ROSETTA TAŞI

M.Ö. 3500-2000 döneminde çok az insan okur yazar olduğu için, yazı kendiliğinden şifreli metin niteliği kazanmaktaydı. 1798 yılında Mısır'da bulunan Rosetta taşı üzerinde üç ayrı metin grubu bulunmaktaydı. Bu gruplardan ilki, Mısır halkının kullandığı Demotik* dili, ikincisi yüzlerce sembolden oluşan Hiyeroglif yazısı ve üçüncüsü okunabilir durumda olan Antik Yunan yazısıydı. Araştırmacılar, bu üç grubun aynı anlamı içereceği varsayımı ile çalışmalara başladılar. 1822 yılında, eski Mısır yazılarının güncel Koptik** diline benzediğini ortaya koyan araştırmacı Jean-François Champollion Demotik ve Hiyeroglif diline ilişkin çözümlemeleri gerçekleştirdi.

*Demotik: Çizimlerin Hiyeroglif'e göre daha basit olduğu demotik (Yunanca demos - halk kelimesinden gelir) günlük yazışmalarda halk tarafından kullanılmıştır.
**Koptik: Hıristiyan Mısırlıların (Kıpti) Yunan alfabesine yaptıkları 6 harflik ekle oluşan yazı dilidir ve Kıpti kilisesi tarafından hâlâ kullanılmaktadır.

wikimedia.org

Elektronik Çağ Öncesi Dönem

kriptoloji tarihi

Mustafa Ümit ÇEŞMECİ

Günümüzde yaygın olarak kullanılan ve kullanım alanları gün geçtikçe genişleyen kripto tekniklerinin temelleri, M.Ö. 2000'li yıllara kadar uzanır. Mısır yazıtlarında rastlanan kriptografik ögeler, kriptoloji tarihinin ilk kayıtlarını oluşturmaktadır.

Nil Nehri yakınlarındaki "Menet Khufu" kasabasında bulunan hiyerogliflerin şifreleri çözüldüğünde, bazı yazılarda daha önce hiç kullanılmamış olan simgelerin kullanılmış olduğu görülmüştür. Bu simgelerin, sadece ilgili kişi tarafından anlaşılabilir olduğu ve bu kişi dışındakiler tarafından anlaşılmaması için kodlandığı sonucuna varılmıştır. Bunun da bilgi güvenliği sağlamak üzere uygulanmış bir kriptolama tekniği olduğu kabul edilmektedir.

O yıllarda kriptoloji sadece diplomatik ve askeri alanlarda kullanılmıştır ve kripto kırma faaliyetleri yok denecek kadar azdır.

Mezopotamya'da, M.Ö. 1500'lü yıllarda kripto kullanıldığı tespit edilmiştir. Bölgede bulunan tabletler üzerindeki şekillerin çözümlenmesinden sonra çivi yazısı anlaşılabilir duruma gelmiştir. Bununla birlikte, bazı metinlerin aynı yöntemler uygulanarak okunamadığı görülmüştür. Daha sonra yapılan kriptolojik analizler sonrasında okunamayan metinlerden birinin, çömlek yapımı için geliştirilmiş olan bir bileşimin şifreli olarak kaydını içerdiği anlaşılmıştır.

M.Ö. 457 yılına gelindiğinde, Anadolu'da Ispartalılar tarafından Scytale olarak adlandırılan kriptolama tekniğinin kullanıldığını görüyoruz. Şerit şeklindeki kağıdın belirli çaptaki bir silindire sarılarak yazının bu şekilde oluşturulan sayfaya yazılması biçiminde özetlenebilecek bu teknik ile, sırası karışık olan harfler-simgeler içeren bir şerit elde edilmekteydi. Bu şerit üzerindeki yazının okunabilmesi için, yazımında kullanılan çapta bir silindire sarılması gerekmekteydi. Bu silindirin aynısı, mesajın gönderileceği kişide bulunmaktaydı. (Günümüzdeki modern kripto tekniklerine bir benzetme yapılacak olursa, silindirin çap değeri kripto anahtarına karşılık gelmektedir.)

Scytale Tekniği.

Roma İmparatorluğu döneminde kriptoloji oldukça gelişmiş ve simgeler üzerinde belirli işlemler kullanılmaya başlanmıştır. M.Ö. 100 yılında doğmuş olan Jül Sezar generallerine gönderdiği mesajlarda, her harfin alfabede kendisinden sonra gelen üçüncü harfle yer değiştirdiği bir kriptolama tekniği uygulamıştır. General Agustus da benzer biçimde, "bir sonraki harfle yer değiştirme" kriptosu kullanmıştır.

Sabit anahtarlı ve güvenliği düşük olan bu yöntem, düşman tarafından bilinmediği için yeterli düzeyde güvenlik sağlamıştır. (Günümüz kriptoanaliz tekniklerinden "Geçiş Sıklığı Analizi" yöntemiyle bu tipte sabit anahtarlı bir şifrelemenin çözülmesi son derece kolaydır.)

Roma döneminde ayrıca steganografi de kullanılmıştır. Gönderilecek olan mesaj, saçları kazıtılmış bir kölenin kafasına kolayca silinmeyecek bir madde (mesela kına) ile yazılmakta ve köle saçları uzadıktan sonra karşı tarafa gönderilmekte, karşı taraf ise kölenin saçlarını kazıyarak mesajı okumaktaydı. Bu yöntemde bilginin güvenliği, uygulamanın düşman tarafından bilinmediği varsayımına dayanmaktadır.

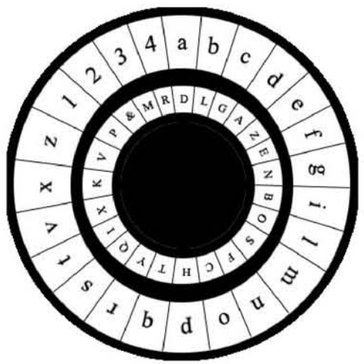
Arap filozof Al-Kindî, modern kriptolojinin temellerini oluşturmuştur

Resim:Al-Kindi.

Mesaj gizleme ve çözme yöntemlerine dair zamanımıza ulaşan en eski eser, filozof Al-Kindî'nin (Doğumu: 801 – Ölümü: 873) Risâle fi'stihrâci'l-mu'ammâ'sıdır. Kriptografinin iki temel yöntemi olan "yerine koyma" ve "yer değiştirme" işlemlerini ilk defa tanımlayan ve bu ikisinin birlikte kullanıldığı karma şifreleme sistemlerini tarif eden Kindî'dir. Şifrelerin çözülmesine ilişkin olarak harflerin kullanılma sıklığının istatistiği ve analizi, kelimelerde bir araya gelen ve gelemeyen harflerin analizi, hitabe ve mektupların başlangıç kısımlarında yer alan muhtemel kelimelerin oluşturduğu zayıflıkların değerlendirilmesi gibi kriptografinin temel esasları yine Kindî tarafından ortaya konmuştur. Al- Kindî ile karşılaştırılabilir seviyedeki batılı bilginlerden Leon Battista Alberti 1466 yılında ve Trithemius 1508 yılında yazılı eserler vermiştir. Al-Kindî ile bu bilim adamları arasındaki yüzyıllar seviyesindeki fark, Arap dünyasının kriptoloji konusundaki öncü rolünü ortaya çıkartmaktadır.

Diğer bir Arap bilgini Abdurrahman el-Halil ibn-Ahmet, M.S. 8. yüzyılda "Kitab-ül Muamma" adlı kriptoanaliz kitabını yazmıştır. Abdullah Kelkeşandi de 15. yüzyılda kriptoanaliz çalışmaları yürütmüş olan bir Arap matematikçidir.

1404–1472 yılları arasında yaşamış olan Leon Alberti, 1466-1467 yılları arasında ilk kez çoklu alfabe kullanarak kriptolama yapmıştır. Bu yöntemde, Sezar şifreleme yöntemine benzer olarak harf kaydırma tekniği uygulanıyordu. Sezar şifrelemeden farklı olarak kaydırma miktarı sabit olmayıp, kullanıcının kararına göre belirleniyordu. Kriptolanacak metinde her harfin kriptolu



Alberti Diski.

karşılığı, Alberti Diski yardımıyla bulunuyordu. İçteki çemberi sabit, dıştaki çemberi onun etrafında dönebilen bu disk yardımıyla, her harfin istenilen miktarda ötelenmiş hali kolaylıkla görülebiliyordu.

Blaise de Vigenère, 1586 yılında Sezar kripto sisteminin bir türevi olan "Vigenère Sistemi" ni geliştirdi. Bu sistemde, şifrelenecek olan karakter Sezar kripto sisteminde olduğu gibi tüm metin boyunca sabit bir miktarda değil, periyodik olarak değişen bir sayı dizisine göre öteleniyordu. Sözgelimi kullanılan şifreleme sayı dizisi 183725 ise, kriptolanacak verinin ilk harfi 1, ikinci harfi 8, üçüncü harfi 3 ve benzer şekilde altıncı harfi 5 karakter öteleniyordu. Yedinci karakter ise tekrar 1 kez ötelenerek, bu kural metnin tamamı şifrelenene dek uygulanıyordu.

Vigenère sistemiyle şifreleme yaparken kolaylık sağlamak üzere "Vigenère Tablosu" kullanılmaktaydı.

Vigenère şifresi 1800'lü yılların ortalarına kadar "kırılması imkansız" olarak nitelendirildi. Charles Babbage, 1854 yılında anahtar uzunluğuna dayalı frekans analizi uygulayarak bu şifreyi kırmayı başardı ve 1864 yılında "Gizli Yazma ve Şifre Çözme Sanatı" adlı kitabında bu yöntemi yayınladı. Kasiski de 1863 yılında Babbage'dan bağımsız olarak aynı saldırı yöntemini geliştirmişti.

1860'lı yıllardaki Amerikan İç Savaşı'nda Güneyliler Vigenère şifreleme yöntemini kullanmışlardır. Yöntemin kırılmazlık lakabına çok güvenerek sadece 3 farklı anahtar kullanmaları, Kuzeyli kriptoanalizcilerin işini kolaylaştırmış

ve kriptolu metinlerin kolaylıkla kırılabilmesini sağlamıştır. 620 bin kişinin öldüğü savaşı Kuzeylilerin kazanmasında kriptoanaliz faaliyetlerinin de önemli bir payı bulunmaktadır.

Friedman bu tipteki ötelemeli şifreleme sistemlerinin analizini yapmak üzere 1925'te bir test geliştirdi. Kendi adıyla tanınan bu test, şifreli metindeki iki harfin açık metindeki aynı karakterden gelme olasılığını irdelemek üzerine kurulmuştu.

Vernam, Vigenère şifreleme sistemini temel alarak, kendi adıyla anılan şifreleme sistemini geliştirdi. Vigenère sisteminde kullanılan periyodik sayı dizisinin periyodunu sonsuza götürmeyi önerdi. Bu durumda, kriptolanacak karakterin kaç kez öteleneceğini belirleyen sayı dizisi kriptolanacak metnin içerdiği karakter kadar sayı içeriyordu. Diğer bir deyişle, her karakter kendisi için özel olan bir sayı kadar öteleniyordu ve bu sayı tekrar kullanılmıyordu. Bu şekilde ortaya çıkan Vernam şifresinin kırılması teorik olarak imkansızdır. Bununla birlikte, uygulanması oldukça zor bir yöntemdir; çünkü, her mesajı şifrelemek veya şifresini çözmek için mesaj uzunluğunda şifreleme dizisinin karşı tarafa iletilmesini zorunlu kılmaktadır.

Kriptoanalistlerin çalışmaları 1876 ABD Başkanlık Seçimlerinin sonucunu etkilemiştir.

Rutherford Hayes ve Samuel Tilden'in aday oldukları 1876 Amerika Birleşik Devletleri başkanlık seçimlerinde, 4 eyaletin seçim sonuçlarında anlaşmazlık yaşanmıştır. Hayes taraftarlarının, Tilden'in hile yaptığını öne sürmesi üzerine araştırma başlatılmıştır. Tilden taraftarlarının birbirlerine gönderdikleri şifreli mesajlar ortaya çıkartılmış, kriptoanalistlerin yaptıkları incelemeler sonunda, gerçek mesajdaki kelimeler yerine farklı kelimeler kullanılarak bir bilgi gizleme tekniği uygulandığı anlaşılmıştır. Sözgelimi, "Hayes" kelimesi yerine "Copenhagen", "Votes" yerine "Rochester", "Tilden" yerine "Russia" vb. kelimeler kullanıldığı tespit edilmiştir. Gerçekleştirilen kriptoanaliz faaliyetleri sonrasında, seçim komisyonu Tilden taraftarlarının hile yaptığına hükmederek 4 eyaletin yönetimini de Hayes'e vermiştir.

Birinci Dünya Savaşı yıllarında telsiz haberleşmesinin icadı ile kriptolojinin önemi çok artmıştır. Telsiz haberleşmesinin doğası gereği, iletilen mesajların sadece gönderildiği kişi tarafından değil, radyo dalgalarını alabilen herkes tarafından dinlenebilmesi söz konusudur. Bu nedenle telsiz haberleşmesinde bilgi güvenliğini sağlamak üzere yeni teknikler geliştirilmesi zorunlu hale gelmiştir.

Birinci Dünya Savaşı'nda Almanlar, ADFGVX olarak adlandırdıkları sistemleri ve "Kod Kitabı" yöntemini kullanmışlardır.

SEZAR ŞİFRELEME YÖNTEMİ

Şifreleme yönteminin gizliliği esasına dayanan Sezar Şifrelemesi, yöntemin bilinmesi durumunda çok basit bir biçimde kağıt kalem yardımıyla çözülebilir. Sezar'ın kullandığı öteleme miktarı farklı olsaydı da şifre kolaylıkla çözülebilirdi.

Bunu bir örnekle açıklayalım:

ŞİFRELEME :

Metin Alfabesi : **A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z**
Üç Harf İleri Şifre Alfabesi : **Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z A B C**

Açık Metin : HEMEN GERİ ÇEKİLİN
Şifreli Metin : JĞÖĞP IĞTL FĞNLOLP

ŞİFRENİN ÇÖZÜLMESİ:

Yöntem basitçe, tüm harf kaydırma olasılıklarının denenmesi olarak tanımlanabilir. 29 harften oluşan Türkçe dili için en fazla 28 deneme yapılarak şifre kırılabilir.

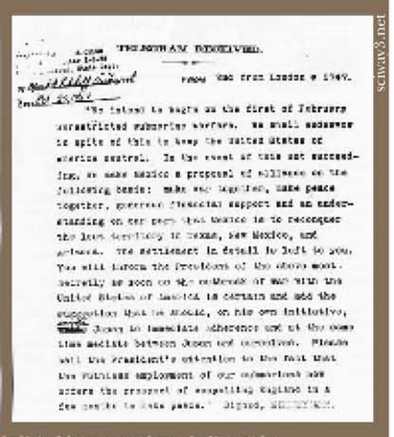
Şifreli Metin : JĞÖĞP IĞTL FĞNLOLP
1 Harf Denemesi : İGOGÖ HGŞK EGMKNKÖ
- Metin anlamlı değil, sonraki adıma geç.

2 Harf Denemesi : IFNFO ĞFSJ DFLJMJO
- Metin anlamlı değil, sonraki adıma geç.

3 Harf Denemesi : HEMEN GERİ ÇEKİLİN
- Metin anlamlı, şifre kırılmıştır.

Tesadüfen birden çok anlamlı metin bulunması düşük bir olasılıktır ve bu olasılık mesaj boyu arttıkça azalmaktadır.

archives.gov



schwabs.net

Zimmermann Telgrafı , şifreli (solda) ve çözülmüş hali (sağda).

İngiliz işaret toplama birimleri elde ettikleri Zimmerman telgrafının kodunu çözerek, mesajın Almanların Meksika'daki elçiliklerine gönderilmiş olduğunu; Meksika'nın ABD'ye savaş ilan etmesi durumunda kendilerine gereken yardımın yapılacağı ve savaş sonrasında Teksas, Arizona gibi eyaletlerin Meksika'ya bırakılacağı güvencesinin verildiğini ortaya çıkarttı. Bu tehdidi öğrenen ABD de Almanya'ya karşı savaşa girdi.

Bu yöntemde, şifrelenecek metindeki her kelimeye karşılık bir sayı grubu kullanılmaktaydı. Örneğin, Zimmermann telgrafı olarak bilinen mesajda "Februar" kelimesi 13605, "fest" kelimesi 13732, "finanzielle" kelimesi 13850 sayıları ile kodlanıyordu.

Kriptoanalistler İkinci Dünya Savaşı'nın Yönünü Belirlemiştir

İkinci Dünya Savaşı'nın yaklaştığı yıllarda ülkeler bilgi güvenliği ve kriptolojinin önemini idrak etmiş durumdaydılar. ABD tüm birliklerindeki kripto birimlerini yeniden yapılandırdı. İşaret istihbarat servislerine yoğun kaynak aktarıldı. Donanmada ilgili birimlere kriptoloji konusunda üst düzeyde dersler açıldı. Kriptoloji ve kriptoanaliz konusunda büyük bir bilgi birikimi elde edildi. Almanya ise, Adolf Hitler liderliğinde hızlı bir silahlanma sürecine girmişti. Çevre ülkelere karşı ırkçı ve saldırgan bir politika takip ediliyordu. 1923 başında Alman donanmasının kullanmaya başladığı Enigma şifreleme cihazı, 1930'lu yılların ortasında, ordunun temel bilgi güvenliği cihazı olarak tescil edildi.

ilord.com

Enigma, Alman General Panzer'in muhabere birliği tarafından kullanılıyor.

wyborcza.pl

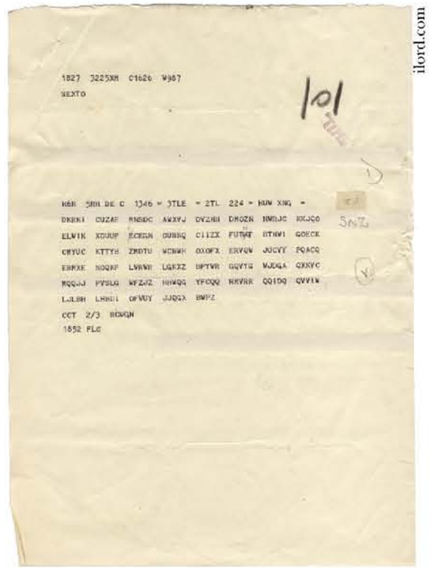
Rejewski, Rozycki ve Zygalski beraber- Rejewski soldan 1., Zygalski soldan 4., Rozycki soldan 6.

Alman ordusu muhabere birimlerindeki görevliler gönderilecek olan mesajı Enigma cihazının tuş takımı üzerinden yazıyor, mesaj cihaz içerisinde şifreleniyor ve elde edilen şifreli mesaj telsiz operatörü tarafından mors kodu kullanılarak, radyo dalgaları ile karşı tarafa gönderiliyordu. Enigma, mekanik ayarlarla yönlendirilen elektronik bir cihazdı. 1918 yılında Arthur Scherbius tarafından ticari uygulamalarda kullanılmak üzere geliştirilmiş ve ilk olarak bankalar arasındaki haberleşmede kullanılmıştı. Alman ordusunun Enigma'yı kullanma kararı sonrasında, İkinci Dünya Savaşı süresince toplam yüzbin kadar Enigma kripto cihazı üretilmiştir. Enigma kripto cihazı, 21. yüzyıla kadar en yüksek miktarda üretilen kripto cihazı olma özelliğini korumuştur.

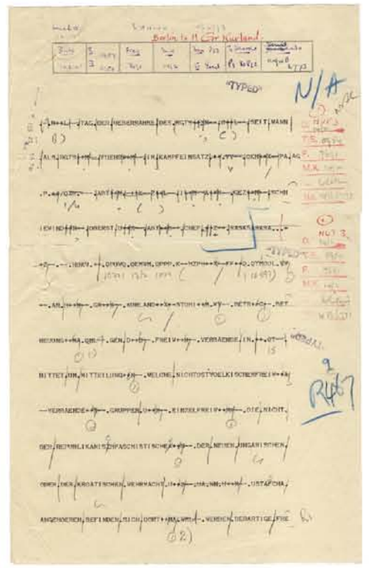
Almanya ile savaşın kaçınılmaz olduğunu anlayan İngiltere, hazırlıklara hız verdi. Silahlanma çalışmaları ile birlikte istihbarat çalışmalarına da önemli miktarda kaynak ayırdı.

Fransa ve müttefiki Polonya'nın endişeleri, Almanya'ya coğrafi yakınlıkları nedeniyle İngiltere'ninkinden daha fazlaydı ve çalışmalara daha erken başlamışlardı. Polonya, istihbaratın

önemini göz önünde bulundurarak BS4 adlı bir şifre kırma ekibi oluşturdu. Ekibin başında Henryk Zygalski, Jerzy Rozycki ve Marian Rejewski vardı. Ekip, Alman ordusunda kullanıldığını bildikleri ticari Enigma cihazının şifrelerini çözecek bir yöntem geliştirmek üzere çalışmalara başladı. Rejewski, "rotor" adı verilen ve metni şifrelemede kullanılan anahtarın bir bölümünü oluşturan tekerleklerin türünü belirleyen matematiksel bir yöntem geliştirdi. Fakat yine de mesajlar çözülemedi, çünkü rotorların içindeki tellerin birbirlerine bağlantı noktaları bilinmiyordu. Bu çözümsüzlük sürerken Polonyalılar hiç beklemedikleri bir kaynaktan bilgi aldılar. Alman ordusundaki bir kripto biriminde bulunan casus Hans Thilo Schmidt (kod adı Aşe), rotor parçaları dahil Enigma cihazının tüm parçaları ile ilgili bilgi sağladı. Casus, zengin bir hayat sağlayacak kadar bol miktarda para ile kandırılmıştı. Cihazın kullanım kılavuzu da alman dokümanlar arasındaydı. Rejewski iç tel sistemini öğrendikten sonra, kullanım kılavuzundaki bilgileri de değerlendirerek ticari Enigma şifrelerini çözecek yöntemi geliştirdi. Enigma ile şifrelenmiş mesajlar çözülebilir oldu.

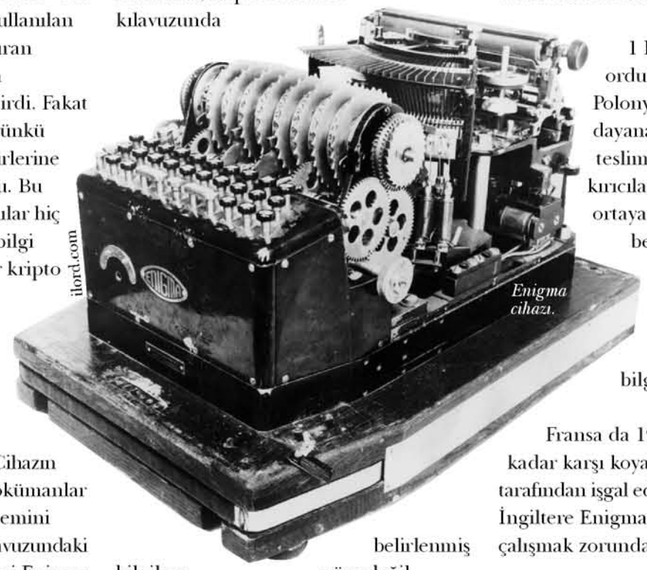


ilord.com



Enigma mesajı , şifreli (solda) ve çözülmüş hali (sağda).

Almanlar da bu arada şifre yöntemlerini geliştiriyorlardı. 1938 Eylül ayında birliklere, Enigma'nın şifreleme anahtarının bir kısmını oluşturan rotorların, kripto kullanım kılavuzunda belirlenmiş bilgilere göre değil, rasgele değerlere göre ayarlanması emri verildi. Cihazlara fazladan rotor ekleyerek ticari Enigma'dan daha güvenli bir Enigma oluşturdular. Bu noktadan sonra Polonyalılar elde ettikleri şifreli Enigma mesajlarını çözemediler. Bunun üzerine, Fransızlardan yardım istediler.



ilord.com

Enigma cihazı.

1939 yılı Ocak ayında Polonyalı, Fransız ve İngiliz istihbarat yetkilileri, Alman şifrelerinin kırılması konusunda Paris'te bir toplantı yaptı. Haziran ayında ise Varşova'da ikinci bir toplantı yapıldı ve Polonyalılar Enigma hakkında elde ettikleri bilgileri paylaştılar. İngiliz ve Fransız temsilciler, Polonyalıların yaptıkları başarılı çalışmalar karşısında şaşkınlıklarını gizleyemediler. Polonyalılar İngilizlere, üzerinde çalışmak üzere iki adet Enigma cihazı verdi.

1 Eylül 1939'da Alman orduları Polonya'ya saldırdı. Polonya ancak bir ay dayanabildi ve daha sonra teslim oldu. Polonyalı şifre kırıcılar yaptıkları çalışmaların ortaya çıkmaması için tüm belgeleri yok edip ülke dışına kaçtılar. Yakalananlar ise Almanlara Enigma'yı kırdıkları yönünde bir bilgi vermediler.

Fransa da 1940 yaz ayları başına kadar karşı koyabildiği Alman orduları tarafından işgal edildi. Bu işgal sonrasında İngiltere Enigma üzerinde tek başına çalışmak zorunda kaldı.

İngilizlerin yapması gereken çok iş vardı. Cihazın tüm yapısını ve nasıl çalıştığını bilmek yetmiyordu. Metni şifrelemede kullanılan anahtarın bulunması matematiksel olarak çok zor ve zaman gerektiren bir işlemdi. Savaşın ilerleyen günlerinde, metinleri şifrelemede

kullanılan anahtarlar sekiz saatte bir değiştirilmeye başlanacaktı. Her değişiklikte, kullanılacak olan yeni anahtarın bulunması gerekiyordu.


ilord.com

Bletchley Park.

Fransa'nın da düşmesiyle, haberleşme verisi toplama ve kriptoanaliz faaliyetleri büyük bir ivme kazandı. Fransa, işgalin kaçınılmaz olduğunu anlar anlamaz elindeki Enigma'yı İngiltere'ye, *CESG* ('*Communications-Electronics Security Group*' – Haberleşme-Elektronik Güvenlik Grubu) yardımcı başkanına verdi. Böylece, tüm umutlar İngiliz kriptoanalistlere kalıyordu.

İkinci Dünya Savaşı Süresince 500.000 Alman Mesajı Tasnif Edildi

Enigma haberleşmesi, radyo dalgaları üzerinden Mors kodları kullanılarak yapılıyordu. Uzak mesafeler arasında haberleşme yapıldığı için, gönderilen radyo dalgaları İngiliz Y-Radyo Dinleme Servisi tarafından da kolayca alınabiliyordu. Amerikan malı hassas alıcılar kullanılarak dinlenen kriptolu Mors mesajları operatörler tarafından yazıya geçiriliyordu.

Daha sonra toplanan tüm mesajlar, şifreli mesajların çözülmesi için kurulan ekibin çalıştığı Bletchley Park'a gönderiliyordu. Toplanan mesajlarda sıklıkla eksiklikler ve yanlışlıklar oluşuyordu. Radyo dalgaları üzerindeki parazitler nedeniyle ya da operatör hatası sonucunda anlaşılamayan harflerin yerleri boş bırakılıyordu. Bu mesajlar görünüşte anlamsız, rasgele sayılardı. Fakat kriptoanalistler için ellerindeki temel malzemeyi oluşturuyorlardı. Savaş süresince yüzbinlerce Alman mesajının toplandığı dikkate alınırsa yapılan dinleme faaliyetlerinin ne kadar emek gerektiren bir iş olduğu kolayca anlaşılabilir.

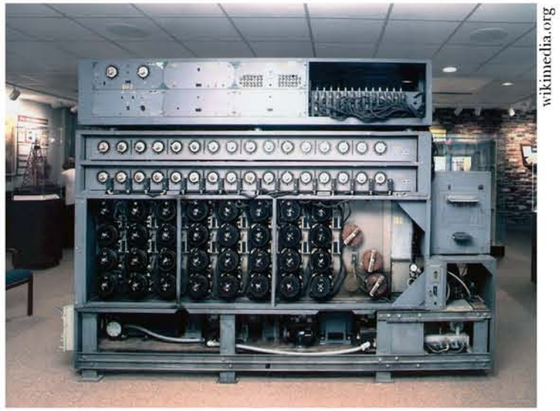

rutherfordjournal.org

Alan Turing.

Bletchley Park'taki kriptoanaliz ekiplerinin başında, bir sivil olan Alfred Laws bulunuyordu. Büyük miktarlarda verinin işlenmesi sistemli bir çalışma gerektiriyordu. Çalışma planlarının oluşturulması, bilgilerin tasnifi gibi eşgüdüm gerektiren konular Gordon Welchman tarafından yönlendiriliyordu. Kurulmuş olan çalışma sistemi, savaşın ilerleyen dönemlerinde personel sayısının onbine çıktığı günlerde son derece yararlı olmuştur. Zamanın altın değerinde olduğu göz önüne alınarak, personelin üç vardiya çalışacağı bir çalışma planı tasarlanmıştır. Onbin personelin üç vardiya çalıştığı bir çalışma grubunun verimli yönetimi, bugün bile oldukça zordur.

Bletchley Park'taki ekipte mükemmel matematikçiler, mühendisler ve satranç oyuncuları bulunuyordu. Satranç oyuncuları da ekibe dahil edilirken, kriptoanaliz faaliyetlerinin bu oyunla benzer şekilde strateji ve sabır gerektirdiği düşünülmüştü. Matematik altyapısı ise işin temelini oluşturuyordu. Ayrıca, matematikçiler tarafından geliştirilen yöntemleri uygulayacak özel cihazları geliştiren mühendisler de çalışmalara önemli destek sağlıyordu.

Bletchley Park'ta çeşitli Alman birimlerinin mesajlarını incelemeye tahsis edilmiş, birimlere özel barakalar bulunmaktaydı. Sözgelimi, Alman donanmasının kullandığı


wikimedia.org

Bombe.

radyo frekanslarından alınan mesajların incelendiği baraka ayrı, kara birliklerinden alınan mesajların incelendiği baraka ayrı, şifresi çözülen mesajlardan elde edilen verilerin sınıflandırıldığı baraka ayrıydı. Bu çalışma grupları arasındaki eşgüdüm, üst düzey yöneticiler tarafından sağlanıyordu.

Alan Turing de Bletchley Park'ta çalışan matematikçilerden biriydi. O yıllarda Cambridge'de dekan konumundaydı. Turing, matematiksel bir model kurarak, "Bombe" adını verdiği elektromekanik bir cihaz geliştirdi. Enigma'nın matematiksel yapısını modelleyen bu cihaz sayesinde, kriptolu mesaj içindeki birbirini izleyen harfler hesaplanabiliyordu. Bombe cihazları kullanılarak, kriptolu Enigma mesajları kırılabildi. Bu anlamda, cihazın kriptoanaliz tarihindeki ilk "Kriptoanalizle Saldırı Bilgisayarı" olduğu söylenebilir.

Savaş süresince İngiliz "Tabulating Machines" şirketi tarafından 211 adet Bombe kriptoanaliz cihazı üretilmiştir. Tonlarca ağırlığı olan bu cihazlardan, ABD firması "National Cash Register" da üretmiştir. Amerikalılar tarafından üretilen cihazlar, İngiliz üretimi cihazlardan fiziksel olarak daha büyüktür, fakat daha hızlı çalışarak daha yüksek işlem gücü sağlamışlardır.

Bu büyük makinalar, bir anlamda modern bilgisayarların ataları olarak kabul edilmektedir.

Enigma mesajlarının çözülebilir olması, çeşitli etkenlerin bir araya gelmesi ile mümkün olmuştur.


cyber-heritage.co.uk

Alman U-Bot Denizaltısı.


wikimedia.org

Pearl Harbor Saldırısı.

Öncelikle, casusluk faaliyetleri sayesinde, Almanların kullandığı Enigma cihazına ait mimarinin ele geçirilmesi işin temelini oluşturmuştur çünkü Enigma cihazının tüm yapısı bilinmeden mesajların çözümü imkansızdır.

Bletchley Park'taki, alanlarında iyi yetişmiş kişiler, sistemli bir çalışma ile yeni kriptoanaliz yöntemleri geliştirebilmiştir. Çalışanların iyi yönetilmesi, başarılı olmalarında son derece önemli bir etken olmuştur. Bu kadrolardaki matematikçilerin, mühendislerin, teknik elemanların ortak çalışmaları ile icat edilen hesaplayıcı cihazlar sayesinde, mesajların çözülebilme süreleri son derece kısalmıştır.

İşaret toplama istasyonlarından sağlanan yüklü miktardaki veri sınıflandırılarak, Enigma cihazına ilişkin istatistiksel veriler elde edilmiştir. Bu veriler de, Enigma cihazında gerçeklenen kriptolama yönteminin zayıflıklarına ışık tutmuştur. Kriptolama yönteminde yapısal zayıflıklar olmasaydı, mesajların çözülmesi söz konusu olamazdı. Bunların ötesinde, Alman kripto personelinin yaptığı güvenlik ihlalleri de cihaz hakkında önemli bilgiler vermiştir. Sözgelimi, mesajın bir kere kriptolanarak gönderilmesinden sonra çok az değiştirilerek tekrar kriptolanıp gönderilmesi gibi ihlâller, İngiliz kriptoanalistlerin işlerini kolaylaştırmıştır.

1940'larda Japonların Amerikan deniz üssü Pearl Harbor'a saldırmaları Amerikalıları da savaşa soktu. Bu durum İngiltere'nin işini oldukça kolaylaştıracaktı. İngiltere derhal ABD ile işbirliği yaptı. Yapılan işbirliği anlaşması bilgi paylaşımını da içeriyordu. Amerikalı kriptoanalistler Bletchley Park'a davet edildi ve ortak çalışmalara derhal başlandı.

Amerikalı kriptoanalistler de İkinci Dünya Savaşı süresince başarılı çalışmalar yürütmüşlerdir. Japonların diplomatik haberleşme kanallarını kriptolamakta kullandıkları "Purple" adını verdikleri kripto sistemleri, ABD İşaret İstihbarat

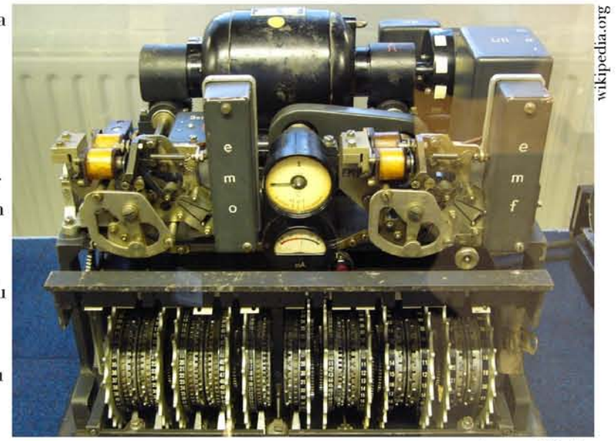
Servisi tarafından, *Operation Magic* adını verdikleri kriptoanaliz projesi kapsamında kırılmıştır.

İngiliz başbakanı Winston Churchill kriptolu Alman mesajlarının çözülmesi işine "Bu benim ultra (üstün) sırrım" dediği için proje, "Ultra Projesi" olarak anılmıştır.

Ultra sırrı, savaşta Almanya'ya karşı müttefik bir ülke olan Sovyetler Birliği'nin lideri Josef Stalin'e açıklanmadı. Bazı önemli ve gerekli bilgiler kendisine farklı yollardan ve kaynak belirtilmeden veriliyordu. Ruslar da bilgilerin kaynağını öğrenmek konusunda ısrarcı olmadılar. Çünkü Bletchley Park'ta 6. barakada çalışan bir casusları vardı ve Enigma şifrelerinin kırıldığını biliyorlardı. Hatta, şifresi çözülen mesajlardan bazıları bu casus tarafından baraka dışına çıkartılarak Moskova'ya gönderiliyordu. Bu yolla Hitler'in 5 Temmuz 1943'te Ukrayna'ya başlatacağı hava harekatı haber alınmıştı. Kızılordu Hava Kuvvetleri bu bilgiler ışığında harekete geçti, fakat Almanlar beklenenden daha erken davrandıkları için elde edilen istihbarat değerlendirilemedi. Kızılordu Hava Kuvvetleri ağır kayıplar verdi.

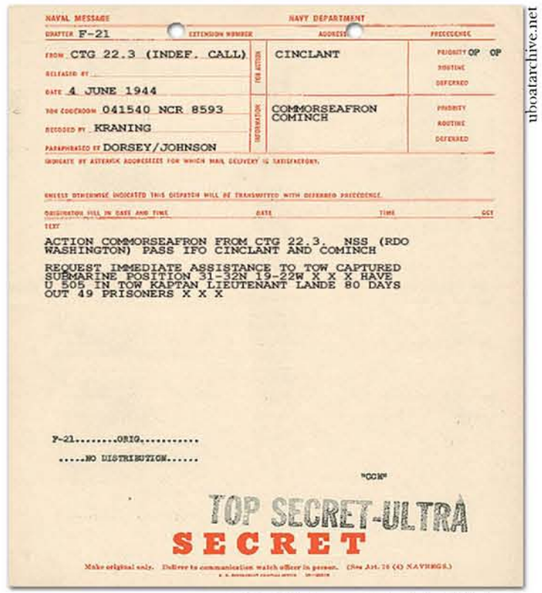
Alman Donanması, Enigma'nın kırıldığından habersiz olduğu halde cihazın güvenliğini arttırmak için, 1942 yılı başlarında, denizaltılarda kullanılan Enigma'ya bir rotor daha ekleyerek rotor sayısını dörde çıkardı. "Shark" adı verilen yeni kriptolu mesajlar, artık çözülemiyordu. İngiliz casuslar bu konu ile ilgili bilgi elde edememişlerdi. Atlantik Savaşı'nda Alman U-Bot denizaltıları, İngiliz gemilerine kan kusturuyorlardı.

1942 yılı sonlarında, Atlantik Okyanusu'nda U110 kodlu Alman denizaltısı, hava almak üzere yüzeye çıkmak zorunda kaldı ve çıktığında İngiliz gemisi tarafından vuruldu. Denizaltı batmadan önce iki İngiliz dalgıç denizaltıya girerek içindeki Enigma cihazını ve bir anahtar kod kitabını çıkartmayı başardılar.



wikipedia.org

Lorenz SZ 40.


NAVAL MESSAGE — NAVY DEPARTMENT

DRAFTER F-21 — EXTENSION NUMBER — ADDRESS — PRECEDENCE

FROM CTG 22.3 (INDEF. CALL) — CINCLANT — PRIORITY OP OP

RELEASED BY — ROUTINE — DEFERRED

DATE 4 JUNE 1944

TOR DTG/ROUM 041540 NCR 8593 — COMMORSEAFRON COMINCH — PRIORITY — ROUTINE — DEFERRED

RECODED BY KRANING

PARAPHRASED BY DORSEY/JOHNSON

INDICATE BY ASTERISK ADDRESSEES FOR WHICH MAIL DELIVERY IS SATISFACTORY.

UNLESS OTHERWISE INDICATED THIS DISPATCH WILL BE TRANSMITTED WITH DEFERRED PRECEDENCE.

ORIGINATOR FILL IN DATE AND TIME — DATE — TIME — GCT

TEXT

ACTION COMMORSEAFRON FROM CTG 22.3 NSS (RDO WASHINGTON) PASS IFO CINCLANT AND COMINCH

REQUEST IMMEDIATE ASSISTANCE TO TOW CAPTURED SUBMARINE POSITION 51-32N 19-22W X X X HAVE U 505 IN TOW KAPTAN LIEUTENANT LANDE 80 DAYS OUT 49 PRISONERS X X X

F-21.....ORIG.....

.....NO DISTRIBUTION.....

"CCS"

TOP SECRET-ULTRA

SECRET

Make original only. Deliver to communication watch officer in person. (See Art. 76 (4) NAVREGS.)

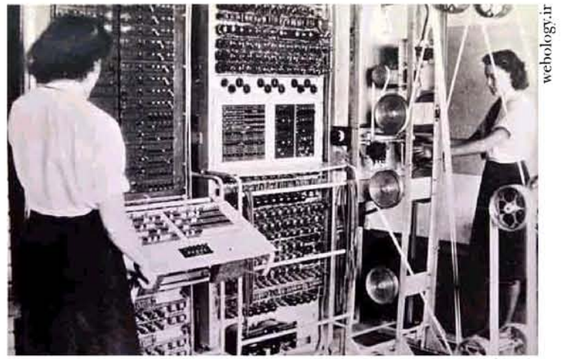
uboatarchive.net

U-Bot Yakalanma Haberinin Bildirilmesi.

İngilizler Enigma cihazına dördüncü bir rotorun eklenmiş olduğunu gördüler ve saldırı yöntemlerini buna göre geliştirdiler. Elde ettikleri kod kitabının da yardımıyla Enigma mesajları tekrar çözülebilir oldu. Almanlar, denizaltı battığı için içindeki gizli malzemelerin ele geçmiş olabileceğinden şüphe etmediler. Shark kodlarının kırılmasıyla U-Bot kâbusu zayıflamış oldu. U-Botların hareketleri izlenebilir olduktan sonra kimileri doğrudan batırıldı, kimileri ise sağlam ele geçirildi. Atlantik Savaşı'nda mesajların dinlenmesi, Alman denizaltılarının mağlup edilmesinde çok yararlı oldu.

Alman zırhlı birliklerinin gücü, hızlı hareket yeteneklerinden geliyordu. Hareketli birliklerin eşgüdümü de büyük miktarda haberleşmeyi gerekli kılıyordu. Bu sayede, İngiliz Dinleme Servisi bol miktarda kriptolu haberleşme verisi toplayabilmiştir.

Şifresi çözülmüş mesajlar son derece iyi şekilde değerlendirilmiştir. Çözülen mesajlarda adı geçen kişilere ilişkin özel dosyalar hazırlanmış ve söz konusu kişinin adının geçtiği tüm mesajlar, bu kişiye özel dosyalarda toplanmıştır. Rütbeleri, görevleri, yaptıkları işler, bu mesajlar kullanılarak belirlenmiştir. Bu yolla Alman birliklerinde komuta kademesindeki personel hakkında bir veri tabanı oluşturulmuştur. Bu veri tabanı sayesinde düşmanın gücü, planları önceden öğrenilebilmiştir. Bu veri tabanı, özellikle Alman zırhlı birliklerinin harekat planlarını ele geçirmede son derece belirleyici olmuştur.


webology.ir

Colossus.

Hitler kurmayları ile haberleşirken, Lorenz SZ 40 şifre cihazını kullanıyordu. İngilizler, 32 karakter ve 12 rotor içeren daktilo benzeri bir "teleyazıcı" ile üretilen bu kodlara "Tunny Code" adını verdi. Daha sonra, bir operatörün kripto ihlali yaparak bir anahtarla şifrelediği mesajın kısaltmalar yapılmış şeklini aynı anahtarla şifreleyerek göndermesi, kriptoanalistlerin önemli bilgiler elde etmesini sağladı. Bu verileri kullanan John Tiltman, açık metinle kayan anahtar dizisini ayrıştırdı. William Tutte ise istatistiksel sapmalar üzerine kurulu olan "Tutte Sistemi" ni geliştirdi ve şifre kırıldı. Bletchley Park'taki kriptoanaliz faaliyetleri kapsamında geliştirilen ve ilk programlanabilir bilgisayar olarak nitelendirilen "Colossus" bilgisayarı üzerinde Tutte'nin analiz yöntemi uygulanarak şifrenin kırılması mümkün olmuştur.

1944 yılına gelindiğinde, Hitler'in tüm mesajları çözülebiliyordu. 15 nisan 1945 tarihinde son mesajı da çözüldü.

Ultra sırrının savaş boyunca korunması çok önemliydi ve son derece iyi korundu. Şifresi çözülen tüm bilgiler düzenli olarak Churchill'e aktarılıyordu. Savaş alanındaki komutanlara ise, sadece kendileri ile ilgili bilgiler aktarılıyordu. Churchill, Ultra bilgilerinin hiçbir operasyonda kullanılmamasında ısrar ediyor, Ultra sırrının ortaya çıkma olasılığını mümkün olduğunca düşük tutmaya çalışıyordu. Bu sırrın korunması için çok dikkatli davranıldı. Gerekli olmadıkça kimseye bilgi verilmedi.

Almanların elinde dinlendiklerine ilişkin birtakım ipuçları olmasına karşın İngilizlerin Ultra Sırrı'nı farkedemediler.

1942 Eylül ayında İngiliz kraliyet donanmasına ait bir motorlu bot Almanlar tarafından ele geçirildi. Botta, Alman konvoylarının hareket bilgilerini içeren ve Almanlar tarafından döşenmiş olan mayınların yerlerinin belirtildiği çeşitli dokümanlar bulunuyordu. Fakat Alman istihbarat servisi bu bilgilerin İngilizlerin eline nasıl geçtiğini sorgulamadı.

Amerikan hava istihbarat subayı Arthur W. Walleman'a, sağduyuya aykırı bir şekilde, Fransa üzerinde B17 uçağı ile istihbarat uçuşu yapma izni verildi. Uçağı 27 Haziran 1944 yılında Almanlar tarafından düşürüldü. Walleman kazadan sağ kurtuldu ve esir alındı. Savaşın geri kalan yıllarını Ultra sırrını istemeden açıklama korkusuyla geçirdi. Walleman uykusunda konuştuğunu biliyordu. Fakat korktuğu olmadı, sır ortaya çıkmadı.

1941'de, bir İngiliz uçak gemisinin Alman U-Botları tarafından sıkıştırılması emrini içeren mesajın şifresi çözüldü. Churchill ve komutanları, Ultra sırrının ortaya çıkabileceğini düşünerek bu mesajı donanmaya iletmedi ve uçak gemisinin batırılmasına seyirci kaldı. Aynı düşünceyle, sırrın ortaya çıkmaması için bazı kasabaların bombalanmalarına da seyirci kalındı.

Ultra sırrı, savaşın bitişinden 30 yıl sonra açıklanmasına dek öğrenilemedi. Bombe bilgisayarları savaşın bitiminde, Colossus bilgisayarı ise, 1960 yılında, güvenlik nedeniyle imha edildi. Bugün müze durumuna getirilen Bletchley Park'ta sergilenmek üzere yeniden Bombe ve Colossus bilgisayarları üretildi.


uboatarchive.net

Amerikalılar tarafından ele geçirilmiş bir U-Bot denizaltısı.

İkinci Dünya Savaşı yılları ilginç kriptolojik uygulamalara da sahne olmuştur. ABD, telefon haberleşmesinde bilgi güvenliğini sağlamak üzere Navajo yerlilerinden yararlanmıştır. Katliamlar sonrasında sayıları 20 kadar kalan bu Kızılderililer, kendilerine özgü Navajo dili ile birlikte İngilizce de konuşabilmektelerdi. Dünya üzerinde Navajo dilini bilen başka kimse bulunmuyordu. ABD bilgi güvenliği subayları bu yerlileri askerlik hizmetine aldı ve çeşitli askeri terimlerin öğretildiği bir eğitim döneminden sonra birliklere dağıtarak güvenli iletişim sağlamakta kullandı. Benzer biçimde, bazı birliklerde Siu (Sioux) ve Komançi (Comanche) Kızılderililerinden de yararlanılmıştır. Savaş sonrasında, ABD Temsilciler Meclisi bu Kızılderililerin pek çoğunu altın madalya ile ödüllendirmiştir.

İkinci Dünya Savaşı'nda meydana gelen yaraların sarılması uzun zaman aldı. Dünyanın politik açıdan yeniden yapılanmasının ötesinde, savaştan alınan dersler ışığında kriptolojinin geleceği de yönlendirildi. Savaş boyunca sürdürülen kriptoanaliz faaliyetlerinden haberi olan ülkeler, kendi kullandıkları kripto yöntemlerinin de kırılmaması için azami çaba sarfettiler. Dünyanın önde gelen matematikçileri kırılamayacak kripto algoritmaları tasarlamaya yöneldiler.

Transistörün icadı sonrasında hızla gelişen elektronik teknolojileri, kriptolojinin gelişim yönünü belirleyen temel etkenlerden biri oldu. Yüksek işlem kapasitesi sağlayan elektronik devreler ve bilgisayarlar, kriptoanaliz çalışmalarında temel yapıtaşı olarak kullanılmaya başlandı. Böylesine güçlü kriptoanalitik saldırı altyapısı karşısında dahi güvenliği sağlayabilecek kripto algoritmalarının tasarımında da görev matematikçilere düşüyordu.

Kripto algoritması tasarımcıları ile kriptoanalistler arasındaki bu denge bugün de sürmektedir ve gelecekte de sürecektir. Kriptoanaliz yeteneklerinin arttığı ölçüde, kripto algoritmalarının güvenilirliği de kanıtlanabilir biçimde artırılmak zorundadır. Kripto algoritmalarının güvenilirliğinin sadece kullanılan kripto değişkenlerinin boyuna bağlı olmadığı, geliştirilen matematiksel çözümleme yöntemlerine karşı da dayanıklı olması gerektiği göz önünde tutulmalıdır.

Güvenli Haberleşme İçin Kullanılan Navajo Yerlileri.

cronkite.asu.edu

KAYNAKÇA

[1] The Codebreakers - The Story of Secret Writing (ISBN 0-684-83130-9) David Kahn, (1967)
[2] www.wikipedia.org
[3] http://www.ellsbury.com/enigmabombe.htm "