Historia złamania Enigmy zaczyna się w roku 1919, po 123 latach niewoli, odrodzona Polska, tuż po pierwszej wojnie światowej znów musi walczyć o swoją wolność.

Młode Państwo Polskie musi obronić siebie i zatrzymać sowiecką armię przed opanowaniem Europy, w tym czasie powstaje zaczątek Biura Szyfrów - Sekcja Szyfrów założona przez por. Józefa Serafina Stanślickiego.

Już w 1919 r. tuż po odzyskaniu niepodległości, Jan Kowalewski , organizator i naczelnik Wydziału II Radiowywiadu Biura Szyfrów Oddziału II Sztabu Generalnego Naczelnego Dowództwa w latach 1919-1924, złamał pierwsze klucze szyfrowe Armii Czerwonej, umożliwiające odczytanie korespondencji bolszewickiej z frontów wojny domowej na Ukrainie, w styczniu 1920 r. rozpoczął łamanie szyfrów niemieckich.

Biuro Szyfrów jako jedno z pierwszych w historii wywiadów zrezygnowało z lingwistów, mistrzów szachowych i innych osób i zatrudniło matematyków ze słynnej, polskiej szkoły matematycznej (Uniwersytet Lwowski i Uniwersytet Warszawski) Stanisława Leśniewskiego, Stefana Mazurkiewicza i Wacława Sierpińskiego.

 Do słynnej przedwojennej polskiej szkoły matematycznej należeli m. innymi Stefan Banach, Hugo Steinhaus, Stanisław Mazur, Kazimierz Kuratowski oraz Stanisław Ulam - twórca metody Monte Carlo, wraz z Węgrem Edwardem Tellerem stworzyli amerykańską bombę termojądrową.

Bydgoszcz ul Wileńska, tutaj urodził się Marian Rejewski, miał zaledwie kilka lat gdy dwaj oficerowie holenderskiej marynarki wojennej Theo Van Hengel i Rudolf Sprengler w 1915 r. konstruują wirnikową maszynę szyfrującą. Holandia jest krajem neutralnym i chce ukrywać swoje informacje zarówno przed Anglikami i Niemcami, zostały wówczas zbudowane dwa egzemplarze takich maszyn, które były używane we wschodniej Indonezji.

 Oficerowie holenderscy ociągali się ze złożeniem patentu, ubiega ich Hugo Alexander Koch, holenderski wynalazca, uzyskał patent nr 10.700 na wirnikową maszynę szyfrującą, o który wystąpił w Holandii w dniu 7 października 1919 r.

Hugo Alexander Koch nie był jedynym który złożył patent na maszynę szyfrującą, w 1919r. Artur Scherbius otrzymał patent na elektromechaniczną maszynę szyfrującą, w tym samym roku wraz z Ernstem Richardem powołuje do życia firmę Scherbius & Ritterwas , firma zakupiła również prawa do patentu, którego właścicielem był Hugo Koch.

 W 1923 r. zostaje pokazana po raz pierwszy, wirnikowa maszyna szyfrująca wyprodukowana przez firmę Scherbius & Ritterwas, znana jako Enigma. Początkowo, była sprzedawana w wersji komercyjnej dla wszystkich, którzy chcieli utajnić swoją korespondencję.

W roku 1926 niemiecka marynarka wojenna modyfikuje cywilną Enigmę i zaczyna szyfrowanie swoich wiadomości przy pomocy tejże zmodyfikowanej maszyny, jednocześnie wersja cywilna Enigmy zostaje stopniowo wycofana z rynku.

W lipcu 1928 r. niemieckie wojskowe stacje radiowe zaczęły nadawać pierwsze wiadomości szyfrowane Enigmą, polski wywiad przechwytuje korespondencję ale kryptolodzy w sekcji niemieckiej Polskiego Biura Szyfrów nie są w stanie złamać szyfru i zaprzestają pracy nad nim, podobnie postępują służby wywiadowcze Francji i Wielkiej Brytanii

W styczniu 1929 roku szefem Referatu Radiowywiadu zostaje Major Gwido Langer, wkrótce zostaje mianowany szefem Biura Szyfrów, zastępcą Majora Langera i szefem sekcji niemieckiej BS-4 zostaje kpt. Maksymilian Ciężki.

Kierownictwo BS-4 nie chce się pogodzić z brakiem możliwości odczytywania zaszyfrowanych wiadomości armii niemieckiej i w tym samym roku, pracownicy Referatu Radia i Szyfrów, major Franciszek Pokorny, kapitan Maksymilian Ciężki, cywilny pracownik Biura, Antoni Palluth oraz profesor Zdzisław Krygowski prowadzą w tajemnicy kurs kryptologii, dla wybranych niemieckojęzycznych studentów matematyki na Uniwersytecie w Poznaniu.

Uniwersytet w Poznaniu nie został wybrany przypadkowo, kierownictwo Biura Szyfrów zdawało sobie sprawę, że tutejsi studenci znają doskonale mentalność, kulturę i język potencjalnego wroga jakim są Niemcy. Profesor Krygowski wybiera spośród studentów ostatnich dwóch lat, grupę 20 osób którzy biorą udział w tajnym kursie kryptologii. Po zakończeniu kursu zostaje wytypowanych trzech najzdolniejszych studentów: Marian Rejewski, Jerzy Różycki oraz Henryk Zygalski którzy zaczynają współpracę z poznańską ekspozyturą Biura Szyfrów, po dwóch latach przerwy Polacy powtórnie próbują złamać szyfr Enigmy. We wrześniu 1932 r. poznańska ekspozytura zostaje zlikwidowana, a trzej matematycy podpisują umowę z Biurem Szyfrów, stają się jego cywilnymi pracownikami i zostają przeniesieni do Warszawy, tutaj pracują intensywnie nad złamaniem kodu Enigmy.

Marian Rejewski w oparciu o materiały (szyfrogramy, książkę kodową ustawień maszyny szyfrującej na wrzesień i październik 1932 roku) dostarczone do Biura Szyfrów przez generała francuskiego wywiadu Gustave Bertranda, które wywiad francuski zakupił od niemieckiego szpiega na rzecz Francji Hansa-Thilo Schmidta, pseudonim Asché, wykorzystując teorię grup, zwłaszcza twierdzenie o permutacjach, odtworzył wewnętrzne połączenia wirników oraz walca odwracającego.

Marian Rejewski we wspomnieniach z 1980 roku napisał, że można było dojść do tych samych wniosków bez danych uzyskanych od wywiadu francuskiego, ale metoda ta byłaby niedokładna i żmudna i w znacznej mierze musiałaby polegać na przypadku. Po opracowaniu przez Mariana Rejewskiego wewnętrznych połączeń wojskowej Enigmy, polskie Biuro Szyfrów zleciło firmie AVA Radio Company , budowę odpowiednika Enigmy zgodnie ze specyfikacjami Rejewskiego. Pierwsze wiadomości armii niemieckiej szyfrowane Enigmą zostały złamane.

Marian Rejewski wspomina: teraz mieliśmy maszynę, ale nie posiadaliśmy kluczy i nie mogliśmy wymagać od generała Bertranda dostarczania ich każdego miesiąca... sytuacja ta była odwrotna niż poprzednio. Konieczne stało się opracowanie metod znajdowania kluczy dziennych.

Nieustanne udoskonalanie przez stronę niemiecką procedury szyfrowania i samej Enigmy wymusiło na Polskich Matematykach stworzenia wielu metod dekryptażu.
Pierwszą z nich była bardzo żmudna, ręczna metoda rusztu zakładająca, że na łącznicy kablowej zamienionych jest tylko sześć par liter, a pozostałe czternaście liter jest niezmienione.

Kolejną była metoda zegarowa Różyckiego, pozwalająca na ustalenie z dużym prawdopodobieństwem, który wirnik znajduje się danego dnia na prawej skrajnej pozycji maszyny

Po 1 października 1936 roku Niemcy zmienili procedury kodowania zwiększając liczbę połączeń na przełącznicy kablowej Enigmy. W rezultacie metoda rusztu znacznie straciła na efektywności, ale wynaleziona w międzyczasie, około 1935 lub 1936, metoda kart charakterystyk była niezależna od liczby połączeń na łącznicy. Katalog kart konstruowano przy wykorzystaniu opracowanego przez Rejewskiego przyrządu nazwanego cyklometrem, który wyliczał permutacje cykliczne. Po zapisaniu w katalogu wszystkich charakterystyk można było z niego odczytywać odpowiednie permutacje odpowiadające ustawieniu wirników danego dnia.

Cyklometr składał się z dwóch zestawów wirników Enigmy i był wykorzystywany do ustalenia długości i liczby cykli permutacji generowanych przez Enigmę. Nawet jednak przy pomocy tego urządzenia stworzenie pełnego katalogu charakterystyk było zadaniem trudnym i czasochłonnym. Dla każdej z 17576 pozycji, w których mogła być ustawiona maszyna należało przeanalizować sześć możliwych sekwencji wzajemnego ustawienia wirników, co w efekcie daje 105 456 wyników. Przygotowanie pierwszego katalogu pochłonęło ponad rok pracy, ale po jej zakończeniu około roku 1935, określenie klucza dziennego było możliwe w czasie od 12 do 20 minut.

Z początkiem listopada 1937 strona niemiecka zmieniła walec odwracający Enigmy, co oznaczało, że cały katalog charakterystyk musiał być przeliczony od początku, mimo tej zmiany w styczniu 1938 referat BS4 Biura Szyfrów odpowiedzialny za dekryptaż szyfrów niemieckich był w stanie odczytać około 75% przechwyconych meldunków zaszyfrowanych Enigmą, a zdaniem Rejewskiego przy nieznacznym zwiększeniu liczby personelu możliwe było odczytanie nawet 90% przekazów

Latem 1937, Biuro Szyfrów zostaje przeniesione do tajnego ośrodka niedaleko Pyr w Lesie Kabackim pod Warszawą. W sierpniu 1938 Niemcy wprowadzili nowe zasady kodowania i przesyłania kluczy dziennych, które spowodowały, że wszystkie ówczesne techniki dekryptażu Enigmy stały się nieaktualne. Polscy Matematycy opracowują nowe metody znajdowania ustawień Enigmy i kluczy. Powstaje bomba kryptologiczna Rejewskiego, napędzane elektrycznym silnikiem urządzenie powstałe z połączenia sześciu kopii maszyny Enigma zdolne znaleźć klucz dzienny w około 2 godziny, ale po wprowadzeniu w styczniu 1939 kolejnej modyfikacji kodowania polegającej na zwiększeniu liczby połączeń na przełącznicy użyteczność bomby znacznie spadła.

W tym samym czasie Zygalski opracował własną metodę opartą na perforowanych papierowych płachtach, nazwanych płachtami Zygalskiego, które były niezależne od liczby zamienionych na przełącznicy kablowej par liter. Jednakże zarówno bomba Rejewskiego jak i płachty Zygalskiego po raz kolejny straciły na użyteczności po wprowadzeniu przez Niemców 15 grudnia 1938 kolejnej modyfikacji kodowania polegającego na rozszerzeniu zestawu wirników o dwa nowe, co dziesięciokrotnie skomplikowało proces dekryptażu. Aby sprostać zadaniu rozszyfrowania kolejnych kodowanych w nowy sposób przekazów konieczne było zbudowanie sześćdziesięciu bomb kryptologicznych i stworzeniu tyluż kompletów płacht Zygalskiego, ale koszt konstrukcji tylu narzędzi przekraczał piętnastokrotnie budżet Biura Szyfrów. Dodatkowo wprowadzona przez Niemców w następnym miesiącu kolejna modyfikacja kodowania polegająca na zwiększeniu zamienionych par liter z 12 do 20 (co zwiększyło do ponad tysiąca liczbę możliwych konfiguracji przełącznicy) jeszcze zmniejszyła efektywność dekryptażu przy pomocy bomb.

W styczniu 1939 r. na konferencji w Paryżu, spotykają się przedstawiciele Biura Szyfrów ze służbami kryptologicznymi Wielkiej Brytanii i Francji. Polską stronę reprezentują pułkownik Gwido Langer oraz kapitan Maksymilian Ciężki. Spotkanie we Francji miało na celu przedstawienia stanowiska wywiadów na jakim etapie mają prace dotyczące złamania Enigmy. Polscy przedstawiciele zachowują milczenie zgodnie z wcześniejszymi ustaleniami w kraju, do ujawnienia informacji o złamaniu miało dojść wyłącznie w przypadku gdy strona francuska lub brytyjska miałaby jakikolwiek sukces w rozszyfrowaniu Enigmy. Brytyjczycy i Francuzi nie mają prawie żadnej wiedzy dotyczącej łamania Enigmy, Polacy nie angażują się w ujawnienie wyników swojej pracy.

Nadchodzi lato 1939 r. z inicjatywy Polskiego Biura Szyfrów zostają wysłane zaproszenia do służb wywiadu Francji i Wielkiej Brytanii na konferencję dotyczącą Enigmy. Do spotkania dochodzi w lipcu 1939 r, stronę francuską reprezentuje Gustave Bertrand, angielską Alastair Denniston Dillwyn Knox. Obie delegacje okazują stronie polskiej niechęć i lekceważenie. 25 lipca 1939 r. obie delegacje jadą do ośrodka radiowywiadu w Pyrach gdzie pułkownik Gwido Langer oraz kapitan Maksymilian Ciężki mając zgodę dowództwa Wojska Polskiego ujawniają sekret złamania Enigmy. Polscy matematycy przedstawiają dowody matematyczne dotyczące rekonstrukcji maszyny i uzyskiwania kluczy ustawień Enigmy, prezentują urządzenia umożliwiające dekryptaż. Na koniec spotkania odszyfrowują przechwyconą świeżą radiodepeszę.

Anglicy i Francuzi otrzymują od strony polskiej po kopii Enigmy wraz z dokumentacją umożliwiającą dekryptaż, 15 sierpnia 1939 r., brytyjska GC&CS przeniosła się do ściśle tajnego miejsca Bletchley Park, gdzie brytyjski matematyk Alan Turing, bazując na pracy polskich matematyków buduje bombę kryptologiczną i dokonuje dekryptażu niemieckich szyfrów, które jak się okazało znacząco zmieniły losy wojny, ale to już całkiem inna historia ........