Prof. dr hab. Grzegorz Nowik
Instytut Studiów Politycznych PAN
Muzeum Józefa Piłsudskiego w Sulejówku
05-540 Zalesie Górne, ul. Biedronki 16.B.
grzegorznowik@egonet.pl, tel. 22-7070-976, 693-34-35-38

Lingwistyczny i matematyczny „atak" na szyfry kluczem polskich sukcesów w zakresie kryptoanalizy w XX wieku

Od „Rewolucji" do „Enigmy"

Profesor David Khan, wybitny badacz i znawca dziejów kryptoanalizy uważa, że jednym z największych sukcesów w dziedzinie dekryptażu (czyli łamania szyfrów i kodów) było złamanie systemu utajniania korespondencji przez niemiecką maszynę szyfrową ***„Enigma"***, wprowadzoną w niemieckich siłach zbrojnych w drugiej połowie lat dwudziestych XX wieku i stosowaną aż do końca II wojny światowej. Racjonalni oficerowie niemieccy, wiedząc, że liczba kombinacji szyfrowych tworzonych przez „Enigmę" jest większa od liczby atomów w kosmosie, albo też sekund, jakie upłynęły od „wielkiego wybuchu" (czyli początku wszechświata) twierdzili, że odczytanie szyfrogramów „Enigmy" jest całkowicie niemożliwe.

A jednak polskie Biuro Szyfrów Sztabu Głównego Wojska Polskiego dokonało tego w końcu 1932 roku, stosując tzw. „atak" na szyfr: lingwistyczny a zarazem matematyczny. Francuskie i brytyjskie zespoły kryptoanalityków stosując jedynie pierwszy rodzaj „ataku" nie były w stanie rozwiązać metody szyfrowania zastosowanej w „Enigmie"". – Pozostaje więc zadać pytanie, jak doszło do tego sukcesu, gdzie zaczerpnięto zamysł takiego podwójnego ataku, skąd wywodził się zamysł zatrudnienia do łamania szyfrów matematyków?

Dodać należy, że pracownicy Wydziału BS „Niemcy" w polskim Biurze Szyfrów (BS–4), Oddziału II Informacyjnego (Wywiadowczego) SG WP, to właśnie trzej matematycy: Marian Rejewski, Jerzy Różycki i Henryk Zygalski, absolwenci Wydziału Matematyki Uniwersytetu Poznańskiego. To dzięki ich pracy i sukcesowi zwycięstwo aliantów w II wojnie światowej dokonało się zarówno szybciej, jak też kosztowało mniej istnień ludzkich oraz nakładów finansowych. Bowiem podejmowane przez alianckie sztaby decyzje były racjonalne, podejmowane na podstawie szerokiego spektrum wiedzy płynącej wprost od przeciwnika, dającej wgląd w plany oraz działania Sił Zbrojnych niemieckiej III Rzeszy.

Jak do tego doszło? Otóż zrekonstruowane – na podstawie odtworzonego matematycznie schematu ideowego (w tym głównie połączeń elektrycznych w tzw. „bębenkach szyfrowych" – maszyny „Enigma", wraz z metodami łamania i urządzeniami pomocniczymi zostały w lipcu 1939 r., przekazane wywiadom wojskowym Francji i Wielkiej Brytanii, które stworzyły – dzięki tej wiedzy – system zwany „Ultra", szeroko zorganizowanego nasłuch radiowego, łamania szyfrów oraz dystrybucji otrzymanych wiadomości.

Ale źródło sukcesów aliantów nie było by możliwe, gdyby nie specyficznie polskie doświadczenia w dziedzinie kryptoanalizy, właśnie wynikające z zastosowania podwójnego: lingwistycznego i matematycznego „ataku" na szyfry, zastosowanego w latach 1919–1920, przez Polaków: oficerów Wojska Polskiego oraz polskich profesorów matematyki, w łamaniu szyfrów rosyjskich podczas wojny z bolszewicką Rosją. Symbolem ówczesnego sukcesu jest szyfr ***„Rewolucja"***, wprowadzony w Armii Czerwonej 12 sierpnia 1920 r. w przededniu szturmu Warszawy. Szyfr ten, dwukrotnego przekształcenia, złamany został w ciągu kilku godzin przez polskiego oficera, porucznika Jana Kowalewskiego oraz profesora matematyki Stefana Mazurkiewicza z Uniwersytetu Warszawskiego. Złamanie tego szyfru, tak jak wielu innych – wcześniej i później – używanych w „czerwonej" Rosji, dało najwyższym polskim władzom wojskowym i cywilnym szczególny oręż umożliwiający, a przynajmniej ułatwiający

pokonanie bolszewickiej Rosji w 1920 roku. Rozszyfrowanie „Rewolucji" oznaczało, nie tylko złamanie kolejnego klucza szyfrowego, ale również – w sposób symboliczny – zatrzymanie pod Warszawą pochodu proletariackiej rewolucji bolszewickiej niesionej na zachód Europy na bagnetach Armii Czerwonej.

Rosjanie, podczas wojny z Polską, zmieniali klucze szyfrowe przeciętnie co dwa tygodnie, dziesięć dni, a nawet co tydzień, na tyle oceniając polskie zdolności w łamaniu szyfrów. Po tym bowiem terminie zdobyte informacje dezaktualizowały się, jak gazeta sprzed dwóch tygodni lub dziesięciu dni. Tymczasem polskie Biuro Szyfrów łamało nowowprowadzane rosyjskie klucze szyfrowe w początkowo w ciągu dwóch-trzech dni, a następnie w ciągu dwóch-trzech godzin… Łamało systematycznie je aż do 1947 roku.

Złamanie niemieckiej ***„Enigmy"*** było więc konsekwencją wcześniejszego złamania ***„Rewolucji"*** i wielu innych rosyjskich szyfrów – dzięki wspomnianej już swoistej metodzie, zastosowanej po raz pierwszy w Polsce i przez Polaków. Był nią podwójny: lingwistyczny, a jednocześnie matematyczny „atak" na szyfry. To co zapoczątkowane zostało w Polsce w 1919 roku, w odniesieniu do szyfrów rosyjskich, przyniosło tak bogate owoce w 1932 roku, gdy sekcja (BS–4 – szyfry niemieckie) Biura Szyfrów zaczęła odczytywać szyfrogramy utajniane za pomocą „Enigmy". Było to prosta konsekwencja doświadczeń z lat 1919–1920, prowadząca do tego, że przyszłych pogromców „Enigmy", w arkana kryptografii wprowadzali starsi koledzy łamiący rosyjskie szyfry z lat 1919–1920, w tym ci którzy 12 sierpnia 1920 r., złamali ***„Rewolucję".*** To oni w strukturach utworzonego w końcu 1918 roku Biura Szyfrów przechowali wiedzę o tej swoistej metodzie i swoje doświadczenie przekazali następcom.

Jak doszło więc do pierwszego w XX wieku polskiego lingwistycznego i matematycznego „ataku" na szyfry rosyjskie. Aby zrozumieć, że nie był to jedynie skutek swoistego zbiegu okoliczności, geniuszu wybitnych jednostek, ale też konsekwencja celowych i zamierzonych działań należy cofnąć się do 10 listopada 1918 r. W niedzielę, w mglisty poranek, około godziny siódmej, na Dworzec Wiedeński w Warszawie (vis a vis Hotelu „Polonia", tu gdzie obecnie znajduje się Dworzec Podmiejski Warszawa-Śródmieście), po szesnastu miesiącach niemieckiego uwięzienia w twierdzy w Magdeburgu powrócił do stolicy komendant Józef Piłsudski. Nazajutrz 11 listopada 1918 r., Rada Regencyjna przekazała mu władzę nad Wojskiem Polskim, a 14 listopada złożyła w jego ręce odpowiedzialność za losy Narodu i odradzającego się Państwa Polskiego. Jedną z pierwszych decyzji, jakie podjął Wódz Naczelny, był rozkaz odnalezienia Józefa Rybaka.

Wywiad i radiowywiad

Oprócz polecenia odnalezienia Józefa Rybaka, Józef Piłsudski natychmiast po objęciu obowiązków Wodza Naczelnego nakazał szybkie rozbudowanie Oddziału Informacyjno-Wywiadowczego Sztabu Generalnego Wojska Polskiego (SG WP). Szefem Oddziału, 12 grudnia 1918 roku, został właśnie przybyły z Wiednia do Warszawy ppłk. Józef Rybak, były oficer austro-węgierskiego Sztabu Generalnego. Dlaczego on? Józef Piłsudski miał dlań wiele szacunku i sympatii, z czasów gdy Józef Rybak, jako młody kapitan CK armii austro-węgierskiej, był – przed 1914 rokiem – szefem wywiadu wojskowego (*Haupt Kundschaft Stellen – HK Stelle*) w sztabie krakowskiego korpusu wyznaczony do kontaktów z towarzyszem „Wiktorem" (Józefem Piłsudskim), ówczesnym emigrantem politycznym z zaboru rosyjskiego, kierownikiem polskiej irredenty i antyrosyjskiego ruchu wojskowo-niepodległościowego w Galicji. Już wówczas Komendant, dostrzegł w kapitanie Rybaku polskiego patriotę w mundurze zaborcy i zdania tego nie zmienił. Dostrzegł w nim patriotę, który wiedział i domyślał się więcej niż meldował swym władzom, stając się bardziej lojalny wobec Józefa Piłsudskiego niż względem swych austriackich mocodawców. Z drugiej strony Komendant widział w nim fachowca, który miał zorganizować centralę polskiego wywiadu

na wzór i podobieństwo *Ewidenzbiuro* austro-węgierskiego Sztabu Generalnego oraz pozyskać do niej – swych kolegów – fachowców.

Podpułkownik Rybak za punkt honoru poczytywał sobie pozyskanie najlepszych specjalistów z wywiadu austro-węgierskiego. Do służby w Oddziale Informacyjno-Wywiadowczym SGWP wciągnął kolegę, najlepszego znawcę spraw Rosji, w tym także rewolucyjnej Rosji, który wiedział o niej więcej niż ktokolwiek inny w tym czasie, nie tylko w Polsce, ale i w Europie. Był nim mjr Sztabu Generalnego Karol Bołdeskuł, oficer radiowywiadu, a następnie od jesieni 1915 r. do sierpnia 1917 r., szef radiowywiadu państw centralnych na froncie wschodnim.

Przez niemal dwa lata mjr. Karol Bołdeskuł kierował działaniami kilku grup radiostacji (*Radiogruppe*) austriackich i niemieckich (liczących po kilka radiostacji nasłuchowych i radiogoniometrycznych) monitorujących rosyjskie sieci radiowe między Rygą a Odessą, przejmujących całą ich jawną i tajną korespondencję operacyjną, dyplomatyczną i wewnętrzną. Następnie w komórkach kryptoanalitycznych austro-węgierskiego Biura Szyfrów korespondencja ta była poddawana dekryptażowi. Było to dla państw centralnych niezwykle cenne – bodaj najcenniejsze – źródło informacji o carskich wojskach rosyjskich podczas I wojny światowej. Było jednym ze źródeł przewagi państw centralnych oraz zwycięstw nad Rosją na froncie wschodnim. Mimo, że na froncie tym wojskami koalicyjnymi (niemieckimi i austro-węgierskimi) naczelne dowództwo sprawowali Niemcy, radiowywiad pozostał w rękach austro-węgierskich, a w strukturach *Abhorchdienst* (nasłuchu radiowego) oraz w komórkach szyfrowych służyło wielu oficerów – Polaków. Dzięki temu doświadczeniu, Bołdeskuł znał nie tylko doskonale metody działania radiowywiadu, ale był bardzo dobrze zorientowany w funkcjonowania rosyjskiej radiotelegrafii (tzw. zasad organizacji sieci radiowych i struktur ruchu radiowego, zakresów fal, sygnałów wywoławczych i innych procedur, a nawet zwyczajów obowiązujących w rosyjskiej radiotelegrafii); znał nazwiska kadry dowódczej i oficerów radiotelegrafii rosyjskiej (zestawiane w specjalnych broszurowych wykazach wraz z OdeB radiostacji), a także stosowane przez Rosjan systemy szyfrowe. Po rewolucji lutowej 1917 r. obserwował w eterze proces rozpadu starej armii carskiej, rozpadu państwa oraz anarchii ogarniającej rozległe imperium Romanowych. Obserwował proces wykorzystywania radiotelegrafii w szerzeniu propagandy, w tym także bolszewickiej oraz początki wojny domowej w Rosji. Słowem mjr Karol Bołdeskuł był w ówczesnej Europie, jednym z najlepszych znawców nie tylko rosyjskiej radiotelegrafii, ale również Rosji i wojsk rosyjskich po obu stronach frontów wojny domowej.

Józef Piłsudski, jako Wódz Naczelny, doskonale zdawał sobie sprawę z wagi wywiadu wojskowego, a szczególnie czerpania informacji (dzięki radiowywiadowi), u źródła, od samego przeciwnika. Wiedział też jaką rangę ma nie tylko stosowanie w Wojsku Polskim różnorodnych systemów utajniania korespondencji operacyjnej, ale także podejmowanie prób przechwytywania korespondencji przeciwnika i prób jej odczytania. Miał wszak ogromne, wieloletnie doświadczenia konspiracyjne. Profesor Ryszard Świętek, w swym dziele: *Lodowa Ściana. Sekrety Polityki Józefa Piłsudskiego*, wymienił kilka różnych szyfrów oraz systemów kodowych do utajniania korespondencji, jakie stosowane były w PPS i OB PPS. Całe środowisko byłych konspiratorów, wywodzących się z PPS i jej Organizacji Bojowej oraz Polskiej Organizacji Wojskowej, gdzie praktyką było szyfrowanie korespondencji organizacyjnej, podjęło służbę w Wojsku Polskim na różnych szczeblach, szczególnie obficie zasilając szeregi służby informacyjno-wywiadowczej. Wielu z nich, przynajmniej teoretycznie miało okazję zapoznać się z zagadaniem szyfrów na łamach „Przeglądu Wojskowego" wydawanego w Legionach, lub w Szkole Podchorążych Polskiej Siły Zbrojnej, gdzie nauczano o radiotelegrafii i konieczności szyfrowania tekstów, a także metodach

podsłuchu (telefonicznego i telegraficznego) oraz nasłuchu (radiotelegraficznego), dla uzyskania informacji o nieprzyjacielu bezpośrednio on niego samego.

Początki polskiej radiotelegrafii

W tym samym czasie, na początku listopada 1918 r., pierwszy szef służby łączności odradzającego się Wojska Polskiego, mjr inż. Kazimierz Drewnowski, absolwent Politechniki we Lwowie, Zurychu i Darmstradt, dowódca formacji łączności w Legionach i Polskiej Sile Zbrojnej (przyszły rektor Politechniki Warszawskiej), polecił ppor. inż. Kazimierzowi Jackowskiemu (zwanemu „Jackiem"), absolwentowi Politechniki Lwowskiej i Monachijskiej, byłemu oficerowi rezerwy radiotelegrafii rosyjskiej – rejestrację oficerów, podoficerów i żołnierzy służących podczas wojny światowej w formacjach radiotelegraficznych państw zaborczych.

W tym czasie istniały już w Polsce – na Politechnice Warszawskiej i Politechnice Lwowskiej – Wydziały Elektryczne prowadzące badania nad radiotelegrafią, choć zaledwie osiem lat wcześniej, w 1909 r., Włoch Guglielmo Marconi otrzymał nagrodę Nobla w dziedzinie fizyki za wynalazek polegający na przekazaniu impulsu elektrycznego na odległość bez użycia metalowego przewodu. Dlatego początkowo nazywano jego wynalazek – telegrafem bez drutu (TBD). Nie była to jeszcze radiofonia – w takiej formie jaką ma współczesne radio, gdy przekazuje się dźwięk na odległość, czy telewizja – gdzie przekazuje się obraz. Była to radiotelegrafia, gdzie porozumiewano się przy pomocy alfabetu Morse'a. Ówczesna nadawcza aparatura radiowa wytwarzała impulsem elektrycznym falę elektromagnetyczną powodująca powstanie w odbiorniku dźwięku, przypominającego buczenie (lub trzask), który dzięki zastosowaniu tzw. *klucza* (zamykającym obwód elektryczny) oddawał krótsze (kropki) i dłuższe (kreski alfabetu Morse'a), tak samo jak w telegrafie przewodowym.

Specjalność ta była tak nowa i rzadka, że oficerów radiotelegrafii we wszystkich ówczesnych armiach (w tym i w Wojsku Polskim) było mniej niż pilotów w lotnictwie. Dlatego por. Jackowski zarejestrował wszystkich wykładowców i studentów radiotechniki Politechniki Warszawskiej, a 10 listopada w gazetach warszawskich zamieścił ogłoszenie: *Baczność! Dla objęcia radiotelegraficznej stacji w Cytadeli potrzebni są niezwłocznie zdolni żołnierze radiotelegrafiści. Zgłaszać się do ppor. inż. K. Jackowskiego – Śniadeckich 4 m. 3.* Wkrótce po tym, w prywatnym mieszkaniu Jackowskiego, zameldowali się b. oficerowie z armii rosyjskiej: porucznik Bronisław Sroka (dowódca oddziału „radio" w I Korpusie Polskim w Rosji) oraz podporucznicy Jan Sawicki i Eugeniusz Rzymowski.

Wybudowana przez Niemców w latach 1915–1916, radiostacja warszawska (o sygnale wywoławczym „WAR") ulokowana była w zewnętrznym forcie Cytadeli (obecnie u wylotu Alei Wojska Polskiego na Żoliborzu) a jej antena rozpięta na dwóch stalowych 70-metrowych masztach ustawionych na dwóch sąsiednich bastionach wału fortecznego. Była ona ogniwem tranzytowym dla utrzymywania łączności między Berlinem a dowództwem wojsk niemieckich na wschodzie (*Ober Ost*) w Brześciu Litewskim via Warszawa i Poznań oraz innymi dowództwami i miastami. Jej zasięg – do 1500 km – umożliwiał nawiązanie łączności ze stolicami większości państw europejskich od Moskwy po Londyn, Paryż, Rzym, Bałkany i Skandynawię. Zdobycie nieuszkodzonej radiostacji otwierało odradzającej się Polsce okno na świat, a z drugiej strony umożliwiało czerpanie z eteru aktualnej wiedzy o wszystkim co działo się owej burzliwej „jesieni ludów" w Europie.

Po zdobyciu radiostacji, nocą z 18 na 19 listopada, nowa polska już załoga, nawiązała łączność ze szwedzką radiostacją „Saj" w Karlsborgu i za jej pośrednictwem por. Bronisław Sroka na zmianę z sierżantem Janem Pradellokiem nadali do Paryża, podpisaną dwa dni wcześniej i przetłumaczoną na język francuski depeszę, notyfikującą rządom państw wojującym i neutralnym powstanie niepodległego państwa polskiego. Ślązak Jan Predellok, z

niemieckiej załogi radiostacji, który wbrew rozkazowi nie zniszczył jej, został z czasem oficerem Wojska Polskiego, a po przejściu na emeryturę wyjechał do rodzinnych Katowic, gdzie zmarł przed wybuchem wojny. Rankiem 19 listopada 1918 r., radiostacja warszawska odebrała pokwitowanie odbioru depeszy ze Szwecji, która zobowiązała się przekazać ją do innych stolic. Również z miejsca najmniej oczekiwanego – z Poznania – z serca zaboru pruskiego, przejęty telegram przynosił krzepiące słowa: *Polski Poznań pozdrawia Warszawę*. Telegram ten wysłał Polak Stanisław Jóźwiak radiotelegrafista w służbie niemieckiej z załogi radiostacji poznańskiej, który po sposobie „gania" (nadawania) rozpoznał w nadawcy depeszy – Jana Pradelloka.

Zdobycie radiostacji warszawskiej spowodowało, że od listopada 1918 roku, zaczął napływać do stolicy, do władz państwowych i wojskowych, nieprzerwany strumień informacji o wszystkim co działo się wokół Polski i w całej Europie. Były to telegramy prasowe i dyplomatyczne, informacje o zapoczątkowanych pertraktacjach pokojowych Ententy z państwami centralnymi, o tworzącym się nowym porządku w Europie, o tworzeniu się nowych państw: Litwy, Czechosłowacki, Ukrainy Halickiej i Naddnieprzańskiej, o wstrząsach rewolucyjnych w Niemczech, o toczącej się wojnie domowej w Rosji, gdzie krzyżowały się eterze jawne i szyfrowane rozporządzenia i komunikaty oraz deklaracje bolszewickie z szyfrowanymi i podawanymi „clarem" telegramami „białych".

Stosunkowo szybko zorganizowany został w Wojsku Polskim system zorganizowanego radionasłuchu. Prowadzony był początkowo, w okresach wolnych od korespondencji własnej, przez załogi kolejnych, zdobywanych na okupantach niemieckich i austriackich radiostacji stałych: w Krakowie (od 4 listopada), w Poznaniu (od końca grudnia 1918 r.), w Przemyślu (od stycznia 1919 r.), a od wiosny 1919 r. we Lwowie. Poważnym problemem były w równym stopniu braki kadrowe jak i sprzętowe. W latach 1918–1920 służbę w elitarnych formacjach radiotelegraficznych pełniło tylko 143 oficerów (blisko połowę wykształcono już w Wojsku Polskim) i niemal trzy razy tyle podoficerów i specjalistów (dwie trzecie wyszkolono już w Wojsku Polskim). Niezbędną pomocą służyła kadra wydziałów elektrycznych Politechniki Lwowskiej i Warszawskiej. Wśród nich był student – podchorąży Wojska Polskiego, a wkrótce profesor i kapitan Wojska Polskiego Janusz Groszkowski, późniejszy prezes Polskiej Akademii Nauk[1].

Biuro Szyfrów

Zasady szyfrowania własnej korespondencji stosowana była już w Legionach Polskich podczas wojny światowej oraz w Polskiej Sile Zbrojnej. Dla umożliwienia radiotelegraficznego kontaktu Rady Regencyjnej z dowództwem I Korpusu Polskiego gen. Józefa Dowbor-Muśnickiego, przywiózł je z Warszawy do Bobrujska 19 lutego 1918 r. por. Paweł Romocki. Miały one służyć do stałej komunikacji, miedzy tą formacją a Warszawą, dla utajnienia korespondencji przed bolszewikami. Były to niemieckie systemy szyfrowe, które mimo zmiany konkretnych kluczy, dawały jednak polskiemu wywiadowi wgląd w systemy szyfrów stosowanych przez Niemcy. Jednocześnie dawały taki sam wgląd Niemców w korespondencję gen. Dowbor-Muśnickiego.

W komisji likwidacyjnej POW kierowanej przez Walerego Sławka, w Belwederze, na przełomie 1918 i 1919 r., zanim struktury wywiadu POW włączone zostały i podporządkowane Sztabowi Generalnemu i Ministerstwu Spraw Wojskowych, do kontaktu z komendami i siatkami POW w Kijowie, Mińsku, Moskwie i innych miejscach używano szyfrów peowiackich. Były więc szyfry swoistym „chlebem powszednim", wszystkich tajnych służb oraz wojska.

[1] To właśnie dlatego, że był oficerem rezerwy WP oraz miał kontakty z polskim wywiadem wojskowym, podczas II wojny światowej współpracował z wywiadem Armii Krajowej, badał fragmenty niemieckiej rakiety V1 i V2, w tym radiową aparaturę naprowadzania oraz silnika rakietowego.

W Sztabie Generalnym tworzonym od października 1918 r. w Warszawie pierwszym oficerem odpowiedzialnym za stworzenie nowych systemów szyfrowych w Wojsku Polskim był Karol Anders z armii rosyjskiej (brat. płk. Władysława Andersa). Najprawdopodobniej jednak nie poradził sobie z tym zadaniem, bowiem gdy 12 grudnia 1918 roku, nowym szefem wywiadu został ppłk Józef Rybak – jak sam odnotował w swych pamiętnikach – otrzymał polecenie zorganizowania komórki szyfrowej, faktycznie zaś centrali wywiadu, na wzór i podobieństwo austriackiego *Evidenzbiuro*. Jeszcze przed wyjazdem z Wiednia, gdzie pracował w polskiej komórce likwidacyjnej austriackiego *Kriegsministerium,* w grudniu zdobył on najważniejsze szyfry austriackie. Dzięki pomocy płk Hermana Pokornego (który po rozpadzie dualistycznej monarchii został oficerem na Węgrzech), przywiózł do Polski następujące szyfry: *Weiser-Pomil, Weiser-Assi, szyfr „M", szyfr XV, Lambda* oraz książkę nt. kryptografii: Edwarda Fleissnera von Ostrowskiego, *Handbuch der Kryptografie. Anleitung zum Chiffrieren udn Deschiffriren von Geheimchreiften*, wydaną w Wiedniu w 1881.

W tym czasie przedstawicielem wojskowym Polskiej Komisji Likwidacyjnej w Wiedniu, a następnie polskim przedstawicielem wojskowym był gen. intendent Edward Poschek. W skład misji wchodził m.in. mjr baron Emil Prochaska (który od listopada 1919 roku pełnił funkcje attaché wojskowego w Austrii), który przyjaźnił się płk Nandorem Taroczym (przedstawicielem wywiadu węgierskiego w Wiedniu). Dzięki tej przyjaźni i zażyłości, płk Taroczy nie tylko pomógł w zorganizowaniu siedziby polskiej placówki wojskowej w Wiedniu przy placu Schwarzenberga 3, ale również z polecenia ppłk Józefa Rybaka dopomógł w zdobyciu kolejnych materiałów z dawnego austriackiego Biura Szyfrów. Na „koleżeńską prośbę" ppłk Rybaka, węgierski przyjaciel zdobył w dawnym Biurze Szyfrów niezbędną dokumentację austriackich komórek szyfrowych, wzory kodów i szyfrów używanych podczas I wojny światowej w armii rosyjskiej, instrukcje prowadzenia radiowywiadu w armii austro-węgierskiej, podręczniki i księgi z zakresu kryptoanalizy. Stały się one podstawowymi pomocami naukowymi utworzonego na początku 1919 roku polskiego Biura Szyfrów.

Materiały te wykorzystał kpt. Eugeniusz Chilarski, który w połowie grudnia 1918 r. został wyznaczony przez ppłk. Rybaka na stanowisko szefa Sekcji Szyfrów Sztabu Generalnego WP. Opracował on kilka wersji pierwszych szyfrów używanych w Wojsku Polskim, oznaczonych jako szyfr „Ch"[czyli Chilarski], z dodatkiem liczby podanej cyfrą rzymską lub łacińską. Składały się nań: kod czteroliterowy – dla dowództw frontowych – utajniający podstawowe struktury organizacyjne terminy i zwroty oraz tzw. kratka szyfrowa wraz z okresowymi zmiennikami. Ponadto opracował innego rodzaju szyfr dla kontaktów z polskimi misjami wojskowymi poza granicami Polski.

Wcześniej, 3 grudnia 1918 r. przybył z Paryża (wraz ze Stanisławem Grabskim z Komitetu Narodowego Polskiego) kpt. Tadeusz Zwisłocki, który od gen. Józefa Hallera przywiózł szyfry, jakie miały być zastosowane do kontaktów władz polskich w Warszawie z KNP oraz dowództwem Armii Polskiej we Francji.

Kapitan Chilarski pełnił obowiązki szefa Sekcji Szyfrów do lutego 1919 r., gdy zastąpił go na tym stanowisku kpt. Józef Stanslicki, także z dawnej armii austro-węgierskiej, który opracował kolejne elementy polskiego systemu szyfrowania korespondencji operacyjnej: kod stacyjny – St.[czyli Sanslicki] wraz z dodanymi cyframi rzymskimi (od I do IX) oraz szyfry St.[czyli Stanslicki] I – XL (czterdzieści odmian – tzw. zmienników, zmienianych co kilka dni) do komunikacji Naczelnego Dowództwa Wojska Polskiego z placówkami zagranicznymi, Dowództwami Okręgów Generalnych, dowództwami frontowymi; natomiast dowództwa frontów i dowództwa dywizji korzystały nadal z Kodu Ch. i szyfru „Sigma" opartego na wzorach austro-węgierskich. Cała ta praca ukierunkowana była na stworzenie systemu utajniania polskiej korespondencji radiotelegraficznej, natomiast tworzenie struktur

polskiego radiowywiadu związane było z osobą mjr. Karola Bołdeskuła, przyjętego został do służby w Oddziale Informacyjno-Wywiadowczym SG WP z inicjatywy ppłk. Józefa Rybaka.

W tym czasie, jak wspomniano, już od końca listopada 1918 roku, polskie radiostacje prowadziły coraz bardziej usystematyzowany nasłuch sieci radiowych i ruchu radiowego wszystkich państw okalających Polskę. Przejmowały głównie jawne komunikaty agencyjne i informacje prasowe, ale monitorowały także wojskowe sieci radiowe, sprawdzając kto z kim porozumiewa się, jakiego rodzaju szyframi. Na tej podstawie w Oddziale Informacyjnym od pierwszych miesięcy 1919 roku sporządzane były serwisy wiadomości o każdym z państw, a przede wszystkim o sytuacji na wschodzie – w Rosji i na Ukrainie. W eterze krzyżowały się radiogramy zawierające bolszewickie dekrety i sprawozdania, komunikaty bolszewickiej agencji telegraficznej ROSTA, teksty wystąpień przywódców przesyłane z centrali do redakcji lokalnej prasy oraz agitacyjne przemówienia i propagandowe artykuły. Pośród nich sporą grupę radiogramów stanowiły teksty szyfrowane, tak przez „białych" jak i „czerwonych", łącznie z flotą czarnomorską, a także szyfrogramy emitowane przez radiostacje ukraińskie oraz węgierskie. Te ostatnie, a szczególnie wymiana korespondencji Budapesztu z Moskwą i Kijowem, tym bardziej były interesujące, że w marcu 1919 r. na Węgrzech rozpoczęła się bolszewicka rewolucja.

Nieliczne polskie ruchome radiostacje nasłuchowe rozmieścił mjr Karol Bołdeskuł niemal w tych samych miejscowościach, gdzie podczas Wielkiej Wojny, w latach 1915–1918, pracowały nasłuchowe radiostacje austriackie i niemieckie. System uzupełniały dwie stacje radiopelengacyjne (kierunkowe), usytuowane wiosną 1919 r. jedna k. Lwowa, i druga k. Białegostoku, przesunięta następnie do Wilna. Ich zadaniem była (na zasadzie krzyżowania się dwóch siecznych – wyznaczających kierunek skąd sygnał był najsilniejszy) lokalizacja radiostacji Armii Czerwonej oraz „białej" rosyjskiej Armii Ochotniczej. Dzięki temu uzyskiwano wiedzę, kto i skąd nadaje, jaki jest jego sygnał wywoławczy i zakres fal, jak są zorganizowane sieci radiowe (grupy związanych ze sobą radiostacji nadających w tym zakresie fal) i kto kieruje nim (tzw. radiostacje kierujące) – czyli kto dowodzi. W ten sposób można było zestawić strukturę organizacyjną wyższych i niższych rosyjskich związków operacyjnych (czyli frontów i armii).

Jednocześnie do dowództw Wojska Polskiego na froncie wydany został rozkaz nakazujący przesyłanie do Sekcji Szyfrów SG WP, wszystkich zdobycznych kluczy szyfrowych oraz materiału szyfrowego. W ten sposób, w kwietniu 1919 roku, do Warszawy przesłane zostały z Wilna, dwa klucze szyfrowe Armii Czerwonej „Majak" i „Mars" (ten ostatni ze „zmiennikiem" 47110), zdobyte wraz z rosyjską radiostacją podczas kwietniowej operacji na Wileńszczyźnie.

Problem był jednak z dekryptażem (łamaniem) szyfrów rosyjskich. W systemie radiowywiadu brakowało bowiem bardzo istotnego (a nawet najważniejszego) ogniwa jakim jest komórka kryptoanalityczna, która zajmowałaby się łamaniem szyfrów obcych. W tym czasie w Europie, po rozpadzie sztabu austriackiego (i jego Biura Szyfrów, który podczas Wielkiej Wojny odnotował wielkie sukcesy w zakresie łamania szyfrów rosyjskich, rumuńskich, serbskich i włoskich), a także na skutek rozpadu dawnych struktur Biur Szyfrów niemieckiego i rosyjskiego (które nie miały na swoim koncie większych sukcesów w zakresie łamania szyfrów obcych), jedynie Anglicy i Francuzi zajmowali się na większą skalę kryptoanalizą, ale ich zainteresowania ogniskowały się dotąd głównie na armii i flocie niemieckiej, więc Polska wchodząc do elitarnego kręgu państw tworzących tak wyspecjalizowane komórki kryptoanalityczne, nie była bynajmniej zapóźniona w tym zakresie.

W tym czasie, po przejściu ppłk Józefa Rybaka do służby w Ministerstwie Spraw Wojskowych, mjr Karol Bołdeksuł, z dniem 1 kwietnia 1919 r., objął funkcję szefa Oddziału Informacyjno-Wywiadowczego SG WP. Rola i główne zadanie mjr Bołdeskuła – dotyczące

zorganizowania radiowywiadu na Rosję wraz z komórką kryptoanalityczną – było tak głęboko utajnione, że nawet prominentni i najbardziej zaufani współpracownicy Józefa Piłsudskiego, nie wiedzieli o tym, krytykując oficera z d. armii austro-węgierskiej i wyrażając zdziwienia dlaczego Wódz Naczelny trzyma go na stanowisko szefa tak newralgicznego organu dowodzenia w Wojsku Polskim.

O weselu panny Sroczanki oraz Jana Kowalewskiego lekturach z dzieciństwa i grzebieniu

Tworzeniu polskiej komórki kryptoanalitycznej, owego brakującego ogniwa w strukturze radiowywiadu, dopomógł szczęśliwy przypadek, choć już w marcu 1919 roku por. Jakub Plezia z Krakowa, pełniący podczas Wielkiej Wojny służbę w austriackim Biurze Szyfrów, opracował raport w tej sprawie, jednak utknął on na trzy miesiące w sejfie dowódcy DOGen. V Kraków i dotarł do kpt. Józefa Stanslickiego dopiero w sierpniu 1919 r. Tymczasem w lipcu 1919 r. do służby w Oddziale Informacyjno-Wywiadowczym SG WP przyjęty został por. Jan Kowalewski, b. oficer rezerwy carskiej armii rosyjskiej. Porucznik Kowalewski, łodzianin, absolwent tamtejszego gimnazjum handlowego i inżynier chemii, którą studiował na Uniwersytecie w Liege, pełnił podczas wojny służbę w rosyjskich formacjach inżynieryjnych. W ich skład wchodziły pododdziały telegraficzne i radiotelegraficzne, więc znał rosyjskie procedury obowiązujące w radiotelegrafii, a co więcej pełnił też służbę w radiotelegrafie i znał zasady szyfrowania korespondencji rosyjskiej. Jednak taką samą znajomością zasad dysponowali mjr Bołdeskuł, kpt Stanslicki i por. Plezia, co nie przekładało się na praktykę łamania rosyjskich (w tym bolszewickich kluczy szyfrowych). Po rozpadzie carskiej armii por. Kowalewski wstąpił do II Korpusu Polskiego w Rosji, a następnie był oficerem wywiadu POW w Kijowie i szefem wywiadu polskiej 4 DS w Odessie (w składzie Armii Ochotniczej gen. Antona Denikina). Początki jego służby w Biurze Szyfrów opisane zostały w opublikowanej w Londynie w 1952 r. biografii Jana Kowalewskiego (tłumaczenie autora):

Pewnego dnia jego kolega porucznik Sroka, chciał iść na dwutygodniowy urlop z powodu małżeństwa swej siostry. Zapytał on Jana czy zastąpiłby go na służbie podczas jego nieobecności. Polegała ona na czytaniu przejmowanej korespondencji radiowej w różnych językach. Zawsze gotowy do pomocy Jan zgodził się. Małżeństwo uroczej panny Sroczanki zapoczątkowało serię wypadków, których następstwa wpłynęły na bieg życia Jana.

Każdego ranka o godzinie ósmej stosy z pakietami radiodepesz przejmowanych przez różne polskie stacje radiotelegraficzne były składane na biurko Jana. Potrafiący czytać niemal we wszystkich europejskich językach z łatwością dawał sobie z tym radę. Trzeciego dnia w pakiecie ze stacji radiotelegraficznej Lwów, znalazł dwa intrygujące telegramy, zapisane kaligraficznym pismem przez podchorążego, który nawet zakreślił ramkę wokół tekstu. Pierwszy telegram był adresowany do dowództwa sowieckiej XII Armii w Kijowie, podpisany przez dowódcę Grupy [Operacyjnej] *Jonę E. Jakira oraz jego szefa sztabu. Drugi był całkowicie zaszyfrowany, z wyjątkiem pierwszego słowa, „Delegat", które było ujęte w cudzysłów. Janowi, gdy patrzył na rosyjskie telegramy, zaświtała w głowie pewna myśl. Był on dobrym matematykiem, powinien sobie poradzić z ich rozwiązaniem. Wynik mógłby być interesujący*.

Tak więc ów szczęśliwy zbieg okoliczności sprowadzał się do: ślubu i wesela panny Sroczanki, lektur z dzieciństwa oraz prozaicznego grzebienia. O ile o ślubie weselu już wspomnieliśmy, cała dotychczasowa znajomość kryptoanalizy por. Jana Kowalewskiego sprowadzała się do znanych mu z dzieciństwa lektur Arthura Conan Doyle'a o *Sherlocku Holmesie* oraz noweli Edgara Alana Poe – *Złoty żuk*. Ta ostatnia opowiadała historię odczytania pirackiego szyfrogramu zapisanego sympatycznym atramentem na skórze, odczytania tekstu i odnalezienia skarbu piratów. Znaleziony przypadkowo na plaży fragment

skóry, nie większy od chustki do nosa, równie przypadkowo ogrzany nad świecą ujawnił tekst zapisany sympatycznym atramentem. Jan Kowalewski pamiętał, że niezbędne jest znalezienie punktu zaczepienia, słabego punktu szyfrogramu. W opowiadaniu *Złoty żuk*, owym „słabym punktem" (albo „punktem zaczepienia") było charakterystyczne nazwisko pirata – *Kidd* – w którym dwukrotnie występowała te same litery – *dd*. Jeśli był to szyfr podstawieniowy – literki *dd* były by zastąpione takim samym znakiem.

Jan Kowalewski znał doskonale język rosyjski, potrafił posługiwać się tym językiem niemal jak ojczystym, potrafił pisać, czytać, mówić, liczyć a nawet myśleć po rosyjsku. Znał rosyjską literaturę i poezję, język techniczny i wojskowy, z czasów służby w armii rosyjskiej poznał wojskowe procedury, schematy rosyjskich dokumentów operacyjnych oraz terminologię, zwroty, charakterystyczny „szymel" rozkazów i meldunków. W czasie wojny światowej, jako rosyjski oficer pisał i czytał oraz szyfrował dziesiątki takich dokumentów. Analogicznie jak w przypadku nazwiska pirata *Kidd*, który okazał się owym „słabym punktem" (labo „punktem zaczepienia"), Jan Kowalewski założył, że w szyfrogramie **powinno**, a w zasadzie **musi** znaleźć się słowo *dywizja*, oraz nazwisko dowódcy w podpisie, wiedział też (dzięki danym z polskich stacji kierunkowych), że depesza została nadana z Odessy, którą w języku rosyjskim pisze się przez dwa *s*.

Rosjanie używali szyfrów kratkowych, o układzie podobnym to tabliczki mnożenia, np. jeśli w pole mnożenia – 2 x 2 – wpiszemy rosyjską literę „*р*" – czyli (*r*), wówczas w szyfrogramie będzie ona oznaczona jako „22"; jeśli w pole 1 x 0 (choć to matematycznie niepoprawne) wpiszemy rosyjską literę „и" – czyli (i) wówczas będzie ona oznaczona w szyfrogramie jako „10". Słowo *dywizja*, ma w języku rosyjskim, charakterystyczny układ sylab i liter. Każda druga litera w sylabie – na którą składają się dwie litery – to litera и (i): („ди–ви–зия").

Jan Kowalewski posłużył się więc grzebieniem, z którego wyłamał zęby w regularny sposób, tak aby w miejsce po ich wyłamaniu wchodziły dwie cyfry oznaczające literki „и" i przesuwając nim po tekście szukał takiej sekwencji znaków (cyfr, które zastępowały w szyfrogramie literę „и"), gdzie co druga grupa (dwóch cyfr) będzie się powtarzała. Gdy ją znalazł, odczytał słowo dywizja. Dzięki temu dysponował już pięcioma literami, co stanowiło około 1/5 alfabetu rosyjskiego.

Kolejne litery odkrył dzięki ewidentnemu, wręcz szkolnemu błędowi szyfrujących, którzy podali nazwisko dowódcy i szefa sztabu dwukrotnie, raz tekstem otwartym (jawnym) – jak być powinno, a innym razem tekstem zaszyfrowanym. Z zasady nie wolno było szyfrować podpisów i nagłówków, bowiem były one niezmienne, a zmieniały się jedynie klucze szyfrowe. W ten sposób znając te nagłówki i nazwiska, można było metodą podkładania tekstu jawnego pod tajny, złamać klucz i odczytać szyfrogram.

Znając – ze słowa „ди–ви–зия" – litery: „и" oraz „я", mógł sprawdzić, że był to Iona Jakir („иона якир"), i poznać dzięki temu kilka kolejnych nowych liter: „о", „н", „а", „к", „р". Ponadto podwójna litera „cc" – („ss") – w słowie Odessa, umieszczonym w nagłówku i powtórzonym w treści szyfrogramu, przy znajomości: „д", „а", dopomogła, w odszyfrowaniu kilku kolejnych liter: „е" i „с". Dzięki temu poznał już 12 liter, a więc niemal połowę alfabetu. Podstawiając w szyfrogramie znane litery pod grupy cyfr, poszukiwał brakujących liter, i w ten sposób odczytywał kolejne słowa, a następnie całą treść szyfrogramu.

W ten sposób w sierpniu 1919 roku Jan Kowalewski złamał – metodą „ataku" lingwistycznego – pierwszy rosyjski szyfr o nazwie „Delegat". Fragment szyfrogramu podano poniżej:

1) Podkreślono w zaszyfrowanej formie litery „и" (czyli zestawienie dwóch cyfr: 10) w słowie: „ди–ви–зия", odnalezione i odczytane przy pomocy grzebienia;

2) Wytłuszczono w szyfrogramie wszystkie litery odnalezione przy zastosowaniu wyżej wymienionych wszystkich trzech pierwszych „słabych punktów" („punktów zaczepienia"):

„dywizja”, „Iona Jakir” i Odessa”. (Ponadto Iona Jakir – był podpisany pod depeszą.) Pozostałe litery pozostały niewytłuszczone, ale można je było odczytać i uzupełnić jak brakujące litery w popularnej „krzyżówce”;

3) Przedstawiono odtworzoną tzw. „kratkę” czyli „deszyfrant”, ujawniony klucz szyfrowy „Delegat”, użyty do zaszyfrowania radiotelegramu. Litery wytłuszczone – odczytane jak wyżej, pozostałe litery odczytane dzięki metodzie „krzyżówki”.

1) Zaszyfrowany radiotelegram (szyfrogram)

400522052343343235343110121003103443053123050135113 1

0512351110150132051235221033353423102235100305311540

4041432205100335021435121135403244431415111015121135

432235121415111010231015123 5 …

2) Odczytany radiotelegram (szyfrogram)

40	05	22	05	23	43	34	32	35	34	31	**10**	12	**10**	03	**10**	34	43	05	31	23	05	01	35	11	31
с	**о**	**р**	**о**	**к**	п	**я**	т	**а**	**я**	**д**	**и**	**в**	**и**	**з**	**и**	**я**	п	**о**	**д**	к	**о**	м	**а**	**н**	**д**

05	12	35	11	10	15	01	32	05	12	35	22	10	33	35	34	23	10	22	35	10	03	05	31	15	40
о	в	**а**	**н**	и	**е**	м	т	о	**в**	**а**	**р**	и	щ	**а**	**я**	**к**	**и**	**р**	**а**	**и**	з	**о**	**д**	**е**	**с**

40	41	43	22	05	10	03	35	02	14	35	12	11	35	40	32	44	43	14	15	11	10	15	12	11	35
с	**ы**	п	р	**о**	и	з	**а**	ш	л	**а**	в	**н**	**а**	**с**	т	у	п	л	**е**	**н**	**и**	**е**	в	**н**	**а**

43	22	35	12	14	15	11	10	10	23	10	15	12	35	…
п	**р**	**а**	в	л	**е**	**н**	**и**	**и**	**к**	**и**	**е**	в	**а**	

3. Odtworzony deszyfrant (klucz) szyfru „Delegat” („Делегат”)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	
0		м	ш	**з**	ю	**о**					**0**
1	**и**	**н**	**в**	г	л	е					**1**
2	ж	б	**р**	**к**	ц	ь					**2**
3	ф	**д**	т	щ	**я**	**а**					**3**
4	с	ы	ч	п*	у	х					**4**
5											**5**
6											**6**
7											**7**
8											**8**
9											**9**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	

*****W oryginale deszyfrantu w kratce tej wpisany jest znak zapytania (**?**), ale z analizy zestawu liter wynika, że brakującą literą była litera (**п**).

Jak odnotował w swych wspomnieniach por. Jan Kowalewski: (…) *złamanie i odczytanie tekstu przyniosło sensacyjne informacje.* Nazajutrz, poinformowany o tym szef Oddziału Informacyjno-Wywiadowczego, ppłk Karol Bołdeskuł w lot zrozumiał wagę sukcesu por. Jana Kowalewskiego – *Złamanie rosyjskich szyfrów ... zelektryzowało Naczelne Dowództwo*

Wojska Polskiego. Szef Sztabu Generalnego [oraz szef wywiadu wojskowego] (...) *polecił Janowi zorganizowanie* (...) [komórki] *dekryptażu.* (...) *Porucznik Jan Kowalewski* (...) *osiągnął bardzo wysoki poziom skuteczności, tak że Polacy czytali* [od tego czasu] *praktycznie wszystkie telegramy wysyłane i odbierane przez Armię Czerwoną.*

W ciągu zaledwie dwóch tygodni, utworzona została w Sekcji Szyfrowej (Oddziału II Informacyjno-wywiadowczego SGWO) – przekształconej w Biuro Szyfrów – nowa komórka organizacyjna pod nazwą „Wydział II Szyfrów Obcych", na czele której stanął Jan Kowalewski. Zatrudniono w niej kilku młodych oficerów o nieszablonowych metodach działania, co charakterystyczne zwartą grupę stanowili wśród nich instruktorzy harcerscy i harcerze ze wszystkich trzech zaborów, osobowości o „swędzących mózgach", jak mówił o nich Jan Kowalewski: por. Jakub Plezia (komendant hufca i komendant chorągwi w Krakowie), ppor. Maksymilian Ciężki (drużynowy i komendant Hufca w Szamotułach), por. Jerzy Suryn (zastępowy w polskiej drużynie harcerskiej w Odessie). Nieprzypadkowo, gdy por. Jan Kowalewski, przed awansem na stopień kapitana musiał w końcu 1920 roku odbyć praktykę frontową, wybrał dowodzenie kompanię w 6 harcerskim pułku piechoty (wojsk Litwy Środkowej).

Złamanie pierwszego klucza szyfrowego Armii Czerwonej i utworzenie Wydziału II Szyfrów Obcych, wypełniło brakujące ogniwo w systemie radiowywiadu. Odtąd nasłuch i przejmowanie jawnej i tajnej korespondencji przeciwnika, ustalanie elementów „ruchu radiowego" oraz lokalizowanie nieprzyjacielskich radiostacji – dopełnione zostało komórką najważniejszą zajmującą się kryptoanalizą, (dekryptażem) czyli łamaniem nieprzyjacielskich szyfrów. Kolejnym etapem tworzenia struktury radiowywiadu było stworzenie komórek kryptoanalitycznych w dowództwach frontów i armii, gdzie na podstawie złamanych w Wydziale II SO BS kluczy szyfrowych, odczytywano na miejscu, na froncie korespondencję przeciwnika, bez potrzeby dwukrotnego przesyłania (z frontu do Warszawy i z powrotem) szyfrowanej i odczytanej korespondencji.

Stworzenie takiego systemu na przełomie 1919 i 1920 r. umożliwiło szybkie odczytywanie korespondencji bolszewickiej ze wszystkich frontów wojny domowej na Ukrainie, w południowej Rosji, na Syberii i na Kaukazie. Jan Kowalewski złamał także szyfry używane przez Armię Ochotniczą gen. Antona Denikina oraz „białą" Flotę Czarnomorską, a także stosowane przez Armię Ukraińskiej Republiki Ludowej (Naddnieprzańskiej). Dało to możliwość śledzenia wydarzeń na rozległych terenach Rosji od Syberii po Piotrogród i od Murmania po Morze Czarne.

Z czasem doszły jednak nowe problemy. Jak zapisał w swych wspomnieniach Jan Kowalewski, o kluczu „Delegat": *Był on nieskomplikowanym szyfrem, w którym dwie cyfry zastępowały jedną literę alfabetu. Do rzędu cyfr otrzymywanych w ten sposób, dodawanych było* [na początku] *dwanaście cyfr* [specjalnego] *klucza. Szyfr po zastąpieniu liter przez cyfry był stałym* [szyfrem podstawowym]*, ale dwanaście cyfr klucza ulegało zmianie. Było tam sześć odrębnych grup cyfr, skąd brało się sześć* [kolejnych] *wersji szyfru „Delegat".*

Podobny zapis znajduje się na zachowanym deszyfrancie (odtworzonym kluczu) „Delegata" – czyli wzorze złamanego klucza szyfrowego: *Odszyfrował Kowalewski por. i oprócz tego dostarczony z niektórymi zmiennikami przez B*[iuro] *W* [ywiadowcze]. *Często była używana baza* [wersja podstawowa] *bez zmiennika i w takich wypadkach na początku depeszy umieszczano hasło „biez pokazitiela, albo nie podawano (czasem „Dieliegat", lub „Dieliegat biez pokazitiela). System szyfrowania ten sam co w poprzednich. Jeżeli stosowano zmiennik to pisano „dieleiegat pierwyj", „dieliegat wtoroj", itp. Zmienników zastosowano 7* [wersji]. *Przy szyfrowaniu zmiennika pod podstawowym szyfrogramem podpisywano współczynnik, raz w porządku normalnym, następnie odwrotnym i tak na zmianę do końca.*

Wspomnienia Jana Kowalewskiego oraz opis na deszyfrancie wskazują na problemy, które pojawiły się wkrótce, w kolejnych wersjach „Delegata", a dotyczyły tzw. zmienników –

czyli *pokazitieli*. W korespondencji Armii Czerwonej i WuCzeKa (bolszewickiej policji politycznej), Rosjanie zaczęli stosować szyfry podwójnego przekształcenia, dla złamania którego metoda lingwistyczna okazywała się niewystarczająca.

Szyfrowanie przy pomocy „Delegata" ze zmiennikiem (*pokazitieliem*), polegało na odjęciu od pierwotnej wersji szyfrogramu przemiennie zastosowanego zbioru sześciu cyfr tzw. zmiennika (w kilku jego kolejnych wersjach). Były one, jak czytamy we wspomnieniach Jana Kowalewskiego, dopisane następnie napisane na początku szyfrogramu, ale tego początkowo nie wiedziano. W ten sposób od zaszyfrowanego pierwszy raz radiogramu, odejmowano zmiennik, co stanowiło wtórne szyfrowanie i do powstałego w ten sposób rzędu cyfr (stanowiących różnicę) dopisywano na początku szyfrogramu ów dwunastocyfrowy zmiennik (np. „Delegat I": 517382-283715).

Od zaszyfrowanego szyfrem „Delegat" teksty radiogramu odejmujemy zapisany przemiennie sześciocyfrowy zmiennik:

400522052343343235343110121003103444053123050135113 1…

517382283715517382283715517382283715517382283715517 3…

9932408796388369531604056147219207385468418774206068 …

Różnica stanowiła nowy, drugi raz (wtórnie) przekształcony szyfrogram, który zapisywano z dodaniem (wytłuszczonego tu) zmiennika na początku:

5173822837159932408796388369531604056147219207385468418774206068 …

Tak dwukrotnie przekształcony tekst nie poddawał się już „atakowi" lingwistycznemu. Jan Kowalewski szybko jednak odkrył stosowanie przez Rosjan metody wtórnego (podwójnego) szyfrowania przy pomocy zmienników, ale gdy z czasem przestano umieszczać na początku szyfrogramu, podając je jedynie w pakietach (do nadawców i odbiorców) na kolejne tygodnie, wówczas „stanął przed ścianą". Ponadto kratka szyfrowa (oparta na kratce tabliczki mnożenia) miała 100 pól, tymczasem alfabet rozpisany w podstawowej wersji zajmował zaledwie czwartą część pól, więc Rosjanie, aby utrudnić stosowanie metody „ataku" lingwistycznego, w kolejnych kluczach – używane najczęściej samogłoski – dublowali albo potrajali. W takiej sytuacji metoda statystycznego badania tzw. „frekwencji" – czyli częstotliwości występowania liter w odpowiednio dużym materiale, nie przynosiła dobrych rezultatów. Gdy wszystkie dotychczas stosowane metody zawiodły, nie zawiodła por. Jana Kowalewskiego intuicja. Zwrócił się on (za zgodą szefa Oddziału Informacyjno-Wywiadowczego ppłk Bołdeskuła) do profesorów matematyki Uniwersytetu Warszawskiego i Lwowskiego: Stefana Mazurkiewicza, Wacława Sierpińskiego i Stanisława Leśniewskiego. Byli to znamienici naukowcy, współtwórcy polskiej szkoły matematycznej. Włączeni do pracy, konstruowali algorytmy pozwalające na odnalezienie zmienników co zapoczątkowało – nieznany dotąd – podwójny: lingwistyczny i matematyczny „atak" na szyfry. Włączeni do pracy wraz ze swymi asystentami z wydziału filozofii Uniwersytetu Warszawskiego konfrontowali swą wiedzę matematyczną z doświadczeniami i umiejętnościami w zakresie terminologii wojskowej z oficerami Wydziału II BS. Zapoczątkowana wówczas współpraca, uwieńczona została w przyszłości – oczywiście w nieporównywalnie większej skali – jednym z największych sukcesów Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego, którzy łącząc metody lingwistyczne i matematyczne złamali szyfry maszynowe „Engimy". Byli oni uczniami prof. Zdzisława Krygowskiego z Uniwersytetu Poznańskiego, prof. Krygowski włączony został w tajemnice kryptoanalizy przez swych kolegów pracujących w Biurze Szyfrów od końca 1919 roku.

Sukcesy polskiego radiowywiadu

Radiowywiad w pełnej swej strukturze miał niezwykłe walory natury operacyjnej i politycznej, dawał bowiem informacje: 1) aktualne, 2) wiarygodne oraz 3) dotyczące niezwykle szerokiego spektrum spraw.

– Aktualne ponieważ, żaden agent polskiego wywiadu nie zdążyłby przesłać informacji z miejsca ich zdobycia do centrali w Warszawie (lub na polską stronę frontu, co zajmowało od kliku dni do kilku tygodni) w czasie w jakim odczytywane były nieprzyjacielskie szyfrogramy (na podstawie ustalonego klucza trwało to kilkanaście minut, a łamanie nowych kluczy zajmowało od kilku godzin do kilku dni (jeśli był to szczególnie trudny nowy klucz szyfrowy).

– Wiarygodne, ponieważ mogły być one i były natychmiast sprawdzalne, a rosyjskie sztaby podczas wojny i długo po niej nie dopuszczały myśli, że ich „stojące na wysokim stopniu trudności" systemy szyfrowe mogły być złamane przez „jakichś Polaków". Posługiwali się więc swoimi szyframi „bezkarnie", a cała przesyłana przez radiotelegraf korespondencja trafiała równocześnie do rosyjskich i polskich odbiorów.

– Wreszcie, jeśli chodzi o spektrum wiedzy, to żaden polski agent, a nawet Lenin, Trocki i Stalin, gdyby tylko byli agentami polskiego wywiadu, nie mieli tak szerokiego dostępu do różnego rodzaju informacji, ani też nie byli by wstanie tak szybko przekazać ich na polską stronę.

Owoce pracy polskiego radiowywiadu dawały więc najwyższym polskim czynnikom wojskowym i politycznym, a przede wszystkim Naczelnikowi Państwa i Wodzowi Naczelnemu – Józefowi Piłsudskiemu oręż szczególny, niezwykle ważny w polityce zagranicznej i działaniach wojennych. Marszałek Piłsudski posiadał również dostęp do informacji pochodzących z deszyfrowanych radiogramów władz cywilnych i wojskowych państw sąsiadujących z Polską: Niemiec, Litwy, Węgier i Czechosłowacji.

Łącznie podczas wojny z bolszewicką Rosją, od sierpnia 1919 roku – do końca 1920 roku Jan Kowalewski i kierowany przezeń Wydział II Szyfrów Obcych złamał około 100 rosyjskich kluczy szyfrowych i odczytał ponad trzy tysiące szyfrogramów bolszewickich (nie licząc „białych" Rosjan, ukraińskich, czeskich, niemieckich i węgierskich), tyle bowiem autor niniejszego artykułu zestawił w przebadanych aktach polskiego wywiadu wojskowego, znajdujących się w Polsce i w Moskwie.

Klucze szyfrowe zmieniane były przez Rosjan co ok. dwa tygodnie do 10 dni. Na tyle oceniali oni zdolności polskiego wywiadu. Złamanie bowiem szyfru po upływie tygodnia – dwóch, dawało dostęp jedynie do zdezaktualizowanych i bezużytecznych informacji. Tymczasem łatwiejsze rosyjskie klucze szyfrowe Jan Kowalewski łamał w ciągu dwóch godzin, a trudniejsze dwa dni.

I jeśli w ówczesnej Europie, w której mapa polityczna po I wojnie światowej uległa ogromnej przebudowie, wytyczymy linię od półwyspu jutlandzkiego do półwyspu apenińskiego, na zachód od tej linii funkcjonowały w Paryżu i Londynie dwie sprawne, budowane przez dziesięciolecia (a nawet stulecia) struktury wywiadu i biura szyfrów zajmujące się kryptoanalizą. O tyle po I wojnie światowej, na wschód od ww. linii, jeden z najsprawniejszy wywiadów, a w jego ramach najnowocześniejszy radiowywiad i Biuro Szyfrów, powstały w Warszawie. Ani Berlin, ani Wiedeń, ani Moskwa nie odgrywały w tym czasie takiej roli jak dawniej. To pozwala zrozumieć, dlaczego zarówno działania wojenne, jak i polityka polska prowadzona była w tym czasie racjonalnie i skutecznie.

Znaczenie radiowywiadu – lustro Piłsudskiego

Na fotografiach i karykaturach Józef Piłsudski przedstawiany był często, gdy siedział w fotelu i układał na niewielkim stoliku ulubione pasjanse. Wyobraźmy sobie, że fotel i stolik są takie same, tyle, że zamiast układać pasjansa, Marszałek gra w pokera z Leninem. Za plecami przeciwnika ustawione jest niewidzialne dlań lustro, więc Piłsudski zerkając w lustro wie jakimi kartami dysponuje Lenin, wie że szachruje, widzi jak wyciąga karty z rękawa, jak licytuje z kamienną twarzą, aby przechytrzyć Piłsudskiego. Ale Marszałek, mruży oczy i ściąga brwi i sam stara się ograć przeciwnika. Gra toczy się o wysoką stawkę.

Owym niewidzialnym lustrem ustawionym za plecami przeciwnika był polski radiowywiad. Oczywiście samym zerkaniem w lustro i wiedzą o tym, jaką ma kartę przeciwnik nie można wygrać partii z doświadczonym szulerem. Polski Wódz Naczelny i Naczelnika Państwa, musi także mieć mocną kartę, tą było waleczne wojsko i postawa Narodu, pomoc materialna z Francji i Stanów Zjednoczonych. Ale w pokerze o wyniku rozgrywki decyduje nie tylko mocna karta w rękach Piłsudskiego, ale również żelazna konsekwencja gracza, jego zdolności i charakter. Potrzebna jest także odrobina szczęścia, ale temu można dopomóc zerkaniem w karty przeciwnika. Wgląd w atuty Lenina, dzięki owemu niewidzialnemu dlań lustru, dawał przewagę, dawał możliwość prowadzenia rozgrywki nie „w ciemno", nie zdając się na łut szczęścia i ślepy los, ale optymalnego licytowania, oceniania szans, dobierania kart, podbijania stawki, albo sprawdzania i wreszcie ograniа przeciwnika.

Doświadczenia i sukcesy polskiego radiowywiadu podczas wojny z bolszewicką Rosją, zaowocowały nawiązaniem ścisłej współpracy w tej dziedzinie z Japonią. Jan Kowalewski w 1923 roku został skierowany służbowo do Tokio, gdzie stworzył podstawy radiowywiadu japońskiego ukierunkowanego na Rosję. Polska (radiostacje w Wilnie, Lwowie,) oraz Japonia (radiostacje wybudowane w Mandżurii) monitorowały do 1939 r. rosyjskie sieci radiowe na całym obszarze Związku Sowieckiego. Łamaniem rosyjskich szyfrów zajmowała się sekcja rosyjska Biura Szyfrów kierowana przez kpt. dr Stanisława Szachno-Romanowicza.

Łamanie szyfrów niemieckich zapoczątkowane zostało w Polsce w 1920 r., gdy francuski wywiad wojskowy udostępnił polskiemu wywiadowi informacje o, stosowanych podczas I wojny światowej szyfrach niemieckich, tzw. „podwójnych zmienników" (albo „przestawienia podwójnego", czy „transpozycyjnego") – *Doppelwürfelverfahren* oraz *Handschlüsselverfahren*. Dzięki temu polskie władze wojskowe i polityczne kontrolowały korespondencję wojskową Niemiec. Miało to swe szczególne znaczenie podczas plebiscytu na Górnym Śląsku i III Powstania Śląskiego w 1921 roku, gdy, awansowany do stopnia kapitana Jan Kowalewski został szefem wywiadu polskiego Dowództwa Ochrony Plebiscytu, a następnie szefem wywiadu Dowództwa Wojsk Powstańczych.

Radiowywiad na Niemcy prowadziły, wybudowane w latach dwudziestych nowoczesne radiostacje nasłuchowe w Starogardzie (Gdańskim), Poznaniu oraz w Krzesławicach k. Krakowa. Sekcja niemiecka Biura Szyfrów (BS–4), łamała na bieżąco, wszystkie stosowane ówcześnie szyfry niemieckie, aż do drugiej połowy lat dwudziestych. W 1926 roku niemieckie siły morskie, a w 1928 roku *Reichswehra* – jako pierwsze w Europie – wprowadziły do użytku maszyny szyfrowe „Enigma". Profesor Stefan Mazurkiewicz, którego konsultowano w zakresie nowych niemieckich szyfrów określił je jako maszynowe i nie dające się złamać przy pomocy tradycyjnych metod, niemniej przekazał sugestie dotyczącego prac nad nimi swemu przyjacielowi prof. Zdzisławowi Krygowskiemu z wydziału matematyki Uniwersytetu Adama Mickiewicza. Wkrótce polskie Biuro Szyfrów zareagowało zorganizowaniem tam kursu kryptoloanalitycznego. Zajęcia prowadzili na nim mjr Franciszek Pokorny, Maksymilian Ciężki i inż. Antoni Palluth, wszyscy oni mieli doświadczenia w łamaniu, począwszy od 1919 r., szyfrów rosyjskich i niemieckich. Stosowali metody „ataku" lingwistycznego i matematycznego na niemieckie szyfry, co wkrótce doprowadziło do sukcesu. Trzech absolwentów kursu: Marian Rejewski (studiujący następnie w Getyndze), Jerzy Różycki i Henryk Zygalski, zostało zatrudnionych w sekcji niemieckiej Biura Szyfrów (BS–4) i w końcu 1932 roku ich prace zostały uwieńczone sukcesem. W ten sposób doświadczenia z lat walk o niepodległości i granice Rzeczypospolitej 1918–1921, wykorzystane zostały z sukcesem podczas II wojny światowej.

Racjonalni oficerowie Reichswehry, wiedząc, że „Enigma" daje więcej kombinacji matematycznych niż ilość atomów we wszechświecie, lub też sekund od wielkiego wybuchu – nie dopuszczali myśli, że ktokolwiek byłby zdolny do złamania szyfrów maszynowych, tym

bardziej, że z każdym (cotygodniowym – przed wojną, a podczas II wojny światowej – codziennym) nastawieniem maszyny, uzyskiwało się nową wersję szyfru.

Marian Rejewski, wywodził się z Bydgoszczy w zaborze pruskim. Ze szkoły oraz studiów matematycznych w Getyndze wyniósł doskonałą znajomość języka niemieckiego, którym potrafił posługiwać się równie biegle jak ojczystym. Potrafił pisać, czytać, mówić, liczyć a nawet myśleć po niemiecku. Znał niemieckie idiomy, poezję i przyzwyczajenie do systematyczności oraz porządku, znał z kursów kryptograficznych wojskowe procedury, schematyczny język dokumentów szkoleniowych i operacyjnych w armii niemieckiej, terminologię i zwroty, charakterystyczny układ tekstów rozkazów i meldunków. Znajomość kultury rosyjskiego zaborcy, która – Janowi Kowalewskiemu ułatwiła złamanie szyfrów rosyjskich w latach 1919–1920, Marianowi Rejewskiemu pomogła w rozwiązywaniu szyfrów niemieckich. Obaj zaborcy, wykształcili polskich pogromców swoich szyfrów, ale najważniejszym czynnikiem który przysłużył się łamaniu szyfrów wroga była oprócz znajomości języka i zwyczajów nieprzyjaciela – matematyka, polska szkoła matematyczna, szkoła logicznego myślenia, która jest źródłem i kwintesencją nauki.

Bibliografia:

[Judith Hare] The Countness of Listowell, *Crusader in the secret war*, London 1952;

David Kahn, *Łamacze kodów. Historia kryptologii (The Codebreakers. The story od Secret Writing*, London–New York), Warszawa 2004;

Grzegorz Nowik, *Zanim złamano „ENIGMĘ”... Polski radiowywiad podczas wojny z bolszewicką Rosją 1918–1920*, cz. 1, Warszawa 2004;

Grzegorz Nowik, *Zanim złamano „ENIGMĘ” rozszyfrowano „REWOLUCJĘ”... Polski radiowywiad podczas wojny z bolszewicką Rosją 1918–1920*, cz. 2, Warszawa 2010;

Marian Rejewski 1905–1980. Życie ENIGMĄ pisane, (praca zbiorowa), Bydgoszcz 2005;

Marian Rejewski 16 VIII 1905–13 II 1980. Bydgoszczanin, wybitny matematyk, genialny kryptolog, pogromca ENIGMY, „Przegląd Historyczno-Wojskowy” R. VI (LVII), Nr specjalny 5 (210), (red. naczelny Grzegorz Nowik) Warszawa 2005;