesajı 3 rotorlu Enigma'da, IVJ mesaj şifresi, IV-II-V (Sol-orta-sağ) rotor sıralaması ve numaraları, KFA rotor kaydırma sırası (Ringstellung) ve (AF BR CD EQ LO IK) Steckerbrett (ön-bağlantıları) bağlantıları ile kodlayalım. Ortaya çıkan şifreli mesaj;

FOFZ SHHE UKOR LHKF PLXI BNKP BSDG MWEZ EWFP SYCJ N olacaktır.

Bu durumda crib'i şifreli metnin en sonuna şifreli ve düz metinleri alt alta gelecek şekilde yerleştirelim. En üstte de alttaki düz metni şifrelediğini düşündüğümüz Enigma makinesinin pozisyon numaraları olsun. Bu pozisyon numaralarımız crib'in başlangıcından itibaren sırayla verilir.

Düz metin ile şifreli metin eşleştirilirken öncelikle Enigma kuralları uygulanarak uyumsuz eşleştirmeleri elememiz gerekmektedir. Mesela yukarıdaki düz metni iki sola kaydırmış olsa idik, 14. Pozisyonda düz metindeki Z harfi; şifrelenmiş olarak Z harfine karşı gelecekti ki, Enigma'nın çalışma şekli nedeniyle bu mümkün değildi. Bir diğer nokta da,

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
P	L	X	I	B	N	K	P	B	S	D	G	M	W	E	Z	E	W	F	P	S	Y	C	J	N	
		S	A	Y	G	I	L	A	R	I	M	L	A	X	A	R	Z	X	E	D	E	R	İ	M	

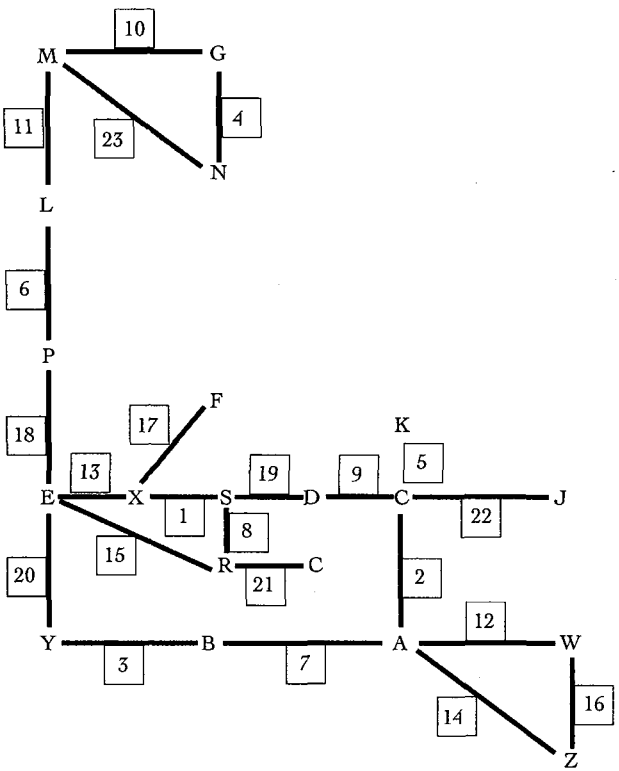
Tablo 1 Şifreli metin ile crib'in alt alta yerleştirilmesi

menülerin test edilebilir hipotezler üretebilmesidir. 3 ya da 4 döngü içermeyen menülerin çok fazla sonuç üretmeleri genellikle mümkün olamamaktadır. O halde test etmeye değer menüler üretmek anlamlı olduğundan, seçilecek menüler denenebilecek sayıda alternatif üretebilmeliydi.

Şimdi crib'in harfleri ile karşı gelen şifreli hallerini bir grafın düğümleri (noktaları) ve pozisyon numaralarını da grafın kenarları (bağlantıları) olarak düşünürsek, yukarıdaki tabloyu Şekil 8'deki gibi bir menu olarak ifade edebiliriz. Menüye dikkatle bakarsak, crib ve şifreli metnin harflerini birbirine bağlayan çizgilere, Tablo 1'de verilen pozisyon numaralarının karşı geldiğini görebiliriz. Örneğin 10. Pozisyonda M crib harfi, G olarak şifrelendiği için menunun en üstünde bu ilişki gösterilmiştir.

Şifreli metin ve düz metni eşleştirdiğimizde, ortaya çıkan menüde dikkati çeken bir nokta şifreli metin ve düz metin harf ikililerinin bazı noktalarda birbirini tekrarlıyor olmasıdır. Örneğin, menünün sağ alt köşesinde görüldüğü gibi, 12 (WA), 14 (ZA) ve 16 (WZ) pozisyonlarında bir döngü vardır (Şekil 9). Şöyle ki, 12. Pencere pozisyonunda şifrelemeyi gerçekleştirdiğini düşündüğümüz Enigma makinesi A harfini W harfine kodlamış, aynı makine 14. Pencere pozisyonunda A harfini Z harfine ve 16. Pencere pozisyonunda ise Z harfini W harfine dönüştürmüştür. Burada A-W-Z-A sıralamasına döngü diyoruz.

Varsayalım ki elimizde 3 tane enigma var. Yine varsayalım ki, orijinal şifrelemenin yapılmış olduğu Enigma'da takılı olan rotorları ve sıralarını biliyoruz. Şimdi elimizdeki 3 Enigma'dan birincisini ZZZ başlangıç pencere pozisyonuna ayarladığımızı varsayalım. Bu Enigma ile 12. pozisyonu simüle ettiğimizi varsayalım. Bu durumda 14. pozisyonu



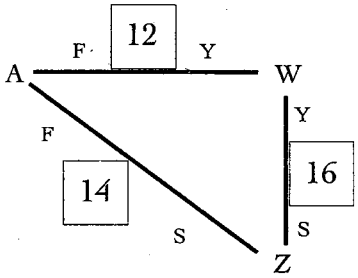
Şekil 8 Örnek menü

simüle eden Enigma'yı ZZB başlangıç pencere pozisyonuna ayarlamalıyız. Aynı düşünce ile 16. Pencere pozisyonunu simüle eden Enigma'da ZZD başlangıç pencere pozisyonuna ayarlanmalıdır.

Şimdi de şunu gözlemleyelim. Seri olarak 14, 16 ve 12. pozisyonları temsil eden Enigmaları seri olarak bağlayalım (Şekil 10). Her Enigma'nın giriş ve çıkışında, normalde 26 klavyenin herbirinden gelen 26 kablo bulunacaktır.

Ancak durumu basitleştirmek için Enigma giriş ve çıkışlarında sadece tek kablo varmış gibi şekillerimizi çizelim. Şekilde 12 no'lu pozisyona karşı gelen Enigma'nın giriş ve çıkışında sırayla A ve W harflerini görebiliriz. Ancak bu iki harfin de ÖBP (Ön-bağlantı Paneli) tarafından dönüştürülmüş olma ihtimali vardır. Böylece ÖBP'yi bir küçük kutucukla temsil edersek, A ve W'ya ÖBP karşılıkları olarak da sırasıyla örnek olarak f ve y atarsak (Yani A→f, W→y, Z→s), bu durumda Enigmaları birbirlerine bağlarken, ÖBP etkisinin önem taşımadığını görürüz.

Eğer Enigmalarımızın başlangıç pozisyonları yukarıda belirlenen düz metnin şifreli metne dönüştürülmesi sırasında belirlenen pencere pozisyonları ile uyumlu ise o zaman seri bağlanmış Enigmaların en soldaki ilk ÖBP girişine A harfini uyguladığımızda, Enigmaların diğer bağlantı noktalarında sırayla Z, W ve A harflerinin üretilmesini bekleyebiliriz. Şimdi bu harflerin ÖBP den geç-

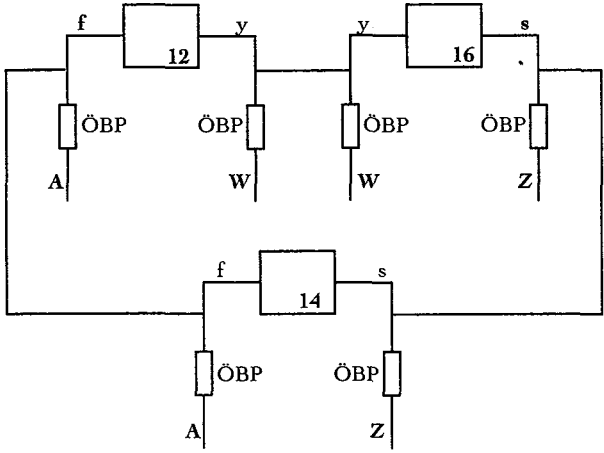


Şekil 9 12, 14, 16 no'lu pozisyonları gösteren döngü

miş hallerini düşünürsek, çevrimin girişine uygulayacağımız f, çıkışlarda y, s ve f harflerinin oluşmasını sağlayacaktır.

Tabi bu 12. pozisyondaki Enigma'nın doğru bir şekilde, şifreleme esnasında karşı gelen pozisyona kurulduğu anda geçerli olacak bir durumdur. Eğer bu karşılıklılık mevcut değilse (yani A→f değilse), girişe uygulanacak f, çıkışta y, s ve f harflerinin üretilmesini sağlamayacaktır. Veya daha doğrusu, çok az sayıda Enigma pencere pozisyonunun döngüde bir çözüm oluşturmasını bekleyebiliriz.

Bu örnek bize menülerden elde edilecek döngülerin Enigma şifrelerini çözmekte kullanılabileceğini göstermektedir. Ancak bunun için öncelikle bir şeyin gerçekleştirilmesi gerekmektedir. Enigma makineleri normalde birbirleri ile art arda bağlanacak şekilde tasarlanmamışlardır. Bunun çözümünü Bletchley Park ekibi, Açık Enigma adını verilen bir tasarımda bulmuştur.



Şekil 10 Yukarıda crib ve şifreli metin eşleştirmesinden elde edilen döngü 1

Açık Enigma (Letchworth Enigma)

Açık Enigmalar döngüleri simüle etmek üzere art arda bağlanabilmelilerdi. Ancak açık Enigmaların asli olarak varlık nedeni Enigma şifrelerinin çözülmesiydi. Bunun için Açık Enigma'dan beklenen, simüle edilen menu döngülerinin sağlandığı pencere pozisyonlarını belirlemekten ibaretti. Bunun için Açık Enigmalar belli bir pencere pozisyonunda başlayarak hızla imkânsız pozisyonları elimine etmek ve mümkün pozisyonları belirlemek üzere motorize olmalıydılar (matematiksel bir Enigma modeli için bkz. ek 2).

Böylece gerçekleştirilmesi gereken sadece açık bir Enigma değil aynı zamanda seri bağlanabilen

ve bir motorla ilerletilebilen, Enigma olmak durumundaydı. Böylece binlerce mümkün pencere pozisyonu, döngünün kurallarını sağlayıp sağlamadıkları için kısa sürede test edilebilirdi.

Çözüme aday pencere pozisyonları ortaya çıkarıldıktan sonra, bu iş için özel olarak atanmış operatörler tarafından, bu pencere pozisyonları birer birer mesajın bütünü için denenmekteydi. Bu işlem için normal Enigma kopyaları kullanılıyordu. Mesajın bu şekilde çözümü ortaya anlamlı bir düz metin çıkarıyorsa şifrenin doğru çözüldüğü ve önerilen aday pencere pozisyonunun doğru olduğu anlaşılıyordu. Bu yaklaşım İngilizlerin Enigma şifrelerini kırmalarının temelini oluşturuyordu.

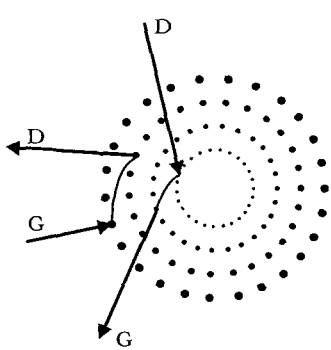
Ortaya konan çözüm, Açık Enigma, hem motor gücü ile ilerletilebiliyor hem de birbirine seri olarak (cascade) bağlanabiliyordu. Açık Enigma'da her bir rotora bir disk karşı gelmekteydi (Şekil 11)[26]. Ortasından bir şafta geçirilebilen diskler bir elektrik motoru tarafından serbestçe döndürülebilmekteydi. Disklerin herbirinde yirmi altışar tane temas noktası içeren daire şeklinde organize edilmiş dört grup bağlantı noktası bulunmaktaydı. Burada her bir bağlantı noktası rotordaki bir harf girişine karşılık geliyor, her disk tek bir rotoru temsil ediyordu. Ancak bir diskte aynı rotor iki kez simüle edilmişti. En dış iki daire arasında ve buna eşdeğer en iç iki daire arasında karşı gelen Enigma rotorundaki bağlantıların aynıları yapılmıştı. Böy-

lece Enigma açık hale getiriliyor ve rotorlar birbirlerine seri bağlanabiliyorlardı.

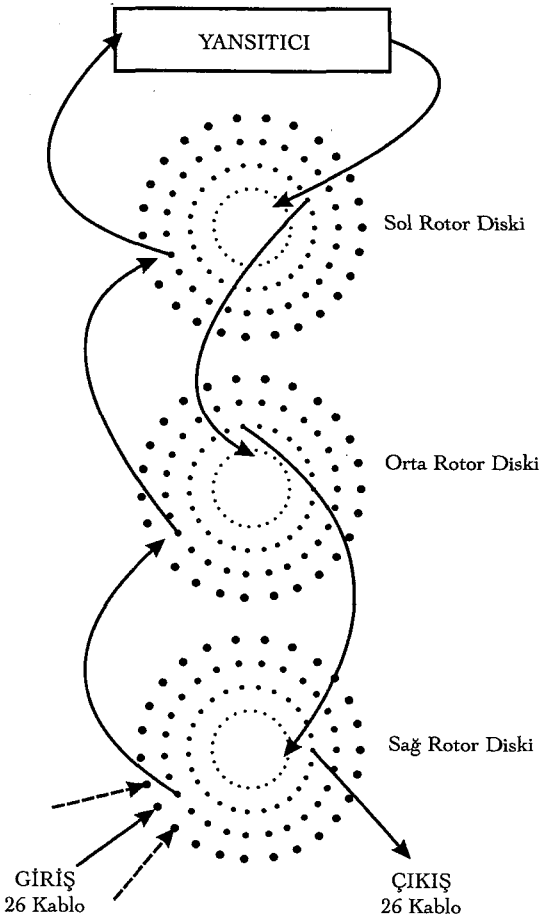
En dış iki dairede simüle edilen rotorun giriş tarafı (sağ tarafı) en dıştaki daire, çıkış tarafı ise ikinci daireydi. Rotorun (yansıtıcıdan) dönüş yönü en içteki iki daire tarafından simüle edilmişti. Burada rotorun çıkış yönü içteki daire olduğundan ve rotorun dönüş yönünün temsil edilmesi için ters-yüz edilmesi gerektiğinden, Şekil 11'de görüldüğü gibi, giriş en içteki daireden yapılmıştır.

Açık Enigma Şekil 11'de gösterilen türden 3 tane diskin birbirine bağlanmasıyla elde edilmişti (Şekil 12). En alttaki disk en sağ rotora karşı gelmekteydi. Sol rotor üstteki disk ile simüle edilmişti.

Açık Enigma aynen normal Enigma'daki gibi simetrik bir yapıya sahipti (Şekil 13). Yani aslında Enigma'nın çıkışı ya da girişi diye bir tarafı yoktu;



Şekil 11 Açık Enigma diski



Şekil 12 Açık Enigma simülasyonu yapan disk bağlantıları

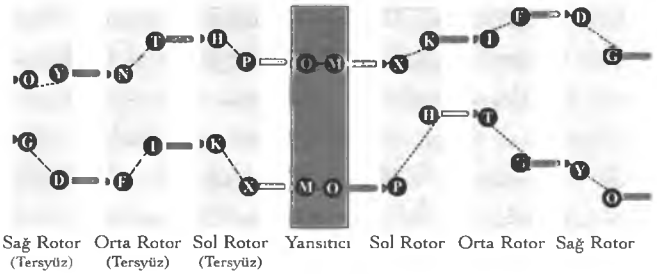
iki tarafta giriş ya da çıkış olarak kullanılabilirdi. Bir tarafa örneğin G harfi uygulandığında diğer tarafta D harfi beliriyorsa, D harfi uygulandığında da G

harfi beliriyordu. Böylece tamamen simetrik olan açık Enigma, değişik şekillerde keyfi olarak bağlanarak son derece sofistike menülerin oluşturulabilmesine olanak tanımaktaydı. Örneğin yukarıdaki cribde 16. pozisyonda düz metin Z harfi şifreli W harfini üretmektedir. Buna karşı gelen Enigma bağlantısı tamamen simetrik olduğundan Şekil 10'da gösterildiği gibi iki gösterim tarzı birbirine eşittir. Çünkü açık Enigma'nın hangi tarafına olursa olsun Z harfinin uygulanması, Enigma'nın simetrik ve yönsüz yapısından dolayı diğer tarafta W harfini üretecektir.

En sağ rotora karşı gelen disk en hızlı dönen disk idi. Bu diskin her turu orta diskin bir pozisyon dönmesini sağlıyordu. En yavaş dönen disk, en soldaki rotoru temsil ediyordu. Böylece açık Enigma, Enigma'nın herhangi bir rotor sıralaması için mümkün olan tüm başlangıç pozisyonlarını otomatik olarak bir motor vasıtası ile tarayabilme özelliğine sahipti.

Crib ve Menülerin Simülasyonu

Açık Enigma'da aslında bir diskin üzerinde sadece bir Enigma rotorunun bağlantıları simüle ediliyordu. En dıştaki iki dairede yer alan noktalar ve en içte yer alan iki dairedeki noktalar arasında rotor bağlantıları iki kez gerçekleştirilmişti. Bunlardan dıştaki elektrik akımının rotora giriş yönünü, içteki bağlantılar ise akımın yansıtıcıdan (Umkehrwalze) yansıtıldıktan sonra rotora dönüşünü simü-

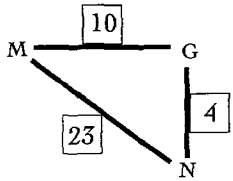


Şekil 13 Açık Enigma ve simetrik yapı

le etmekteydi. Böylece oluşturulan Enigma rotorları cribler vasıtası ile ortaya çıkarılan menülerin şematik yapısına göre başlangıç değerlerine ayarlanıp birbirlerine bağlanabiliyorlardı. Bunun sağladığı avantaj ise Enigma rotorlarının hareketlerinin otomatize edilerek elde edilen menüye uygun durumların tüm başlangıç pozisyonları denenerek ortaya çıkarılmasıydı.

Menu içerisindeki döngü sayısı menünün bir çözüm üretmede ne kadar faydalı olabileceğinin bir işareti idi. Böylece mümkün olduğu kadar çok hipotez denenebilir ve döngüler vasıtası ile test edilebilirdi. Daha sonra Gordon Welchman tarafından yapılan örümcek ilavesi menülerin kullanımını daha da artıracaktı.

Örneğin Şekil 14 ve Şekil 15'de yukarıda elde ettiğimiz menüden elde edilmiş iki döngünün açık Enigma motorlarınca nasıl simüle edilebileceğini görüyoruz.

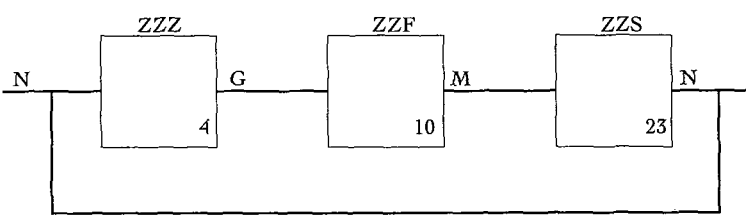


Şekil 14 Döngü 2

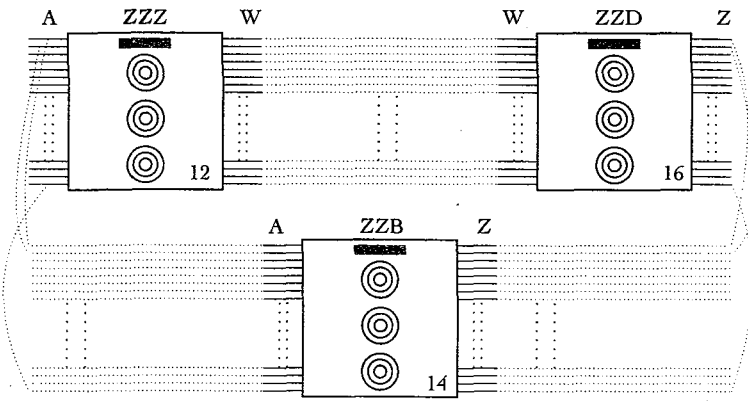
Şimdi tekrar Şekil 9'daki döngümüze dönelim. Bu döngünün Açık Enigma eşdeğerini Şekil 16'da görebiliriz.

Şekil 9'daki menünün 12 no'lu pozisyonunu simüle eden Enigma ZZZ başlangıç durumuna getirilmiş, diğerleri de kendi pozisyonları ile orantılı olacak şekilde karşı gelen başlangıç durumlarına ayarlanmışlardır. Öyle ki 12 no'lu pozisyonu temsil eden Enigma girişine bir harf uygularsak, karşımıza şu durumlar çıkabilir.

Birinci durumda (Şekil 17), eğer bu durum menü ile uyumlu bir durum ise, birinci Enigma'nın girişinde A, çıkışında W, ikinci Enigma'nın çıkışında



Şekil 15 Döngü 2'ye karşı gelen açık Enigma bağlantıları ve pencere posizyonları



Şekil 16 Şekil 9'da gösterilen döngünün açık-Enigmalar kullanılarak simülasyonu

Z, üçüncü Enigma'nın girişinde A çıkışında Z tellerinde (veya da bu harflerin ön-bağlantı paneli karşılıklarında, yani f, y, s) akım bulunacaktır. Bu durumda ZZZ başlangıç pozisyonu menü ile uyumlu olarak kaydedilir. Şebekedeki tüm Enigmaların başlangıç pozisyonları bir kaydırılarak yeni durumun menü ile uyumlu olup olmadığına bakılır. Bu işlem şu anki rotor sıralamasının mümkün tüm başlangıç pozisyonları için tekrarlanmaya devam edilir.

İkinci olası durum ise şebekede pek çok telde, belki de tamamında, akım bulunmasıdır. Bu da bu durumda bağlanan Enigmaların menü ile uyumlu bir sonuç üretmedikleri anlamına gelir. Bu durumda da Enigmalar bir pozisyon ilerletilerek bir sonraki pencere pozisyonu menu ile uyum için test edilir.

Şimdilik Steckerbrett etkisini göz önüne almayalım.

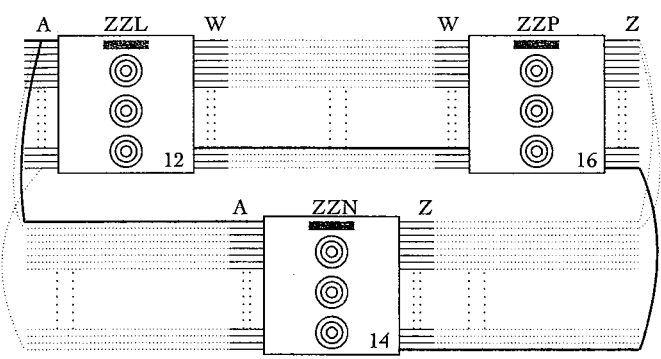
Böylece gerçekleştirilen Enigma pozisyonlarının menü ile uyumluluğu çalışması sonucunda elde edilen uyumlu başlangıç pozisyonları listelenir. Tabi ki bu işleminde mümkün olan her rotor pozisyonu için denenmesi gerekmektedir. Ancak bu işlem rotor sıralamalarını tahmin ederek biraz daha çabuklaştırılabilmekteydi. Alman prosedürleri günlük mesaj anahtarlarının ve rotor sıralamalarının aynı ay içinde iki kez tekrarını yasaklıyordu. Dolayısıyla ayın sonuna doğru seçilebilecek rotor sıralama seçim alanı daralıyordu [24].

Menu ile uyumlu olarak elde edilen pencere pozisyonları, şifreli mesajın tek tek yukarıda bulunan pozisyonlara ayarlanarak normal bir Enigma ile yazılması ve ortaya çıkan metnin anlamlı olup olmaması ile test edilmekteydi. Tabi ki elde edilen uyumlu pozisyonların içinde sadece bir tanesi, doğru şifre anahtarına karşı gelmektedir.

Açık Enigma bağlantılarında pozisyonların sırasının önemli olmadığı görülür. Burada önemli olan bir elektrik akımı döngüsü durumunun yaratılabilmesidir. Enigma'nın tamamen simetrik bir yapısı olduğunu biliyoruz. Örneğin 16. pozisyonda Enigma'ya girilen düz metin Z çıkış şifreli metin ise W olmasına rağmen şekilde bu bağlantı tersine çevrilmiştir. Bu yapılabilir çünkü o pozisyonada Enigma W ile Z'yi kısa devre ettiğinden Enigma'nın girişi-

ne uygulanacak harf ne olursa olsun diğeri elde edilecektir (Şekil 12).

Bir diğer husus ise, Enigma'nın çıkışına uygulanacak bir elektrik akımının iki yönlü olarak akacak olmasıdır. Spesifik olarak, akım Enigma çıkışma uygulansa bile, girişte hangi tele kısa devre olmuşsa o tele de akım geçecektir. Çünkü belli bir pozisyonda Enigma 26 harften 13 tane çifti birbirine kısa devre etmektedir. Örneğin Şekil 16'da 12. pozisyondaki Enigma'nın girişine uygulanacak A harfine karşı gelecek bir akım 14. pozisyonu temsil edecek Enigma üzerinden F harfini üretirken, 12 ve 16 pozisyonları temsil eden Enigmalar üzerinden C harfini üretebilir. Bu durumda C harfi 14 no'lu pozisyonu simüle eden Enigma tarafından R harfine kısa devre edilmişse, 12 ve 14 no'lu pozisyonlara karşı gelen Enigmaların girişinde R telinde akım bulunacaktır. Öte yandan 16 numaralı Enigma'nm



Şekil 17 Stabilize olmuş döngü

çıkışında bir önceki döngüde beliren C harfi tersten 16 ve 12 no'lu Enigmalara uygulanarak örneğin O harfine ait telin yine 12 no'lu Enigma girişinde akım taşımasına neden olabilecektir. İşte böylece hem tersten hem düzden hızla akan elektrik akımı sonuç olarak stabil bir duruma gelecek ve yukarıda belirlenen durumlardan birine göre lambaları yakacaktır.

Steckerbrett (Ön-Panel Bağlantıları) Etkisi

Yukarıda belirlenen analizde Steckerbrett etkisi ihmal edilmiştir. Daha önce de belirtildiği gibi, üzerinde çalıştığımız örnek mesaj şifrelenirken, AF harfleri birbirlerine ÖBP tarafından bağlanmıştır. Örneğimizi basitleştirmek için varsayalım ki WY ve ZS bağlantıları da Steckerbrett tarafından gerçekleştirilmiş olsun. Bu durumda Şekil 16'da verilen Enigma şemasının stabil bir duruma gelebilmesi için farklı bir analiz gerekmektedir.

Şimdi menüyü oluşturduğumuz tabloyu yeniden göz önüne alalım (Tablo 2). Bu tabloda düz metin ile şifreli metin arasında iki satır daha oluşturulmuştur. Düz metinin hemen üzerindeki satırda, düz metin harflerinin Steckerbrett'ten geçtikten sonraki durumları görülmektedir. Şifreli metnin hemen altında ise Enigma'dan geçen Steckerbrett'le de kodlanmış olan metnin şifreli hali görülmektedir. Steckerbrett Enigma'dan çıkan şifreli

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
P	L	X	I	B	N	K	P	B	S	D	G	M	W	E	Z	E	W	F	P	S	Y	C	J	N	Z	P	T
									Z				Y		S		Y	A		Z							
		Z	F					F					F		F		S										
		S	A	Y	G	I	L	A	R	I	M	L	A	X	A	R	Z	X	E	D	E	R	I	M		

Tablo 2. Ön-bağlantı panelinin etkisi

metinleri bir kez daha kodlayarak sonuç şifreli metne dönüştürmektedir.

Aslında yukarıda oluşturulan menü Steckerbrett bağlantıları ile birlikte gösterildiğinde (Şekil 17) enteresan bir gözlemleme yapmak mümkün olabilmektedir. Örneğin W harfi Steckerbrett'ten geçtikten sonra Y harfine dönüşüyorsa şekilde iki noktada Y harfinin belirmesini bekleyebiliriz. Öte yandan Z harfi Steckerbrett karşılığı S ise bunun da iki noktada belirmesini bekleyebiliriz. A içinde Steckerbrett dönüşümü F harfi olduğundan iki noktada da F harfi belirmesini bekleyebiliriz.

Şimdi Şekil 16'da kesikli çizgilerle gösterilen bağlantıları yaptığımızı düşünelim. Rotorların başlangıç pozisyonlarının doğru noktada olduğunu varsayalım. Bu durumda 12 no'lu pozisyonu simüle eden açık Enigma'nın girişine F harfi uyguladığımızda çıkışında Y harfi, bunun da sıradaki Enigma'nın çıkışında S harfi ve bunun da 14. pozisyonun simüle eden açık Enigma'nın çıkışında F harfinin belirmesi gerekir. Bu durumda Enigma şema-

sı stabil bir duruma ulaşmıştır. Tüm temas noktalarında sadece bir telde akım vardır.

Şimdi bir an için seçilmiş olan rotor başlangıç pozisyonlarının, gerçekte kullanılmış mesaj anahtarından farklı olduğunu varsayalım. Örneğin 12 no'lu pozisyona karşı gelen açık Enigma'nm girişine R harfi uyguladığımızı varsayalım. Bu da çıkışta G harfine, o da 16 no'lu pozisyonu simüle eden açık Enigma vasıtası ile O harfine dönüşsün. 14 no'lu pozisyonu temsil eden açık Enigma'da O yu L ye dönüştürmüş olsun. Bu durumda 12 R harfini uyguladığımız noktada iki tane telde akım olur; R ve L. Burada A harfinin Steckerbrett dönüşümü olarak R harfini seçtik. Bu işleme bir "hipotez" diyeceğiz. Herhangi bir bağlantı noktasında birden fazla noktada akım bulunması hipotezimizin yanlış olduğunu gösterir. Eğer, hipotezimiz doğru olsaydı, yani rotorların başlangıç pozisyonları doğru seçilmiş olsalardı ve ayrıca A harfinin Steckerbrett karşılığı da gerçekte R olsaydı, o durumda döngüden geçen akımın hemen stabilize olarak tek noktada, yani R harfini gösteren telde mevcut olması gerekirdi. Bu durumda ise hipotezimiz, yani "seçilen başlangıç pozisyonu ve A'mn Steckerbrett karşılığının R olması" hipotezi doğru olurdu.

Steckerbrett bağlantılarına göre, girişte S tuşuna basıldığında öncelikle Steckerbrett bu bağlantıyı Z harfine çevirecek ve Z değeri akım karşılığı olarak Enigma'nın girişine uygulanacaktır. Aynı

şekilde Enigma'nın çıkışında S harfi görüldüğünde bunun Steckerbrett tarafından çevrilmeden önce Enigma'dan çıkışta Z harfi şeklinde çıktığını söyleyebiliriz.

Tablo 2'de sadece belirli Steckerbrett bağlantıları basitlik için gösterilmiştir. Ortadaki iki satır çıplak Enigma giriş ve çıkışlarını göstermektedir. Diğer Steckerbrett ve düz metin girişleri göz önüne alındığında yukarıdaki tablo ortaya çıkacaktır.

Şimdi Şekil 16'nın analizini yeniden gerçekleştirelim. Artık girişe A uyguladığımızda bu Steckerbrett tarafından dönüştürülecek ve çıplak Enigma'nm girişlerine F uygulanmış olacaktır. Yani 12 no'lu menü pozisyonunu temsil eden açık Enigma'nın girişine F olarak uygulanacaktır. Çünkü Steckerbrett A harfini F harfi ile değiştirecektir. Aynı şekilde, eğer test edilen başlangıç pozisyonu doğru ise W ve Z harfleri yerine sırasıyla Y ve S harfleri görülecektir. Yani aslında açık Enigma modelinin oluşturduğu Şekil 16'daki şebekenin girişine F harfi uygulandığında, seçilen başlangıç pozisyonları doğru olduğunda, sırayla Y ve S lambaları yanacaktır. Bunların dışında da herhangi bir lamba yanmayacaktır.

Şekil 10'da Steckerbrett bağlantılarının da gösterildiği açık Enigma şemasını görmekteyiz. Burada en solda A harfinin Steckerbrett üzerinden geçerek F harfine dönüştüğünü görmekteyiz. Böylece 12. pozisyonu temsil eden Enigma girişine ger-

çekte F harfi uygulanmaktadır (AF Steckerbrett bağlantısı varsayılarak). WY Steckerbrett bağlantısını varsayarak 12. pozisyonu simüle eden Enigma çıkışında Y harfi beklenecektir. Y harfi Steckerbrett'ten geçtikten sonra W harfine dönüşecektir. 16. pozisyonu simüle eden Enigma'nın girişlerinde de Y harfi olmalıdır. Çünkü W ve Y Steckerbrett ile birbirlerine bağlanmıştır. 16. pozisyonu simüle eden Enigma'nın çıkışında ise S harfini bekleyebiliriz (eğer başlangıç pozisyonları doğru ise!). S harfi Steckerbrett'ten geçerse Z harfine dönüşecektir. Dolayısıyla 14. pozisyonu simüle eden Enigma'nın sağ girişinde S harfi görünecektir. Şimdi bir an için 14. pozisyondaki Enigma'nın S harfini M harfine dönüştürdüğünü varsayalım. Burada M harfi geri besleme ile 12 pozisyondaki Enigma'nın girişine uygulanacağından ve burada zaten F kablosunda akım bulunduğundan şimdi hem M hem de F kablolarında akım bulunacaktır. İşte bu durum da zaten hipotezin yanlış olduğunun bir göstergesidir. Seçilen başlangıç pozisyonunda eğer 14 no'lu pozisyonu simüle eden Enigma M yerine F harfini üretseydi, o zaman bütün sistem stabil hale gelmiş olacaktı ve 12. pozisyondaki Enigma'nın girişinde sadece bir kabloda akım olacaktı ki o da F kablosu olacaktı. Bu durumda da hipotez gerçekleşmiş olacaktı. Oysa 12. pozisyondaki Enigma'nın girişinde iki ayrı kabloda akım bulunması zincirleme olarak, Enigmalar üzerinden oluşacak pek çok

kısa devreler vasıtası ile daha pek çok kabloda da akım bulunmasını getirecektir.

Steckerbrett bağlantıları için Enigma operatörlerine on adet kablo sağlanmıştı. Yani en fazla on harf eşleştirilebiliyordu. Her seferinde bu on kablonun tamamının kullanılması da gerekmiyordu. O halde pek çok harf Steckerbrett bağlantısında başka bir harfe bağlı değildi. Steckerbrett bağlantılarının tamamı doğru olarak keşfedilemese bile, yine de mesajın bir kısmı anlaşılabilir olabilir ve (Almanca bilen!) bir insan tarafından incelenerek daha da fazla bağlantılar tahmin edilebilirdi.

Bombe

Yukarıda tanımlanan makineye Bombe adı verilmekteydi. Özet olarak, mesajlarda olması olası düz metinler (crib) kullanılarak menüler oluşturuluyor, bu düz metinler şifreli metinlerle karşılaştırılarak döngüler oluşturulmaya çalışılıyordu. Sonra da bu döngüler açık Enigmalarla simüle ediliyor ve değişik başlangıç pozisyonları için Steckerbrett bağlantıları test ediliyordu. Bu işlem elektrik motorları ile gerçekleştirildiği için oldukça hızlı gerçekleştirilebiliyordu. Gordon Welchman'ın bir ilavesi ile Bombe'de bir iyileştirme daha gerçekleştirildi. Diagonal board adı verilen bu ilave bağlantı, Steckerbrett bağlantılarının belirli bir özelliğinden yararlanarak pek çok hipotezin hızlı bir şekilde yanlışlanmasını sağlayabiliyordu.

Diagonal Board

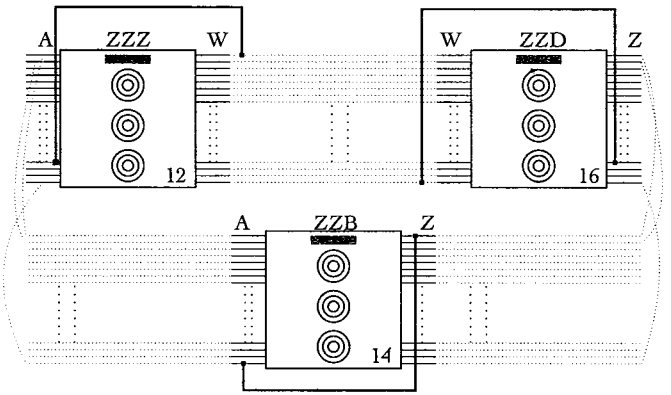
Bir hipotezin yanlışlanmasının açık Enigma bağlantı noktalarında birden fazla kabloda akım bulunması sonucu gerçekleştiğini gördük. Yukarıdaki menü örneğimizde W ve Z bağlantılarının olduğunu, bulunduğu noktaları düşünelim. Biliyoruz ki W ve Z Steckerbrett uygulanmadan önce klavyeden girilen harfleri göstermektedir. Bir an için W'nin Steckerbrett karşılığının Z olduğunu varsayalım. Bu durumda Steckerbret'tin simetrik yapısı nedeniyle Z noktasında da W belirmesi gerektiğini biliyoruz. O halde W harfinin beklendiği noktadaki z telini Z harfinin beklendiği noktadaki w teline kısa devre ederek önemli bir avantaj elde edebiliriz. Böylece W karşılığı Z olduğunda W noktasındaki z teli üzerindeki akım Z noktasındaki w teline kısa devre edilmiş olur. Eğer Z'nin Steckerbrett karşılığı W olmuyorsa o halde Z noktasında w teline ilave olarak bir tel daha akım taşıyacaktır. Kısa sürede ileri ve geri hareketelerle akım pek çok bağlantının akım taşımasına ve hipotezin hızla yanlışlanmasına neden olacaktır. Aksi halde, yani W noktasında Z ve Z noktasında W olması halinde ise yapılan kısa devreden hipotez herhangi bir zarar görmeyecektir (Şekil 18).

Peki Steckerbrett karşılığı olarak W noktasında A belirseydi. O zamanda A noktasında W belirmesi gerekirdi. O halde yukarıdaki mantığı uygulayarak Wa kablosunu da Aw kablosuna bağlamak bize hipotez testlerimizde bir avantaj daha sunmak-

tadır. Aynı mantığı sürdürerek W'nin her bir teli (Wx) karşı gelen harfin w teline (Xw) bağlanarak elde ettiğimiz avantajı en yüksek değerine taşıyabiliriz. Böylece oluşturulan örümcek benzeri yapıya Diagonal Board denmiştir (Şekil 19).

Diagonal Board'da her bir harf 26 kablo ile temsil edilmekteydi. Dolayısı ile toplamda 26 x 26 kablo mevcuttu. Burada her bir harfi temsil eden 26 kablo yine 26 harfi temsil etmekteydi. Örneğin A kablosunu ele alalım. A kablosu aslmda 26 adet kablonun oluşturduğu bir demet kablodan ibaretti. Burada her kablo numaralanmış ve A->1, B->2, C->3, vs. şeklinde harflere karşılık düşünülmüştü. Her harfe karşı gelen demet, ilgili kablo vasıtası ile diğer harflere karşı gelen kablo demetlerine bağlanmıştı (kısa devre edilmişti). Örneğin A harfindeki 2. kablo, B harfindeki 1. kabloya, A harfindeki 3. kablo, C harfindeki 1. kabloya vs., bağlanmıştı. Böylece 375 adet kablo ile tüm diagonal board bağlantıları yapılabilmekteydi.

Diagonal board, Steckerbrett bağlantılarında belirebilecek Steckerbrett bağlantılarının bir kısmının doğruluğunu kontrol edebilen bir yapıdır. Eğer bir menü içerisinde herhangi iki nokta arasında bir uyumsuzluk yakalanırsa bu kısa devrelerle kısa sürede tüm ağın tellerine akım kısa devre etme potansiyeline sahipti ve hipotezin yanlışlandığı anlamına geliyordu.



Şekil 18 Diagonal bağlantılarla hipotez yanlışlamasının güçlendirilmesi (Ön-panel etkisi)

Hipotezler

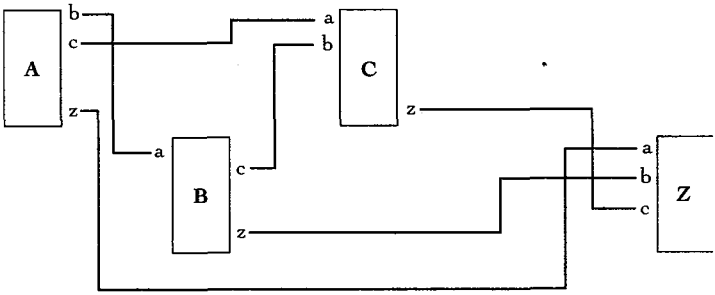
Genel olarak bir hipotezin testi, elektrik akımı hızında gerçekleşebilmektedir. Enigma içinden ve dışından oluşan kısa devreler vasıtası ile akım hızla ileri ve geri akmakta ve stabil bir duruma ulaşmaktadır. Burada 3 türlü stabil durum oluşabilmektedir. Ya uyguladığımız hipotez doğrudur ve açık her Enigma'nın giriş ve çıkışında sadece bir telde akım bulunmaktadır. Bu durum potansiyel bir çözümdür. Ya da tüm tellerde akım bulunmakta ama her Enigma bağlantı noktasında sadece bir telde akım bulunmamaktadır. O halde çözüm bu üzerinde akım olmayan tele karşılık gelen harftir. Diğer olasılık ise üzerinde akım bulunan tel sayısının arada bir yerde olması, yani 26 lambanın bir kısmının yanık bir kısmının sönük ol-

ması durumudur. Bu üçüncü durumda denenmemiş hipotezlerden bir kısmı denenmelidir. Doğru olma ihtimali olan hipotezin sönük lambalar arasında olma ihtimali vardır. Bu deneme işlemi anlaşıldığı kadar Machine Gun ya da makineli tüfek denilen bir ilave cihaz tarafından gerçekleştirilmekteydi.

Menü hazırlandığında Diagonal Board'un kabloları menüde kendilerine karşı gelen harflerin kablolarına bağlanmaktaydı. Böylece yukarıda en basit haliyle gördüğümüz Steckerbrett hipotezleri çok daha hızlı biçimde yanlış alternatifleri elimine edebiliyordu.

Register

Register menüye uygulanacak hipotezlerin oluşturulduğu bir cihazdı. Elektronik yapısı hakkında elimde detaylı bir bilgi olmamakla beraber, bu cihazın değişik hipotezlerin testi için bağlandığı yerde belli bir kabloya akım uygulayabiliyor ve birden fazla kabloda elektrik akımı mevcut olduğunda bunu tespit edebiliyor olması gerekir. Registerin başarılı bir operasyon için iki durumu birbirinden ayırabilmesi gerekmekteydi. Bunlar tek kabloda akım olması hali ve birden fazla kabloda akım olması hali idi. Üçüncü durum, 25 kabloda akım olması ve sadece bir kabloda akım olmaması hah ise, tespit edilirse doğru hipotezin tespit edilmesini bazı durumlarda sağlayabilirdi.



Şekil 19 Diagonal Board bağlantıları

Bombe elektronik yapısı ile hızlı bir şekilde mümkün tüm Enigma pozisyonları için hipotez testleri oluşturabilmekteydi. Menü ile uyumlu bir pozisyon yakalandığında Bombe duruyor, Steckerbrett bağlantıları ve pozisyon not edildikten sonra bir operatör tarafından operasyona devam etmesi sağlanıyordu.

Hipotezlerin Test Edilmesi

Bombe matematiksel olarak bir hipotez test makinesiydi. Menülerle belirlenmiş olan her bir döngü bir hipoteze karşı geliyordu. O da şuydu; Döngü girişine uygulanan harfi çıkışında da üretmeliydi. Aksi halde hipotez yanlışlanmış olacaktı.

Enigma döneminde bilgisayarlar henüz keşfedilmemişti. Bombe'nin tasarımını ilginç kılan buydu. Bombe'de hipotezin test edilmesi birden fazla uçta akım olması durumu ile ifade edilmişti. Eğer sadece bir uçta akım varsa hipotez doğrulanıyor, birden fazla uçta akım olması halinde ise hipotez yanlışlamyor-

du. Daha önceki şekillerde görüldüğü gibi, bu durum oldukça mantıksal idi, çünkü hipotez menülerle belirlenmiş döngülerin girişine uygulanan akımlarla ifade edilmekteydi. Şekil 16'da eğer test etmek istediğimiz hipotez, A'nm yerine Steckerbrett ile F konup konmamış olması idiyse, A yerine F uygulanarak ve sistem stabil hale geldiğinde akımın uygulandığı bağlantı noktasında kaç uçta akım oluştuğunu belirleyerek hipotezi test edebilmek mümkün oluyordu.

Diagonal Board ise çok spesifik bir şartı kontrol ederek hipotezlerin test edilmesini kolaylaştırıyordu. Bombe'de ana mesele çözüme aday pencere pozisyonlarının çok fazla olabilmesiydi. Diagonal Board hipoteze uygun durumların sayısını azaltabilme potansiyeline sahipti. O nedenle hipotez test sürelerini azaltabilirdi.

Şifrelerin Kırılması

Şifrelerin kırılması işlemi şifreli metinlerin dinleme istasyonlarınca toplandıktan sonra Bletchley Park'a iletilmesi ile başlıyordu. Merkeze ulaşan şifreli metinler gönderildikleri kaynaklara göre sınıflanıyor ve muhtemelen yine bu kaynaklara göre cribler oluşturuluyordu. Şifreli metnin içinde bulunması olası olan bu cribler şifreli metnin seçilen kısmı ile karşılaştırılıyor ve menüler oluşturuluyordu.

Cribler Enigma'da hiçbir harfin kendisine şifrelenemeyeceği prensibine uygun olarak şifreli metne kaydırma suretiyle eşleştiriliyordu.

Şifreli metinle cribin eşleştirilmesi için adaylar üretildikten sonra, bu eşleşmelerden menüler oluşturuluyordu. Bir menünün işe yarayabilmesi için üç beş döngü içermesi gerekiyordu. Döngü içermeyen menüler zaten çözüm üretemeyecekleri gerekçesi ile dikkate alınmıyordu. İşe yarayacağı düşünülen menüler Bombe kullanılarak simüle ediliyordu. Diagonal Board bağlantıları da yapıldıktan sonra, menünün test edileceği rotorlar ve sıralamaları seçiliyordu.

Bombe ve Diagonal Board hazırlanınca, Bombe otomatik olarak çalışmaya bırakılıyor, zaman zaman geçerli durumlarda Bombe otomatik olarak duruyor, başlangıç pozisyonları ve Steckerbrett bağlantıları kayıt edildikten sonra operatör tarafından işlemin devam etmesi sağlanıyordu.

Aday başlangıç pozisyonları ve Steckerbrett bağlantıları ortaya çıktıkça, bekleyen Enigma operatörlerince deneniyor, anlamlı bir metin çıkıp çıkmadığına bakılıyordu. Anlamlı bir metin çıktıysa bu Steckerbrett bağlantılarının ve mesaj anahtarının çözüldüğü anlamına geliyordu. Steckerbrett bağlantıları tüm bir Enigma ağı için aynı değerleri taşıdığından, bir sonraki mesajın çözümünde kolaylık sağlıyordu. Bir kez bir mesaj şifresi kırıldığında, Steckerbrett bağlantılarına ilaveten rotor seçimleri ve sıralamaları da o gün için bulunmuş oluyordu.

IV. Bölüm

Şifreleme ve Şifre Kırılması

Enigma tarihte ilk, tam otomatik ve kitlesel kullanıma uygun, kriptografik güvenirliği oldukça yüksek ve elektronik bir şifreleme aygıtı idi. İcadın sahibi Scherbius[27] aygıtının başarısını görecek kadar yaşayamadı. 1928'de bir kazada yaşamını yitirdi. Ama Enigma hâlâ pek çok insanın ilgisini çekiyor ve çekmeye devam edecek.

Enigma'da muhteşem olan cihazın kendisi kadar, böyle bir cihazın ilk kez olarak kitlesel kullanıma alınabilmesi ve kitlesel kullanımı destekleyecek olan prosedürlerin geliştirilerek uygulanabilmesi idi. Önce Polonya'nın ama sonrasında özellikle İngiltere'nin şifre kırma işlemini olağanüstü ciddiye

alması ve binlerce insanı bu işe angaje edebilmesi de Enigma'nın tarihteki yerini belirlemesinde önemli oldu. Sonuçta, matematikçi ve elektronikçilerine güvenen bir ulusun belki biraz da çaresizlik içinde inanılmazlarla yola çıkarak başarıya ulaşması, Enigma hikâyesinin ihtişamını daha da artırdı. Enigma macerasında yer alan insanların öyküleri, binlerce insanın tek bir maksatla uyum içerisinde çalışabilmeleri kanımca tarihin en önemli ve en dramatik insan hikâyelerinden birisidir.

Enigma macerası bize şifreleme işleminin sadece matematikle değil ama sistemi kullanan insanların günlük yaşamları ve kültürleri ile de ilgili olduğunu göstermektedir. İngiliz matematikçi Turing'in farkettiği gibi pek çok mesaj ortak kelimeler, benzer hitap şekilleri ve sonlanmalar ve bazen de aynı bilgileri bulundurmaktaydı. Tüm bunlar Enigma mesajlarının çözümlenebilmeleri için etkin şekilde kullanıldı. Enigma operatörleri de prosedürlerin dışına çıkarak Enigma mesajlarının çözümlenmesine istemeden de olsa katkıda bulundular. Mesaj anahtarları duygusal nedenlerle veya dikkatsizce seçildi. Böylece anahtarların tahmin edilebilmeleri kolaylaştı.

Hepimiz biliriz ki askeri mektuplar veya sivil hükümet yazışmaları hep "İlgili makama", "Şu ya da bu komutanlığa" yazılır, "Saygılarla arz" edilir ya da "Bilgilerinize arz" edilir. Bunlarm hepsi ve alışılmış tüm hitap tarzları, rakibinizin şifre kırıcı-

larının yüzüne kurnaz bir gülücük konduracak kültürel izlerdir. Bu türden tahmin edilebilir metinler zamanımızın en güvenli şifrelerini dahi kırmakta kullanılabilirler. Şifreli iletişim işleminin güvenliğinin sağlanması davranışsal bir değişikliğin oluşmasını da gerektirmektedir.

Potansiyel rakiplerin şifrelerini kırabilmek öncelikle onların dillerini iyi anlamaktan geçer. Konuşulan dil tabi ki bu işin başlangıcıdır ama yetmez. Onların da kültürel davranışlarının mesajlarına yansıma şekli savaş öncesinde dosyalanmahdır. Faydalı faydasız şifrelenmiş metinler ve onların düz metin karşılıklarından bir kütüphane oluşturulmalıdır. Görülecektir ki potansiyel düşmanın kültürel davranışları istatistiksel bir çözüm noktasının başlangıcı olabilecektir. Böylece savaş sırasında çok daha hızlı yol alınabilir. Düşmanın aklı okunabilir ve henüz eylemlerine başlamadan engellenebilir.

Modern Şifreleme Yöntemleri

Önce sayısal iletişim de kaydedilen ilerlemeler ve ardından bilgisayar teknolojisindeki gelişmeler İkinci Dünya Savaşı sonrası bir bilişim ve iletişim devrinin oluşmasına yol açtı. İletişimin bu kadar kolaylaşması ve sayısallaşması, metin bilgilerinin yanında, ses, video ve resim gibi yeni bilgilerin de üretilmesi ve taşınmasına yol açtı. Buna bağlı olarak iletişimde güvenliği sağlayan şifreleme sistemleri de önemli bir evrim geçirdiler.

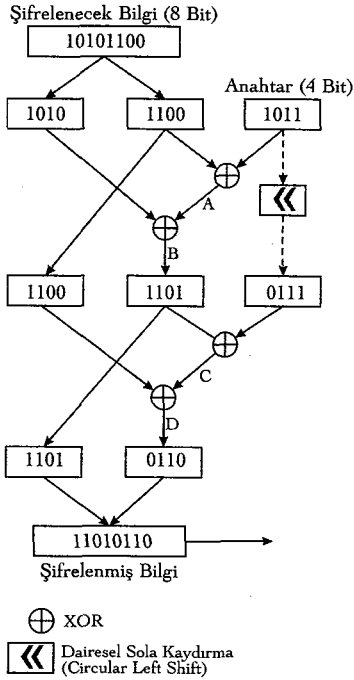
İkinci Dünya Savaşı'ndan önce ulaşılabilen teknoloji Enigma'nın en iyi örneklediği harf tabanlı bir şifrelemeyi otomatize etmeyi ve kitlesel kullanıma açmaya izin veriyordu. Bu yaklaşım da, bu kitap boyunca görmeye alıştığımız yöntem, şifreleme cihazının girişinde beliren harfin cihaz çıkışında bir başka harfle, şifrelenmiş harfle, yer değiştirmesinden başka bir şey değildi. Bu harf harf yapılan şifreleme bilgisayarların işlem yapma kabiliyet ve kapasitelerinin çok yüksek olmaları sonucu önemini yitirdi. Bilgisayar şifreleme algoritmaları bir dizi harfi yan yana koyarak ve bu harflerin sayısal eşdeğerlerini işleme koyarak yepyeni şifreleme yöntemlerini hayata geçirebilmeye izin verdi.

Bunu bir örnekle şöyle ifade edebiliriz. Örneğin SEVGİ kelimesini Enigma ile şifrelersek ortaya çıkacak şifreli metnin EVOLI gibi SEVGİ kelimesinden harf harf türetilmiş bir sonuç olacaktır. Oysa modern bilgisayar şifreleme algoritmaları önce SEVGİ kelimesinin ikili tabanda sayısal karşılığını bulacaktır. Diyelimki bu 7648 gibi bir rakam olsun. Şimdi bu rakamı işleme tâbi tutarak, örneğin çarpma, üs alma, bölme vs., yeni bir rakam elde edilecek ve bu elde edilen şifreli rakam alıcısına gönderilecektir. Yani şifreleme algoritması harflerle ilgilenmeyecek ancak harflerin sıralanmasının karşılığı oluşan sayıları (bilgi bloklarını) işleme koyarak çalışacaktır.

Zamanımızda yaygın kullanılan algoritmalardan bir sınıfı simetrik anahtarlı şifreleme algortiması olarak bilinir. Bu sınıf şifreleme sistemlerinde algoritmalar genel olarak gizli değildirler. Burada gizlenmesi gereken şey şifre anahtarıdır. Bu anahtar bir başkasının eline geçerse, algoritma bilindiğinden şifreyi çözmek çok zor olmaz. Şifre anahtarı hem alıcıda hem de göndericide olmak durumundadır. Aynı algoritma uygulanarak ve şifre anahtarı kullanılarak şifreler alındığı tarafta deşifre edilirler. Anahtar güvenliği ve dağıtımını sağlamak bu tür şifreleme yaklaşımları için ciddi bir önem arzeder. Bu tür algoritmalar güvenliklerini basit bir prensibe dayanarak sağlarlar; içinden anahtar olarak belirlenebilecek sayıların adedi o kadar fazladır ki, hiçbir bilgisayar bu olası anahtarları teker teker denemek suretiyle gerçek anahtara ulaşmak kabiliyetine pratik olarak sahip değildir.

Simetrik şifreleme yöntemlerinden en yaygın bilineni Data Encryption Standard'tır (DES)[29]. Bu yöntemin pek çok benzerleri de türetilmiştir [17, 18]. Bu yöntemler genel olarak kaynaklarını Feistel şifreleme yönteminde bulurlar [31].

Şekil 20'de oldukça basitleştirilmiş bir simetrik şifreleme algoritması konuyu açıklığa kavuşturmak için gösterilmiştir. Burada şifrelenecek bilgi elektronik sistemlerin kullandığı ikili (binary) tabanda gösterilmiştir. Buna göre örneğin "A" harfi



Şekil 20 Basitleştirilmiş Şifreleme Algoritması

elektronik sistemlerde "10101100" olarak gösterilmiş olsun. İkili tabanda sıfır (0) ve bir (1) dışında bir rakam kullanılmamaktadır. İkili tabanda bu rakamların adı "bit" olarak bilinmektedir. İkili tabanda 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1 ve 1 + 1 = 0 olarak sonuç verirler. Normal olarak kullandığımız onlu sistemde 1 + 1 = 2 olacağını bilmemize rağmen, ikili tabanda yalnızca sıfır ve bir rakamları kulanıldığmdan 1 + 1 = 0 olarak tanımlanmıştır. Bu toplama işlemi ikili tabanda (modülo iki toplama)

şeklinde de bilinir. Ayrıca bu işlem XOR işlemi olarak da bilinmektedir.

Feistel türü şifrelemede şifresiz düz bilgi gönderici ve alıcının bildiği bir anahtar ile XOR yapılarak şifrelenmektedir. En basit hali ile yukarıda belirtilen "A" harfine karşılık gelen "10101100" bilgisini şifrelemek için bir anahtar seçmeliyiz; diyelim ki seçtiğimiz anahtar "10111011" olsun. Şifreli metin bu iki bilginin yukarıda belirtildiği şekilde XOR (veya dijit-dijit ikili tabanda modülo iki toplama) edilmesi ile oluşur:

10101100 - düz bilgi
10111011 - anahtar
+_____
00010111 - şifrelenmiş bilgi

Deşifreleme işlemi ise bunun tam tersi olacaktır. Şifrelenmiş metni alan alıcı anahtar bilgisini şifrelenmiş bilgiden çıkararak;

00010111 – şifrelenmiş bilgi
10111011 – anahtar
-_____
10101100 – düz metin elde edecektir.

Burada çıkarma işleminin oldukça önemli bir özelliğine dikkatinizi çekmek isteriz. Düz şifrelenmemiş bilgiyi P ile ve anahtarı k ile göstererek, P + k (veya P xor k) ile elde edilecek sonuca C diyelim.

Bu durumda C'nin şifrelenmiş bilgi olduğunu da not ederek, C + k (veya C xor k) değerinin P'ye yani düz şifresiz bilgiye dönüştüğünü görürüz. O halde Feistel tipi şifrelemede alıcının yapması gereken kendisine ulaşan şifrelenmiş bilgiyi anahtar bilgisi ile XOR etmekten ibaret olacaktır.

Şekil 20'de sunulan örnek şifreleme sistemi temel olarak yukarıda tarif edilen işlemi gerçekleştirmektedir. Ancak burada şifresiz düz bilgi ile şifrelenmiş hal arasındaki görünür ilişkileri karartmak için şifrelenecek bilgi parçalara ayrılmış ve bu parçalar anahtarla değişik şekillerde XOR yapılmıştır. Burada bilgi iki adımda şifrelenmektedir. Birinci adımda bilgi dörder bitlik iki parçaya ayrılmakta ve bunlardan sağ parça (1100) bir sonraki adımda sol parçayı teşkil etmek üzere değiştirilmeden aktarılmaktadır. Sol parça (1010) ise bir anahtarla XOR işlemine tâbi tutulmaktadır. Burada seçilen orijinal anahtar "1011" öncelikle sağ parça (1100) ile XOR işlemine tâbi tutulmakta ve elde edilen sonuç (0111 olacaktır) sol parça (1010) ile tekrardan XOR işemine tâbi tutularak ikinci adımın sağ parçasını (1101 olacaktır) teşkil edecek şekilde aktarılmaktadır.

İkinci adımda işlemin aynısı uygulanmakta ancak bu adımda kullanılan anahtar, orijinal anahtarın en soldaki bitinin kaldırılıp en sağ bit olarak ilave edilmesi ile elde edilmektedir (bu işleme ikili tabanda dairesel kaydırma adı verilmektedir – left

circular shift). Böylece ikinci adımda elde edilen sol ve sağ taraflar birleştirilerek (11010110) olarak şifreli bilgi elde edilmektedir. Böylece "A" harfi olarak verilen düz bilgi (10101100), şifreli hali ile (11010110) olarak ortaya çıkmıştır.

Deşifreleme işlemi ise burada uygulanan işlemin aynısı olacaktır. Ancak ilk adımda kullanılacak olan orijinal anahtar şifrelemede ikinci adımda kullandığımız orijinal anahtar olarak kullanılacaktır. Bu kısım okuyucuya pratik yapması için bırakılmıştır. *İpucu. Şifrelenmiş bilginin sol dört biti (1101), şifrelemenin son adımında (0111) anahtarı ile XOR edilerek C elde edilmişti (sonuç 1010 olacaktır). Sonra C = "1010" ise önceki adımın sol parçası olan L = "1100" ile XOR edilmiş ve D = "0110" elde edilmiş idi. Bu durumda D = L XOR C olduğundan, L = D XOR C olacaktır. Aynı mantığı bir önceki adıma taşıyarak deşifreleme işlemini tamamlayabiliriz.*

Şekil 20'de sunulan şifreleme algoritmasında kullanılan anahtar uzunluğu 4 bittir. Bu da toplam 16 değişik anahtarın kullanılmasının mümkün olduğu anlamına gelmektedir. O halde dışarıdan birisinin şifreli metinleri çözmesi sorun olmayacaktır; denenecek anahtar sayısı toplamda 16 tanedir. Ancak anahtar uzunluğu artıkça, mümkün olan anahtar sayısı da artacağından bu işlem daha da zorlaşacaktır. Örneğin 128 bit uzunluğundaki bir anahtar için 10^{38}'den daha fazla sayıda anahtar

mümkündür. Simetrik şifreleme sistemlerinin güvenliği temel olarak anahtar uzunluğuna dayandırılmıştır. 1038 anahtarı, saniyede bir milyar anahtar deneyebilecek bir bilgisayar bile trilyonlarca yılda deneyerek bitiremez. İlave olarak, bu tür algoritmalar, anahtarı lineer permütasyonlar ve non-lineer yerine koyma yöntemleri ile kolayca analiz edilemeyecek şekilde işleyerek kullanmaktadırlar. Böylece düz şifrelenmemiş bilgi girişleri ile şifrelenmiş bilgi çıkışları arasında herhangi bir istatistiksel bağın mümkün olduğunca görülemez hale gelmesi hedeflenmiştir.

Yaygın olarak kullanılan bir diğer şifreleme algoritması da asimetrik algortimalar olarak bilinir. En iyi bilinen örneği RSA [21] algoritması olan bu tür yaklaşımda iki anahtar söz konusudur. Birinci anahtar göndericiye özel, ikincisi ise umuma açıktır. Bu iki anahtar birbirinin kodladığı metinleri çözmeye yarar. Eğer umuma açık anahtar kullanılarak şifreleme yapılırsa bu ancak özel anahtar tarafından çözülebilir. Eğer özel anahtar tarafından şifreleme yapılırsa bu da ancak umuma açık anahtar tarafından çözülebilir. Bu tür algoritmaları dijital imza için gerekli olan kimlik doğrulama ve imza olarak kullanmak mümkündür.

RSA algoritması özellikle internet uygulamalarında yaygın olarak kullanıldığından küçük bir örnek vermek istiyoruz. Varsayalım ki sizin için bir özel bir de umuma yönelik iki anahtar (dijital serti-

fika) üretmek istemekteyiz. Burada ilk adım iki tane asal sayı seçmektir. Örn. p = 3, q = 5. Sonra bu rakamlar birbiri ie çarpılarak r = p x q = 3 x 5 = 15 elde edilir. Daha önceki bölümlerde bahsi geçen ETF (Euler Totient Fonksiyonu) değeri r için (p-1) x (q-1) = 2 x 4 = 8 olur. Burada göndericinin özel şifre anahtarı (veya özel dijital sertifikası) d olarak adlandırılır ve ETF değerinden daha büyük olan asal sayı olarak seçilebilir, yani d = 11. Bu durumda, e (umuma yönelik sertifika değeri) d sayısının ETF e göre tersi olur. Detaylara girmeden bunun anlamı e ile d sayılarının çarpılıp ETF değeri olan 8'e bölündüğünde kalan 1 (bir) olacak şekilde seçilmeleridir. Bu durumda 3 x 11 = 33 olduğundan ve bu rakam 8'e bölündüğünde kalan 1 olduğundan e = 3 seçilir ve e ile d ETF'ye göre birbirinin tersidir denir.

e ve d değerleri elde edildikten hemen sonra p ve q değerleri yok edilmelidir. Aksi halde bu sayıları bilen kişiler e ve d'yi kolayca üretebilirler. Bir kez e ve d değerleri elde edildikten sonra şifreli bilginin elde edilmesi, düz bilginin d'ye göre üstünün alınması ve bu rakamın r = 15 sayısına bölünerek kalanının alınmasından ibarettir. Alıcı ise şifrelenmiş bu bilginin, umuma açık olan e sayısı ile üstünü alıp yine r'ye bölerek kalanının ahnması ile elde eder. Yukarıdaki örnek için göndermek istediğimiz bilginin 2 olduğunu varsayalım. d = 11 olduğundan 2^{11} hesaplanıp 15'e göre kalanı alındığında şifrelenmiş bilgi 8 olur. Alıcı tarafında, e = 3 olduğu bilin-

diğinden, 8^3 hesaplanıp 15'e göre kalanı alındığında 2, yani şifrelenmemiş metin elde edilir. Bunun tersi de geçerli olacaktır. Yani 2'nin önce 3'e (mod 15), sonra 11'e (mod 15) üstünün alınması da yine 2 sonucunu verecektir.

Simetrik algoritmalar içinde şifre değişimi ve dağıtımı yöntemleri önemli ölçüde güvenli hale getirilmişlerdir [22]. Bilgisayar iletişimi, banka işlemleri ve diğer güvenlik gerektiren online işlemlerin sayısındaki patlama şifreleme sistemlerinin günlük yaşantımıza derin bir şekilde girmesinin yolunu açmıştır. Bu şifreleme sistemlerinin bilinen güvenlikleri yüksektir. Örneğin RSA sistemi seçilen bir rakamın asal çarpanlarına ayrılması bilinen algoritmaların büyük sayılara uygulanabilirliğinin pratikte mümkün olmaması prensibine dayanır. Yukarıdaki örnekte 15 gibi küçük bir sayının asal sayılar 3 ve 5'in çarpımı olarak ifade edilebileceği kolayca belirlenebilir. Oysa daha büyük sayılar için, bir sayıyı asal çarpanlarına ayırmanın bilinen en iyi yöntemi tüm olasılıkların teker teker denenmesidir (Burada son yıllarda bazı daha başarılı yöntemlerin geliştirildiğini ama bunların konumuzun kapsamının üzerinde olarak değerlendirdiğimizi not edelim). Seçilen sayılar büyüdükçe bu işlemin pratik olarak yapılabilirliği hızla azalmakta ve kısa sürede imkânsız hale gelmektedir.

RSA, temel olarak modüler aritmetik tabanlı bir şifreleme yöntemidir. Modüler aritmetiğin grup

özellikleri, Fermat ve Euler teoremleri sistemin matematiksel tabanını oluşturmaktadır. Yeni yöntemler elliptic curve adı verilen bir grup eğrinin grup özellikleri kullanılarak oluşturulmuştur [18]. Bu sistemin güvenliği ve verimliliği RSA'a göre daha yukarılardadır.

Modern şifreleme yöntemleri, yukarıdaki kısa sunumdan anlaşılacağı gibi, sayılar teorisine dayanmaktadır. Enigma ise çoklu alfabe kullanılarak karakter (harf) yer değiştirmesi işlemine dayanmaktadır. Enigma'da rotorların mümkün olan her bir pencere pozisyonu için bir alfabe mevcuttur ki toplamda bu, belirli bir rotor seçimi ve sıralaması için, 17,576 değişik alfabeyi içerir. Rotor seçimi (3/5) ve sıralamasını da hesaba katarsak, bu rakam daha da yükselmektedir. Buna rağmen bu rakamlar bugünkü şifreleme yöntemlerinin güvenliği yanında oldukça kolay kalırlar. Yeni yöntemler sayılar teorisinin sonsuz uzayının modern bilgisayarlarca ulaşılamaz kısımlarına doğru kaymaktadır.

Şifreleme ve deşifrelemede matematiksel yöntemler kadar, elektronik ve diğer yöntemlerin de önem taşıdığını ifade etmiştik. Şifreleme ve deşifreleme sadece matematiksel yöntemlerin yanında prosedürel ve kültürel, davranışsal elemanları da hesaba almak zorundadır. Şifreleme ve deşifrelemenin başarısında bunun önemi vardır. Şifreleme ve deşifreleme bugün tarihte olduğundan çok daha önemlidir. Sivil amaçlar yanında askeri iletişim, kimlik be-

lirleme, güdümlü silah sistemlerinin kontrolü, bilgiye ulaşım ve bilgi güvenliği gibi konular da şifrelemenin uygulama bulduğu önemli alanlardır.

Sonuç

Enigma ile 1918 yılında başlayan elektronik ve matematik temelli kriptolojik sistemler İkinci Dünya Savaşı ile birlikte savaşın kaderini etkileyebilecek kadar önemli hale gelmişlerdir. Bilgisayar ve bilgisayar temelli iletişimin yaygınlaşması, internet üzerinden gerçekleştirilen finansal ve ticari işlemler, dijital imzanın kullanımına yönelik yeni kanunlar kriptolojinin önemini daha da artırmıştır. Bilginin en önemli değer katkılarından birisi olduğu modern dünyada kriptolojik çalışmaların ihmal edilebilirliği mümkün değildir.

Enigma konusu modern zamanlar için derslerle doludur. Bu çalışmamız ile ortaya konduğu gibi hiçbir şifreleme metodu yeteri kadar güvenli değildir. Uygulanan metotların başarısı matematik ve elektroniğe olduğu kadar, insan faktörüne ve uygulanan prosedürlerin başarısına da bağlıdır. Enigma'dan bu yana çok çok daha sofistike kriptolojik yöntemler oluşturulmuştur; hatta kuantum fiziği bile bu amaçla kullanılmaya başlanmıştır. Buna rağmen, Enigma ile başlayan kriptoloji yolunda insanlık henüz başlangıçtadır.

Bilgisayarların yaygınlaşması ve iletişimin günlük yaşantımızın neredeyse hissetmediğimiz ölçü-

de içinde olması sonucu, bilgi güvenliğinde şifreleme yanında, bilgisayar virüsleri, truva atları, klavye dinleyicileri gibi casus yazılımlarında son derece önemli rol oynadığına şüphe yoktur. Modern bilgi güvenliği çalışmaları bu faktörleri de içine almalıdır.

Öte yandan kriptolojik yöntemlerin oldukça yaygın uygulanabilir olmasının başka sonuçları da olacaktır. Örneğin çok basit bir program yüklemesi yapılarak bir telsizin, cep telefonunun veya karasal bir telefonun dinlenmesi neredeyse imkânsız hale getirilebilir. Elektronik dökümanların şifrelenmesi de benzer şekilde yaygın ve kolaydır. Bilgiyi, bilinen kriptolojik yöntemlerle, şifreleri bilmeyen birisi için hiç ortaya çıkmayacak şekilde tamamen gizlemek mümkündür. Bu da, zamanımızın sorunu terör ve mafya ile mücadeleyi devlet için ciddi ölçüde zorlaştıracaktır.

Önümüzdeki yıllar kırılması çok daha zor matematik ve elektronik temelli kriptolojik sistemlerin geliştirilmesine uygun bir ortam yaratacaktır. Umarız ki kitabımız bu yönde bir ilgi uyandırmıştır.

3 Nisan 2008 Perşembe
Ataşehir

Referanslar

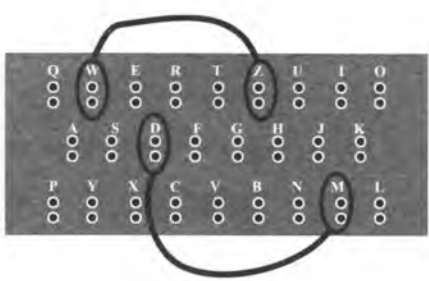
1. The Odyssey, Homer, Çeviri: R. Fitzgerald, 1961 (Vintage Classics, 1990).
2. Histories, Herodotus, Çeviri: Aubrey de Selincourt, 1954, Penguin Books
3. http://www.codesandciphers.org.uk
4. http://www.avoca.ndirect.co.uk/enigma/index.html
5. http://en.wikipedia.org/wiki/Rejewski
6. http://www.nsa.gov/publications/publi00016.cfm
7. http://www.hut-six.co.uk/
8. http://en.wikipedia.org/wiki/Fjalka
9. http://w1tp.com/enigma/imcpue.htm
10. http://tr.wikipedia.org/wiki/K%C4%B1br%C4%B1s_Bar%C4%B1%C5%9F_harekât%C4%B1
11. http://en.wikipedia.org/wiki/Code_talker
12. İlk Türkçe Şifreleme Kitapları, Haluk Oral, Matematik Dünyası, 2003 kış, sf. 59-60
13. Polybius Şifresi, Ali Eskici, Matematik Dünyası, 2004 yaz, sf. 72-73
14. http://en.wikipedia.org/wiki/Caesar_cipher
15. Galois Theory, Emil Artin, Dover Publications, 1998, Mineola, NY, USA
16. The Equation That Couldn't Be Solved, Mario Livio, Simon & Schuster, 2006.
17. Applied Cryptography, Bruce Schneier, John Wiley & Sons, 1996
18. Cryptography and Network Security, William Stallings, Prentice Hall, 2006
19. A Course in Number Theory And Cryptography, Neal Koblitz, Springer Verlag, 1994
20. Elementary Number Theory, Charles vanden Lynden, McGraw-Hill, 2001

21. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir, and L. Adelman, Communications of the ACM, February 1978
22. New Directions in Cryptography, W. Diffie, M. E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976
23. http://en.wikipedia.org/wiki/Enigma_rotor_details
24. Turing's Treatise on Enigma, http://frode.home.cern.ch/frode/crypto/Turing/
25. http://users.telenet.be/d.rijmenants/en/enigmaproc.htm
26. http://www.ellsbury.com/enigmabombe.htm
27. http://en.wikipedia.org/wiki/Arthur_Scherbius
28. Enigma The Battle For The Code, Hugh Sebag-Montefiore, Weidenfeld and Nicolson, London, 2000
29. Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS) 46-2, http://www.itl.nist.gov/fipspubs/fip46-2.htm , 30 Dec. 1993.
30. Türk Alfabesindeki Harflerin Kullanım Sıklığı, http://tr.wikipedia.org/wiki/T%C3%BCrk_alfabesindeki_harflerin_kullan%C4%B1m_s%C4%B1kl%C4%B1klar%C4%B1
31. Cryptography and Computer Privacy, H. Feistel, Scientific American, May 1973, Vol. 228, No 5, pp. 15-23 (http://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/index.html)

Ekler
Ek-1: Ön-Bağlantı Paneli

Ön panelde harfler rotorlara girmeden evvel bir ön bağlantıyla çifter çifter birbirine bağlanabiliyordu. Bu da Enigma operatörüne sağlanan özel kablolarla gerçekleştiriliyordu. Ancak ön panelde birbirine bağlanmayan harfler de bulunuyordu. Gerçekte ön-panel bağlantısı hiç yapılmazsa tüm harfler bir ön değiştirme yapılmadan da sistem çalışıyordu.

Ön panel bağlantısı şöyle çalışıyordu. 26 harften seçilen sayıda çift birbirine kablo ile bağlanıyordu. Örneğin W harfi Z harfine bağlandığında Enigma operatörü W tuşuna basınca aslında sağ (ilk) rotora iletilen harf W yerine Z oluyordu. Tersine bakıldığında da aynı durum işliyordu. Rotor mekanizması bir harfi kodladığında Z harfini üretiyorsa, ön



Ön-Bağlantı Paneli

panel bağlantısı bunu da W'ye çevirerek ışıklı panoya yansıtıyordu.

Şimdi bunun sistemin karmaşıklığına olan etkisini görelim. Enigma ön panelinde toplam 26 harf vardı. Buna n dersek, n = 26. Enigma operatörleri en fazla 10 kablo kullanarak harfleri çifter olarak birbirine bağlayabiliyordu (standart Enigma kutusunda en fazla 10 yedek kablo sağlanmıştı).

Şimdi p kablo sayısını göstersin. Ön panelde bağlantı yapılmak mecburiyeti olmadığı için p'nin en küçük değeri 0 (sıfır) en büyük değeri ise 13 (on üç) olabilirdi.

Şimdi p'nin bir olduğunu varsayalım, yani elimizde tek bir kablo bulunsun. Bunun bir ucunu sokabileceğimiz 26 delik mevcuttur. Kablonun iki ucunu da aynı deliğe sokmak mümkün olmadığından diğer ucun girebileceği 25 delik kalmıştır. Böylece ilk kabloyu bu şekilde yerleştirmek için toplam olasılık sayısı 26 x 25 olmaktadır.

Ancak biraz dikkatli bir analizle bu sayının içinde bazı tekrarların olduğunu görebiliriz. Örneğin ilk ucu A'ya bağladığımızda ikinci ucu B'ye bağlarsak ortaya AB bağlantısı çıkar. Eğer ilk ucu B'ye bağlayıp ikinci ucu A'ya bağlarsak ortaya çıkan bağlantı BA yani yine AB olur (çünkü AB = BA) . Burada her bir çiftin iki kez ortaya çıktığını görebiliriz. Yani aslında geçerli olasılık sayısı 26 x 25 / 2 olmaktadır.

Şimdi iki kablo aldığımızı varsayalım. İlk kabloyu 26 deliğe yerleştirme durumunu yukarıda he-

saplamıştık. İkinci kabloyu yerleştirmeye başladığımızda tek fark 24 deliğin kalmış olmasıdır. Böylece toplam olasılık sayısı (26 x 25)/2 x (24 x 23)/2 olacaktır. Ancak dikkatle baktığımızda burada da tekrarların olduğunu görürüz. Örneğin birinci kablo AB'yi bağlıyorsa, ikinci kablo CD'yi bağlıyorsa, bu birinci kablonun CD'yi bağlaması ve ikinci kablonun AB'yi bağlaması durumuna eşdeğerdir. Bu fazlalıklardan da elimizde her bir çift için tam olarak 2 tane bulunduğundan gerçekten geçerli bağlantı sayısı (26 x 25)/2 x (24 x 23)/2 x 1/2 olacaktır.

Şimdi elimizde üç tane kablo olduğunu varsayalım. Burada da ilk iki kablo yukarıdaki gibi yerleştirilecek ve üçüncü kabloya sıra geldiğinde 26 delik yerine 22 delik kalmış olacaktır. Böylece ortaya çıkan rakam (26 x 25)/2 x (24 x 23)/2 x (22 x 21)/2 olacaktır. Ancak dikkatli bir analizle burada da tekrarların olduğunu görürüz. Örneğin ilk kablo AB, ikinci kablo CD, üçüncü kablo EF bağlantılarını yapmış olsun. Bu durum ilk kablonun CD, ikincinin AB üçüncünün ise EF kablolarını bağlamasıyla eşdeğerdir. Bu üç çiftin bu şekilde alabileceği değerlerin toplam sayısı 3 x 2 x 1 olur. Bu da (3!) p! sayısına eşittir.

Bu şekilde p'nin değerlerini artırdığımızda önümüze bir formülün belirmeye başladığını görürüz. n = 26 ve p kablo sayısını gösterdiğinde toplam ortaya çıkan olasılık sayısı;

$n!/(n-2p)!p!2^p$

Toplam olasılık sayısı ise sıfırdan (0), on (10) a kadar olan p değerleri için hesaplanacak sonuçların toplamı olur. Örneğin 10 kablo için ($p = 10$) bu rakam 150 trilyondan daha büyük olur. Böylece Enigma şifrelerinin sadece deneme-yanılma yolu ile kırılması ihtimali tamamen ortadan kaldırılmıştır.

Ek-2: Enigma Rotorlarının Matris ile Modellenmesi

Kolaylık için modellemek istediğimiz rotorun sadece 6 girişi ve çıkışı olsun. RI ve RII diye adlandıracağımız bu rotorların giriş çıkış bağlantıları

RI

ABCDEF

CDBFAE ve

	A	*B*	*C*	*D*	*E*	*F*
A					1	
B			1			
C	1					
D		1				
E						1
F				1		

RII

ABCDEF

DEFBCA ve

	A	*B*	*C*	*D*	*E*	*F*
A						1
B				1		
C					1	
D	1					
E		1				
F			1			

Klavye girişini ise tek satırlık KL = [A B C D E F] ile gösterelim. RI girişine KL uygulursak RI Klavyeyi çıkışına KL1 = [C D B F A E] olarak transfer edecektir (KL x RI). Ortaya çıkan sonuç matrisi RII ile çarparsak elde edeceğimiz sonuç KL2 = [F A E D B C] olur. Şimdi önce RI ile RI-I'yi çarparak (RI x RII)

	A	*B*	*C*	*D*	*E*	*F*
A		1				
B					1	
C						1
D				1		
E			1			
F	1					

elde ederiz. [Eğer KL x (RI x RII) hesaplanırsa sonuç [F A E D B C] olur ki bu da KL2'ye eşit olur. Yani her iki durumda da elde edilen alfabeler aynı olur.

Yansıtıcıdan dönerken rotorların matris modelleri, orijinal rotor matrisinin transpozesi olur. Yansıtıcı ise ayrı bir matris olarak modellenir.

Enigma matris modeli

KL x SR x OR x LR x YA x SR^T x OR^T x LR^T

SR: Sağ Rotor, OR: Orta Rotor, LR: Sol Rotor, YA: Yansıtıcı

Pencere pozisyonu olarak belirlenecek bir kolon alınabilir. Her matris serisinin çarpılmasından bir alfabe elde edilir. Her çarpmadan sonra matrislerin

Enigma çalışma modeline göre rotasyona uğratılması gerekir. Bunun için SR matrisinin bir kolonunun sola kaydırılması, ilk kolonun ise matrisinin sağ kolonu haline getirilmesi gerekir. SR'nin her bir tam rotasyonu OR'de, OR'nin de tam rotasyonu LR'de bir rotasyonu tetiklemesi gerekmektedir. Matris transpozeleri de benzer şekilde ayarlanmalıdır.

İkinci Dünya Savaşı süresince kıtalara yayılmış olan birlikler, okyanuslarda dolaşan denizaltılar ve su üstü gemileri, komuta merkezleri ve birbirleri ile iletişmek ve koordine olmak zorunda idiler.

Birinci Dünya Savaşı'nda yenilgiyi tatmış olan Alman orduları buna hazırlıklıydılar. Tüm ordu birimleri arasındaki bilgi iletişimini güvenle sağlayacak olan şifreleme teknolojisi "Enigma", çoktan geliştirilmiş ve kullanıma alınmıştı. Almanların makinelerine olan güvenleri tamdı.

Enigma şifrelerinin düşmanları tarafından kırılmasının mümkün olmadığına inanıyorlardı.

Oysa İngilizler, savaştan neredeyse otuz yıl sonra, savaş sırasında Enigma şifrelerini kırdıklarını ve bu başarının savaşı kazanmalarında en büyük etkenlerden biri olduğunu iddia edeceklerdi.

Süleyman Sevinç, *Enigma* adlı bu eserinde, Almanların savaş boyunca kullandıkları şifreleri ve İngilizlerin bu şifreleri kırma çabalarını açık bir dille anlatıyor.

Enigma bu çalışmalara ışık tutan ilk Türkçe yayındır.

ISBN 978-975-403-504-9

Fiyatı: **4,5** TL (KDV dahil)

Basılı fiyatından farklı satılamaz