Marian Rejewski

W s p o m n i e n i a

z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego

w latach 1930 - 1945.

Marian Rejewski

W s p o m n i e n i a
z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930 - 1945.

W s t ę p.

Kryptologia, czyli nauka o szyfrach, nie ma wielu adeptów. W Polsce, w okresie międzywojennym, samodzielnych kryptologów nie było nawet dziesięciu. Kilku zabrała śmierć w czasie wojny, kilku innych, jeżeli nie zmarło po wojnie, rozproszonych jest po świecie. W Kraju jestem w chwili obecnej z pewnością jedynym przedstawicielem ich przedwojennej garstki.

W czasie drugiej wojny światowej, kiedy łączność utrzymywano przeważnie drogą radiową, szyfry odgrywały niemałą rolę. Stanowiły broń swoistego rodzaju. Udział Polaków w skutecznym wykorzystywaniu tej broni we walce z Niemcami był nader poważny. Koncentrował się głównie w Biurze Szyfrów Oddziału II Sztabu Głównego i jego późniejszych odpowiednikach. To co mi było wiadomym o pracy i sukcesach komórki szyfrów niemieckich przed i w czasie wojny i co mi jeszcze nie uleciało z pamięci, starałem się przedstawić na niniejszych kartkach.

I.

Stałą pracę w Biurze Szyfrów rozpocząłem dnia 1.IX.1932 roku, ale pierwszy mój kontakt z Biurem Szyfrów nastąpił już kilka lat wcześniej, nie pamiętam dokładnie, czy to było z końcem roku 1928, czy z początkiem roku 1929. Wówczas to kierownictwo Biura Szyfrów zorganizowało w Poznaniu wśród studentów kończących studia matematyczne i władających biegle językiem niemieckim kurs kryptologii.

Spotkanie z przedstawicielami Biura Szyfrów nastąpiło w lokalu Instytutu Matematycznego Uniwersytetu Poznańskiego, którego kierownikiem był dziś już nie żyjący prof. Zdzisław Krygowski. Przedstawicielami Biura Szyfrów w czasie spotkania i jednocześnie wykładowcami na kursie, który niedługo potem się rozpoczął, byli: mjr Pokorny, ówczesny szef Biura Szyfrów, por. Maksymilian Ciężki, kierownik komórki szyfrów niemieckich i Antoni Palluth, pracownik cywilny tegoż Biura. Studentów obecnych było dwudziestukilku, wybranych przez prof. Krygowskiego, ale zapewne i II Oddział dokonał uprzednio odpowiedniej selekcji.

W czasie kursu trwającego kilka miesięcy /dwa razy w tygodniu wieczorami po kilka godzin/ zapoznano uczestników z podstawowymi pojęciami z dziedziny szyfrów, z klasyfikacją szyfrów i z niektórymi elementarnymi metodami rozwiązywania szyfrów. Stosunkowo dużo czasu poświęcono na zapoznanie nas z teorią i praktyką rozwiązywania szyfru zwanego przestawieniem podwójnym. Szyfr ten był wówczas w ogólnym użyciu przez niemieckie wojska lądowe i istnienie komórki szyfrów niemieckich opierało się w pewnym stopniu na tym, że umiano rozwiązywać telegramy radiowe zaszyfrowane przy pomocy wspomnianego szyfru.

Szyfr ów, zwany przez Niemców początkowo Doppelkasten-verfahren, a później Handschlüsselverfahren, opisany jest w istniejącej lite-

raturze fachowej. W szczególności w jednym z podstawowych francuskich dzieł z dziedziny kryptologii, z którym miałem możność zapoznać się w czasie wojny, lecz którego autora niestety już nie pamiętam, przedstawiony był sposób rozwiązywania tego szyfru identycznie tak samo, jak to uczyniono w czasie kursu. Nie ulega więc wątpliwości, że Biuro Szyfrów w czasie urządzania kursu było już w posiadaniu omawianego dzieła. Ale wydaje się, że wcześniejsze, samodzielne próby rozwiązania szyfrów przez polskich kryptologów nie dały pozytywnych wyników. Tak przynajmniej można by wnioskować ze słów jednego z wykładowców, który w czasie kursu wspomniał mimochodem, że jeden z profesorów matematyki Uniwersytetu Warszawskiego /później dowiedziałem się, że był to prof. Mazurkiewicz/ proszony o pomoc oświadczył, że szyfr jest nierozwiązalny.

Po zakończeniu kursu stworzono w Poznaniu małą ekspozyturę Biura Szyfrów mieszczącą się w suterynach Komendy Miasta znajdującej się wówczas przy ul. Św. Marcina w bezpośrednim sąsiedztwie Zamku. A ponieważ w Zamku mieścił się Instytut Matematyczny, przeto lokalizacja ekspozytury była niezwykle dogodna dla tych kilku osób, które zaangażowano do pracy, to jest dla mych kolegów kończących studia i dla mnie będącego wówczas asystentem Instytutu. Dla ścisłości nadmieniam, że zacząłem w ekspozyturze pracować później od swych kolegów, gdyż po ukończeniu studiów w marcu 1929 roku opuściłem Poznań i udałem się do Getyngi w Niemczech, by wrócić dopiero w jesieni 1930 roku dla objęcia proponowanej mi przez prof. Krygowskiego asystentury.

W pracy naszej w ekspozyturze nie byliśmy krępowani żadnymi godzinami, każdy mógł pracować, kiedy mu było najdogodniej, z tym tylko, że każdy winien był przepracować 12 godzin tygodniowo. Praca nasza polegała wyłącznie na rozwiązywaniu w dalszym ciągu przestawienia podwójnego, bo klucze szyfru zmieniały się co 24 godziny i trud rozwiązywania trzeba było podejmować codziennie na nowo. Trud

pesz była, o ile pamiętam, nieciekawa, w przeważającej mierze były to depesze ćwiczebne. Tyle w każdym razie można powiedzieć o tych kilku, przeważnie krótkich, depeszach, które służyły do odtworzenia klucza. Treść pozostałych, nieraz bardzo długich, wieloczęściowych depesz była nam nieznana, więc bardzo jest możliwym, że z punktu widzenia wywiadu wojskowego były interesujące. Nie trudziliśmy się, by je odczytać, nie było to zresztą naszym zadaniem, lecz cały materiał szyfrowy z danego dnia, po odtworzeniu klucza, odsyłaliśmy dla dalszej eksploatacji do Centrali do Warszawy.

A oto, w możliwie największym skrócie, opis szyfru i jego deszyfrażu:

Szyfrant otrzymuje dwa rzędy liczb zwanych kluczami "A" i "B". Długość kluczy i porządek liczb w kluczach zmieniana jest codziennie. Długość kluczy waha się w granicach od 16 do 29. Zmiana porządku liczb w kluczach polega na przestawieniu kolejnych liczb naturalnych w granicach klucza czyli, w terminologii matematycznej, na permutacji tych liczb.

Niech na przykład dla określonego dnia dane są następujące klucze

A /17/: 9, 4,16, 8,11, 3,13, 6,17, 2,15,10, 1,12, 5,14, 7

B /19/: 9, 6,14,11, 1,17, 5,13, 4,16,12, 2,19, 7,10,15, 3,18, 8

i niech szyfrant ma za zadanie zaszyfrować następujący tekst:

Das Lied von der Glocke. Ein Gedicht von Schiller.

Szyfrant naprzód preparuje odpowiednio tekst. Preparacja polega na tym, że poszczególne słowa oddziela literami X i że bigram ch zastępuje jedną literą Q. Poza tym, ponieważ przepis wymaga, by szyfrogram nie zawierał mniej niż 50 liter, uzupełnia tekst w razie potrzeby dalszymi X-ami na końcu lub w środku depeszy:

DASXLIEDXVONXDERXGLOCKEXXEINXGEDIQTXVONXSQILLERXXX

Następnie na kratkowanym papierze wypisuje klucz "A" i pod

nim w odcinkach 17-literowych /bo taka jest w danym dniu długość klucza "A"/ wypisuje spreparowany tekst, tak by pod poszczególnymi liczbami klucza znalazły się po jednej literze tekstu:

9	4	16	8	11	3	13	6	17	2	15	10	1	12	5	14	7
D	A	S	X	L	I	E	D	X	V	O	N	X	D	E	R	X
G	L	O	C	K	E	X	X	E	I	N	X	G	E	D	I	Q
T	X	V	O	N	X	S	Q	I	L	L	E	R	X	X	X	

tabl. "A"

Ostatni wiersz tablicy "A", bo tak nazwiemy tę tablicę, nie musi być pełny. Następnie wypisuje szyfrant na kratkowanym papierze klucz "B" i pod nim w poziomych wierszach 19-literowych /bo taka jest w danym dniu długość klucza "B"/ wypisuje kolejne kolumienki liter z tablicy "A", poczynając od kolumienki XGR znajdującej się pod liczbą 1 klucza "A" i kończąc na kolumience XEI znajdującej się pod liczbą 17 klucza "A". W ten sposób utworzy się tak zwana tablica "B"

9	6	14	11	1	17	5	13	4	16	12	2	19	7	10	15	3	18	8
X	G	R	V	I	L	I	E	X	A	L	X	E	D	X	D	X	Q	X
Q	X	C	O	D	G	T	N	X	E	L	K	N	D	E	X	E	X	S
R	I	X	O	N	L	S	O	V	X	E	I							

Tablica "B"

Wreszcie przepisuje w poziomych grupach po 5 liter pionowe kolumienki tablicy "B", poczynając od kolumienki IDN znajdującej się pod liczbą 1 klucza "B" i kończąc na kolumience EN znajdującej się pod liczbą 19 klucza "B" i w ten sposób otrzymuje gotowy szyfrogram

IDNXX IXEXX VITSG XIDDX SXQRX EVOOL LEENO RCXDX AEXLG LQXEN

W nagłówku szyfrogramu umieszcza jeszcze sygnały stacji nadawczej i stacji odbiorczej oraz długość depeszy. Depesza powinna zawierać nie mniej niż 50 liter i nie więcej niż 180 liter. Dłuższe teksty należy dzielić na kilka części.

Deszyfrowanie odbywa się w sposób podobny jak szyfrowanie,

z tym tylko, że wszelkie czynności należy teraz wykonać w kolejności odwrotnej. Deszyfrant po otrzymaniu szyfrogramu sprawdza więc naprzód, czy ilość liter szyfrogramu zgadza się z liczbą podaną w nagłówku, następnie na kratkowanym papierze wypisuje klucz "B", a pod nim rysuje kontur w kształcie /przeważnie/ nieregularnego prostokąta, którego dolny bok jest /na ogół/ załamany, tak aby ilość kratek wewnątrz prostokąta była równa długości szyfrogramu. Przypadkowo może się zdarzyć, że prostokąt będzie regularny i jego dolny bok nie będzie załamany, wtedy mianowicie, gdy długość szyfrogramu jest wielokrotnością długości klucza "B". Na ogół jednak prostokąt jest węższy po prawej, a szerszy po lewej stronie. W naszym przykładzie, gdy długość szyfrogramu wynosi 50, kontur winien mieć kształt następujący

9	6	14	11	1	17	5	13	4	16	12	2	19	7	10	15	3	18	8
				I							X							
				D							K							
				N							I							

kontur "B"

to jest składać się z dwóch pełnych wierszy po 19 kratek i z trzeciego, niepełnego wiersza o 12 kratkach. Do tego konturu szyfrant wpisuje pionowymi kolumienkami od góry w dół kolejne litery szyfrogramu IDNXKIXEXX....., poczynając od wypełniania kratek znajdujących się pod liczbą 1 klucza "B", potem pod liczbą 2 klucza "B" itd i w ten sposób w końcu otrzyma tablicę "B", jak na str.5. Z kolei deszyfrant wypisuje na kratkowanym papierze klucz "A" i pod nim nowy kontur

9	4	16	8	11	3	13	6	17	2	15	10	1	12	7
					I				V			X		
					E				I			G		
					X				L			R		

kontur "A"

który w naszym przykładzie powinien składać się z dwóch pełnych wierszy po 17 kratek i jednego niepełnego wiersza z 16 kratek. Wpisując do tego konturu pionowymi kolumienkami z góry w dół litery tablicy "B", tak jak następują po sobie w poziomych wierszach XGRVIL....., poczynając od wypełniania kratek znajdujących się pod liczbą 1 klucza "A", potem pod liczbą 2 klucza "A" itd, deszyfrant otrzyma w końcu tablicę "A", jak na str. 5, z której bezpośrednio, wzdłuż poziomych wierszy, może odczytać kler czyli tekst pierwotny.

Opisaliśmy powyżej, jak odbywa się, a raczej jak w okresie przedwojennym odbywało się szyfrowanie i deszyfrowanie tekstów przy pomocy systemu zwanego "Doppelkastenverfahren". Interesuje nas jednak daleko więcej, jak szyfr ten się rozwiązuje, to znaczy jak odtwarza się bez znajomości kluczy pierwotną treść depesz tym systemem zaszyfrowanych i jak wchodzi się w posiadanie samych kluczy.

Metoda rozwiązywania szyfru opiera się na uwadze, że przy dostatecznie dużym materiale szyfrowym pochodzącym z tego samego dnia nie wszystkie depesze będą miały różne długości, lecz że zawsze znajdzie się, szczególnie wśród krótszych depesz, kilka o tej samej liczbie liter. Jest rzeczą zrozumiałą, że wszystkie depesze tej samej długości /i z tego samego dnia/ można uważać jako zaszyfrowane tym samym sposobem. Jeżeli więc wypiszemy je, jedną pod drugą, literę po literze, na odpowiednio długiej taśmie papieru, potem taśmę rozetniemy na pionowe paski, tak by na każdym pasku było po jednej literze każdej depeszy i spróbujemy kolejność pasków tak poprzestawiać, by na przykład w górnej depeszy otrzymać jakąś sensowną treść, to automatycznie również w pozostałych depeszach powinna pojawić się sensowna treść. Innymi słowy, jest to metoda ciągłego dopasowywania do siebie poszczególnych pasków i sprawdzania, czy [illegible]

depeszach jednocześnie powstaną możliwe dla języka niemieckiego bigramy, trigramy, tetragramy itd., aż stopniowo zaczną pojawiać się fragmenty słów i zdań.

Metoda ta, zwana metodą anagramów, nie jest specyficzną dla omawianego systemu szyfrowego, lecz da się zastosować do wszystkich szyfrów przestawieniowych, w których dysponuje się kilkoma szyfrogramami tej samej długości, pod warunkiem, że traktować je można - tak jak w naszym przypadku - jako zaszyfrowane w ten sam sposób.

Spróbujmy teraz przedstawić ją na przykładzie. Niech więc danych będzie następujących sześć szyfrogramów pochodzących z tego samego dnia i mających tę samą długość 50 liter :

BGRXE RTXXI EKSUQ EDXAW SLAXT TDIKE CXIGX OLXUR LWNII QPQSN
SWXAN MDENL NAHSE XTNNT IXXQR RQSEL HATNE ERXNH AMSEX RMXIX
IDNXK IXEXX VITSG XIDDX SXQRX EVOOL LEENO RCXDX AEXLG LQXEN
EWLIX NXEEI NWEIE NXTAX BSMGX BXXGA XGIEB NEXIG EABXH LEQNL
KHSNG LEULR XHONA SXENE HIVDQ BEWBX XCLEU UNXCS ABKMR XEUXI
EDREE NRNNZ RAWRO XNEXM XLXUE GSDOK MXGLR SIXNQ ETXIX EXEZE

Jak już wspomnieliśmy, należy je przepisać na odpowiednią taśmę papierową, którą potem przetniemy na pionowe paski. Z powodów, które za chwilę wyjaśnimy, należy kolejne litery depesz ponumerować, tak aby każdy pasek po rozcięciu miał swój numer /np. nad literami/. Pierwszych kilka pasków będzie więc wyglądać następująco:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
B	G	R	X	E	R	T	X	X	I	E	K	S	U	Q
S	W	X	A	N	M	D	E	N	L	N	A	H	S	E
I	D	N	X	K	I	X	E	X	X	V	I	T	S	G
E	W	L	I	X	N	X	E	E	I	N	W	E	I	E
K	H	S	N	G	L	E	U	L	R	X	H	O	N	A
E	D	R	E	E	N	R	N	N	Z	R	A	W	R	O

Jako punkt wyjścia mogą służyć litery C i K w pierwszym

frogramie. Litera C bowiem w języku niemieckim przed samogłoską występuje niesłychanie rzadko, a przed spółgłoskami jedynie w połączeniu z literami H lub K. A ponieważ CH zastępuje się w szyfrze literą Q, przeto najprawdopodobniej litery C i K /jedyne w tym szyfrogramie/ należą do siebie. Mamy więc już pierwszy bigram

31	12
C	K
H	A
L	I
X	W
X	H
M	A

Na prawo od paska 12 winien się znaleźć, jak łatwo zauważyć, pasek mający na czwartym i piątym miejscu samogłoskę. Pasków takich jest kilka, mianowicie

8	13	15	34	41	47
X	S	Q	G	L	P
E	H	E	N	A	M
E	T	G	N	A	Q
E	E	E	E	E	E
U	O	A	E	A	E
N	W	O	L	E	X

ale tylko paski 8, 34 i 47 tworzą z paskami 31 12 możliwe trigramy. Drogą dalszych prób ulegają eliminacji paski 34 i 47, tak że pozostaje jako możliwy tylko pasek 8 tworzący z pierwszym bigramem następujący trigram

31	12	8
C	K	X
H	A	E
L	I	E
X	W	E
X	H	U
M	A	N

Nie ma celu dalsze, drobiazgowe pokazywanie, jak otrzymany fragment kleru można rozszerzyć przez dokładanie pasków z prawej i lewej strony. Nie istnieje pod tym względem żadna ogólna regu[illegible]. W każdym konkretnym wypadku należy postępować indywidualnie, kierując się znajomością języka i jego cech, znajomością wcześniejszych tekstów, intuicją. Podajemy tutaj od razu końcowy rezultat, to jest kler wszystkich sześć depesz /dla ewentualnego sprawdzenia/

GLUECKXUNDXGLASXWIEXLEIQTXBRIQTXDASXEINXSPRIQWORTX
WASXHAENSQENXNIQTXLERNTXDASXLERNTXHANSXNIMMERMEHRX
DASXLIEDXVONXDERXGLOCKEXXEINXGEDIQTXVONXSQILLERXXX
WEINXWEIBXGESANGXHABEXIQXGELIEBTXMEINXLEBENXLANGXX
HANSXHUCKEBEINXDERXUNGLUECKSRABEXVONXWILHELMXBUSCX
DERXMANNXSOLLXZUMXKRIEGERXERZOGENXWERDENXXNIETSCEX

Oraz osobno - dla oszczędzenia miejsca - kolejność numeracji pasków w ten sposób otrzymaną:

2 41 14 16 31 12 8 39 43 27 29 34 22 19 49 24 20 45 30 35 37 [illegible]

33 48 7 32 1 3 10 15 26 18 17 23 13 4 11 28 50 9 21 47 6 [illegible]

46 42 36 40 25 38

Kolejność ta ma, jak za chwilę okażemy, zasadnicze znaczenie dla dalszego rozwiązania szyfru. Jak dotąd bowiem znajomość [illegible] sześciu szyfrogramów nie pozwala jeszcze na odczytanie pozostałych szyfrogramów z tego samego dnia. Trzeba jeszcze [illegible]ować klucze "A" i "B". Do tego celu służy właśnie kolejność numeracji pasków. Przyjrzyjmy się jej dokładnie. Zauważymy [illegible] charakterystyczne konfiguracje liczb bliskich siebie /w [illegible] arytmetycznym/. I tak na przykład liczby 41 i 43 znajdują [illegible] w odległości 7 cyfr od siebie. Ale w tej samej odległości [illegible] dują się też liczby 30 i 32 oraz liczby 4 i 6. Obok siebie [illegible] liczby 27 i 29, ale także liczby 1 i 3 oraz liczby 44 i 46 [illegible] od siebie [illegible] 3 cyfry.

obok siebie / para cyfr 14 i 12 /

35 i 33, 11 i 9. Tak samo o trzy cyfry są od siebie oddalone pary liczb 22 i 24, 15 i 17, 36 i 38. Podane konfiguracje zaznaczyliśmy podkreśleniami wzgl. łukami. W tworzeniu się takich i podobnych konfiguracji nie było by może nic szczególnie zaskakującego, gdyby nie to, że ich wzajemna odległość jest równa i wynosi 17 cyfr. A więc o 17 cyfr odległe są liczby 41 i 30, 30 i 4, liczby 27 i 1, 1 i 44, liczby 22 i 15, 15 i 36, itd itd. To spostrzeżenie upoważnia nas do twierdzenia, nie będziemy wyjaśniać, dlaczego, że długość klucza "A" wynosi 17. Znając w ten sposób długość klucza "A", wypisujemy kolejność numeracji pasków ponownie, ale teraz już w odcinkach po 17 liter otrzymując coś w rodzaju tabeli "A", jednak bez klucza "A".

2	41	14	16	31	12	8	39	43	27	29	34	22	19	49	24	20
45	30	35	37	5	33	48	7	32	1	3	10	15	26	18	17	23
13	4	11	28	50	9	21	47	6	44	46	42	36	40	25	38	

Pionowe kolumienki tej tabeli przepisujemy teraz w pozycji poziomej

2 45 13	41 30 4	14 35 11	16 37 28	31 5 [illegible] 2 [illegible] 9	
8 48 21	39 7 47	43 32 6	27 1 44	29 3 46	34 10 42
22 15 36	19 26 40	49 18 25	24 17 38	20 23	

i próbujemy ustawić je tak względem siebie, aby pod sobą znalazły się kolejne liczby w porządku rosnącym

27 1 44	12 33 9				
	2 45 13	34 10 42			
29 3 46	14 35 11				

Po niewielu próbach uda nam się otrzymać następującą tabelę

9	6	14	11	1	17	5	13	4	16	12	2	19	7	10	15	3	18	8
22	15	36	27	1	44	12	33	9	41	30	4	49	18	25	39	7	47	20
23	16	37	28	2	45	13	34	10	42	31	5	50	19	26	40	8	48	21
24	17	38	29	3	46	14	35	11	43	32	6							

W tabelce tej wystarczy nad kolumienką 1,2,3 napisać liczbę 1,

nad kolumienką 4,5,6 liczbę 2, nad kolumienką 7,8 liczbę 3, itd., aby otrzymać klucz "B".

Wreszcie dla otrzymania klucza "A" należy nad kolumienkami poprzedniej tabeli, to jest tabeli "A" umieścić liczby od 1 do 17 w takiej kolejności, w jakiej kolumienki te znajdują się w tabeli "B" w pozycji poziomej. A więc nad kolumienką 22,15,36 należy umieścić liczbę 1, nad kolumienką 27,1,44 liczbę 2, nad kolumienką 12,33,9 liczbę 3 itd., i w ten sposób otrzymujemy tabelę "A" wraz z kluczem "A"

9	4	16	8	11	3	13	6	17	2	15	10	1	12	5	14	7
2	41	14	16	31	12	8	39	43	27	29	34	22	19	49	24	20
45	30	35	37	5	33	48	7	32	1	3	10	15	26	18	17	23
13	4	11	28	50	9	21	47	6	44	46	42	36	40	25	38	

i nic już nie stoi na przeszkodzie dla odczytania pozostałych depesz danego dnia, tak jak to robią deszyfranci.

Należy jeszcze nadmienić, że podany przykład, który posłużył do zademonstrowania metody rozwiązania szyfru, jest wyidealizowany i w praktyce raczej się nie zdarzał. Komplety z sześciu krótkich depesz tej samej długości trafiały się tylko zupełnie wyjątkowo i zazwyczaj rozwiązanie opierało się na komplecie z czterech lub trzech depesz, a niekiedy nawet dwie depesze były podstawą do rozwiązania danego dnia. Poza tym szyfrogramy nie były, jak w przykładzie, bezbłędne, lecz obarczone nieraz dość licznymi błędami popełnionymi bądź przez telegrafistów nadających, bądź odbierających dany szyfrogram, co oczywiście w wysokim stopniu utrudniało stosowanie metody anagramów. Również klucze "A" i "B" nie zawsze składały się tak idealnie jak w przykładzie, lecz rozpadały się czasem na kilka części, i trzeba było korzystać z dalszych szyfrogramów, by je złożyć. Dlatego też okres pracy w Ekspozyturze trwający dla mych kolegów trzy, dla mnie dwa lata, był może nieco jednostronnym, lecz tym niemniej doskonałym wprowadze-

niem w skomplikowaną dziedzinę kryptologii i przygotowaniem do dalszej, bardziej samodzielnej pracy. Dokonaliśmy zresztą pewnych ulepszeń zarówno w teorii jak i w praktyce rozwiązywania przestawienia podwójnego. I tak na przykład podana wyżej metoda znajdywania kluczy "A" i "B" stanowi naszą modyfikację metody wyłożonej na kursie /i w podręczniku francuskim wspomnianym na str.3/. Wykazaliśmy też, że w niektórych wypadkach można dla rozwiązania danego dnia posługiwać się depeszami, których długości nie są równe, lecz różnią się między sobą o jedną literę.

Na zakończenie wypada dodać, że technicznie rozwiązywanie przestawienia podwójnego odbywało się nieco inaczej, niż to przedstawiono. Pisanie bowiem szyfrogramów na taśmach papieru, rozcinanie tych taśm na paski, a zwłaszcza manipulowanie takimi papierowymi paseczkami dla otrzymania kleru było by nad wyraz niewygodne. Dlatego mieliśmy do naszej dyspozycji duże ilości specjalnie na ten cel zamówionych ebonitowych patyków, podzielonych na kratki /jak na rysunku obok/, do których wpisywało się ołówkiem dermatograficznym na samej górze kolejne liczby, a pod nimi litery depesz. Patyki służyły do wielokrotnego użytku, bo oczywiście po skończonej robocie ścierano szmatką niepotrzebne już liczby i litery.

II.

Z dniem 1.IX.1932 r. nastąpiła likwidacja Ekspozytury w Poznaniu. Ja i moi dwaj koledzy, Henryk Zygalski i Jerzy Różycki, którzy w międzyczasie też już ukończyli studia matematyczne, zaangażowani zostali do pracy stałej, już teraz w pełnym wymiarze godzin, w Biurze Szyfrów w Warszawie. Tymczasem szefem Biura Szyfrów został mjr Karol Gwido Langer, który następnie awansował do stopnia podpułkownika. Zresztą i por. Ciężki awansował do stopnia kapitana, a później majora. Z innymi osobami nie stykaliśmy się w Sztabie przy Placu Saskim /Marszałka Piłsudzkiego/ prawie zupełnie. Było kilka sekretarek, kilku pracowników zajętych rozwiązywaniem przestawienia podwójnego. Poza tym niektóre osoby znało się z widzenia przy przechodzeniu przez korytarze gmachu Sztabu, jak kierownika komórki szyfrów rosyjskich kap. Gralińskiego i kierownika komórki szyfrów polskich kap. Petrykowskiego. Wkrótce zresztą odizolowano moich kolegów i mnie tak dokładnie od reszty pracowników, że nawet woźny wnoszący herbatę na śniadanie nie miał prawa wstępu do naszego pokoju, u którego drzwi rozwieszono na domiar czarną kotarę, wskutek czego pokój nasz żartobliwie przezwano black chamber według książki Yardleya. Zapomniałem dodać, że Antoni Palluth, o którym poprzednio wspominałem i który był jednym z najwcześniejszych pracowników Biura Szyfrów i niewątpliwie niemało się przysłużył przy jego zorganizowaniu, w owym czasie, gdy przybyliśmy do Sztabu, już się szyframi zajmował mało lub wcale nie. Zdaje się, że skierowano go do pracy nad różnymi zagadnieniami technicznymi do firmy "A.", która wykonywała zamówienia dla Biura Szyfrów, jak np. specjalne wozy z aparatami podsłuchowymi, maszyny do szyfrowania etc.

Pierwszą całkowicie samodzielną pracą, którą w Biurze Szyfrów wykonaliśmy, było rozwiązanie czteroliterowego kodu używanego przez niemiecką marynarkę wojenną. Początek pracy był trudny. Zapoznaliśmy się przede wszyskim bardzo dokładnie z materiałem szyfrowym, sporządziliśmy frekwencję wszystkich grup kodu, różne ewidencje występowania dłuższych sekwencji grup kilkakrotnie, etc. Ale nie mieliśmy żadnego punktu zaczepienia. Spodziewaliśmy się jedynie, że kod będzie ułożony alfabetycznie. Pamiętam, że bazując na tej hipotezie i licząc się z prawdopodobieństwem, że przynajmniej część depesz będzie miała charakter ćwiczebny, przyjęliśmy na chybił trafił, jako treść pewnej krótkiej, składającej się z sześciu grup depeszy : Wann wurde Friedrich der Grosse geboren. I o dziwo, założenie nasze okazało się w 100 % trafne. I choć dalsze rozwiązanie kodu też szło dość opornie, to jednak w ciągu kilku miesięcy treść większości depesz była przez nas odczytana. Okazało się przy tym, że kod tylko częściowo ułożony był alfabetycznie i że słowa często się powtarzające, znaki przystankowe, określenia gramatyczne etc miały w kodzie po kilka określeń w układzie niealfabetycznym. To właśnie było przyczyną, dla której nie tak łatwo uporaliśmy się z rozwiązaniem kodu. Treści depesz - poza pierwszą rozwiązaną wyżej przytoczoną -dziś już dokładnie nie pamiętam. Była w nich mowa o sprawach personalnych, o rejsach okrętu, ich wyekwipowaniu /np.Sonnensegel mitnehmen/, występowały nazwy portów /np indyjski port Trinkomalee/ itd. W każdym razie depesz ćwiczebnych zbyt wiele nie było, więc dostarczony przez nas materiał, odpowiednio wykorzystany, mógł przedstawiać niemałą wartość. Jako ciekawostkę mogę jeszcze podać, że w kodzie nie wykorzystano wszystkich 26 liter alfabetu łacińskiego, lecz tylko 18 liter, ale niewiadomo, dlaczego. Wreszcie, w celu umożliwienia konfrontacji, gdyby w archiwum wojskowym przypadkowo znalazł się egzemplarz omawianego

m z pamięci kilka określeń kodu:

YOPY - Wann

YWIN - Welcher

BAUG - Und

KEZL - Letzten Buchstaben streichen.

III.

Zanim jeszcze ukończyliśmy pracę nad rozwiązaniem kodu morskiego, zlecono mi nową pracę, początkowo dodatkowo w godzinach wieczornych, później - gdy otrzymałem pierwsze pozytywne wyniki - w normalnych godzinach urzędowania. Dostarczono mi dość obfity materiał zaszyfrowany nowym rodzajem szyfru używanym przez niemieckie wojsko lądowe. Szyfr pojawił się - jeżeli się nie mylę - kilka lat wcześniej. Przypuszczam nawet, że kurs kryptologii i ekspozyturę w Poznaniu zorganizowano właśnie w związku z pojawieniem się nowego rodzaju szyfru. Czy to z odczytanych depesz zaszyfrowanych systemem przestawienia podwójnego, czy też z innych źródeł, dość, że wiedziano, że jest to szyfr maszynowy. Wiedziano nawet, że maszyna, którą szyfrowano, nazywa się "Enigma". Rzucało się zresztą w oczy, że szyfr nie był ani szyfrem przestawieniowym, ani jakimś mało skomplikowanym szyfrem podstawieniowym, gdyż w tekstach nie napotykano na dłuższe powtórzenia, a frekwencja liter była dość jednorodna. Łatwo też zauważono, że sześć pierwszych liter każdej depeszy, które nazywać będziemy początkiem depeszy, odgrywa specjalną rolę. Bo jeżeli zdarzyły się dwie depesze, które miały pierwszą literę równą, to i czwarte litery były równe. Jeżeli w dwóch depeszach drugie litery były równe, to i piąte litery były równe, i wreszcie jeżeli w dwóch depeszach trzecie litery by-

ły równe, to i szóste litery były równe. Wszystko więc wskazywało na to, że początek każdej depeszy, czyli jej sześć pierwszych liter, to jej /trzyliterowy/ klucz dwukrotnie zaszyfrowany. Gdyby mogły być pod tym względem jeszcze jakiekolwiek wątpliwości, to następujące spostrzeżenie powinno je rozproszyć.

Jeżeli dwie depesze o tych samych początkach, a takich depesz było nieoczekiwanie dużo, napiszemy jedną pod drugą

```
rfbwl d|pcai hwbqx emtpo bfvgq ihfgr ojvdd zluws jurnk tkcly smnae
rfbwl d|nwel soapx oazyb byzrq qcjdx cfkhi ngdfc mjvpi ktehm slrug
```

wtenczas równe litery na tych samych miejscach będą się trafiać, średnio biorąc, dwa razy częściej, niż wtedy, gdy napiszemy pod sobą dwie depesze o /choćby częściowo / różnych początkach

```
rkxwf o|kisc ixjwt wqapd redbw lfvgk ylrmz cojhs tnpbo afnug vuemh
wdxro o|hrkt gusdt udeql swfpv fqmrc  yavzj lyikn oxhon mgepw
```

/Przy obliczaniu ilości równych liter nie bierzemy oczywiście pod uwagę równych liter w samych początkach depesz/. Przyczyna tego zjawiska jest prosta. Przy równej częstotliwości występowania wszystkich 26 liter alfabetu łacińskiego dwie równe litery w dwóch depeszach trafiają się średnio 1 raz na 26, czyli około 3,85 razy na 100. Natomiast przy nierównej frekwencji liter, jaka występuje w języku niemieckim, teoretyczną częstość występowania w dwóch depeszach równych liter na odcinku 100-literowym otrzymuje się ze wzoru

$$100\left\{\left[fr/a/\right]^2+\left[fr/b/\right]^2+\cdots\cdots\cdots\cdots+\left[fr/z/\right]^2\right\}$$

gdzie symbol fr/a/ oznacza frekwencję litery a w języku niemieckim, symbol fr/b/ - frekwencję litery b w języku niemieckim, itd. Wartość powyższego wyrażenia, którą łatwo obliczyć, jest znana

frekwencję wszyskich liter w języku niemieckim, wynosi około 7,65 czyli rzeczywiście jest w przybliżeniu dwukrotnie większa od wartości otrzymanej przy równej frekwencji liter. Częstość występowania dwóch równych liter na tym samym miejscu w dwóch tekstach niemieckich nie zmieni się, jeżeli oba teksty zaszyfrujemy tym samym kluczem. W ten sposób mamy sprawdzian, czy dwie depesze są zaszyfrowane tym samym kluczem, czy różnymi kluczami. Nie ma jeanc... potrzeby dodawać, że przytoczone przykłady depesz o początkach równych względnie różnych są fikcyjne i o wiele za krótkie, by mogły służyć za podstawę do wyciągania wniosków opartych na statystyce. Służyły one tylko do zilustrowania zastosowanej przez nas metody.

Skoro więc jesteśmy już przekonani, że początki depesz, czyli sześć pierwszych liter, są kluczami depesz, zajmijmy się nimi dokładniej. Przypuśćmy, że w określonym dniu mają postać następującą

auq amn	maw uxp	sug smf
bnh chl	nxd qtu	tmn eby
bct cgj	nxd qtu	tmn eby
cik bzt	nlu qfz	taa exb
ddb vdv	obu dlz	use nwh
ejp ips	pvj feg	vii poh
fbr kle	qga lyb	vii poh
gpb zsv	rjl wpx	vqz pvr
hno thd	rjl wpx	wtm rao
hno thd	rjl wpx	wtm rao
hxv tti	rjl wpx	wtm rao
ikg jkf	rfc wqq	wki rkk
ikg jkf	syx scw	xrs gnm
ind jhu	syx scw	xrs gnm
jwf mic	syx scw	xoi guk
jwf mic	syx scw	xyw gcp
khb xjv	syx scw	ypc osq
khb xjv	sjm spo	ypc osq
ldr hde	sjm spo	zzy yra
ldr hde	sjm spo	zef yoc
maw uxp	sug smf	zsj ywg

Dla większej przejrzystości rozbiliśmy każdy początek n... /ie

grupy trzyliterowe, tak że pierwsza grupa stanowi klucz po pierwszym, druga grupa ten sam klucz po drugim zaszyfrowaniu. Uderza, jak.o tym już wzmiankowaliśmy na str. 17., wielka ilość depesz o takich samych początkach. Różnych trzyliterowych kluczy można utworzyć 26·26·26 = 17576. W tych warunkach, w grupie obejmującej kilkadziesiąt depesz, a takie właśnie ilości depesz codziennie dostarczano, dwie depesze z tym samym początkiem powinny trafiać się zupełnie wyjątkowo. Skoro jednak jest inaczej, skoro powtórzeń początków jest bardzo dużo, musimy wnioskować, że szyfranci mają szczególne upodobanie do pewnych kluczy, może na przykład takich jak AAA, BBB, ABC, XYZ.

Przypuszczenie nasze okazało się słuszne. Co więcej, okazało się, że można, nie znając zupełnie konstrukcji maszyny do szyfrowania względnie mając o niej bardzo niekompletne informacje, odpowiedzieć w bardzo wielu wypadkach na pytanie, jakie klucze szyfranci sobie obrali, innymi słowy rozszyfrować klucze. Metodę, która do tego prowadzi, podamy poniżej.

Bierzemy naprzód pod uwagę tylko pierwsze i czwarte litery początków depesz. W depeszy rozpoczynającej się od liter ddb vdv pierwszą literą jest d, czwartą v. Napiszmy te dwie litery obok siebie w takiej właśnie kolejności

dv

Szukamy depeszy rozpoczynającej się od litery v. Jest nią depesza vii poh. Ponieważ czwartą literą jest p, więc piszemy tę literę na prawo od liter dv

dvp

Szukamy depeszy rozpoczynającej się od litery p. Jest nią depesza pvj feg. Ponieważ czwartą literą jest f, więc piszemy literę f na prawo od liter dvp

Tak postępujemy dalej. Otrzymujemy kolejno litery

dvpfkxgzyo

Następną literą w tym rzędzie byłaby litera d. Ale litera d znajduje się już na początku. Nie piszemy jej drugi raz, lecz otrzymane dotychczas litery umieszczamy w nawiasie

(dvpfkxgzyo),

i nazywamy cyklem. Gdybyśmy wyszli nie z depeszy ddb vdv, lecz na przykład z depeszy khb xjv, otrzymalibyśmy cykl

(kxgzyodvpf).

Takie dwa cykle, w których kolejność liter jest ta sama, a różnica polega tylko na tym, że na ich początku są różne litery, uważamy za identyczne. W szczególności więc identycznymi są cykle

(dvpfkxgzyo)
(vpfkxgzyod)
.....
(odvpfkxgzy)

w których dokonaliśmy cyklicznego przesunięcia liter. Stąd nazwa cykli. Weźmy teraz literę, która w powyższym cyklu nie występuje, na przykład literę e i wychodząc z tej litery powtórzmy cały proces jeszcze raz. Otrzymamy cykl

(eijmunqlht).

Ponieważ w ten sposób nie wyczerpaliśmy jeszcze wszystkich liter alfabetu, bierzemy z kolei dalszą literę, która nie wystąpiła ani w pierwszym, ani w drugim cyklu, na przykład literę a. Ale litera a przechodzi na czwartym miejscu znów na a. Więc litera a tworzy cykl sama dla siebie

(a).

Ponieważ i teraz nie wyczerpaliśmy jeszcze wszystkich liter al

betu, przeto bierzemy literę nie występującą ani w pierwszym, ani w drugim, ani w trzecim cyklu i tak postępując dalej, otrzymamy jeszcze cykle

$$(bc), \qquad (rw), \qquad (s).$$

Wszystkie te cykle piszemy w jednym rzędzie bezpośrednio obok siebie i oznaczamy przez A_1A_4 dla zaznaczenia, że powstały z pierwszych i czwartych liter początków depesz

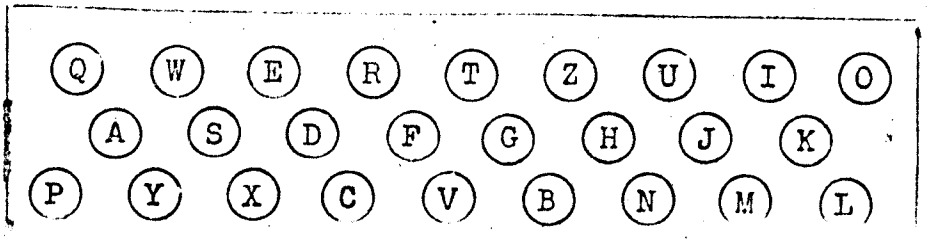
$$A_1A_4 = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

W dokładnie taki sam sposób tworzymy

$$A_2A_5 = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$
$$A_3A_6 = (abviktjgfcqny)(duzrehlxwpsmo)$$

z drugich i piątych względnie z trzecich i szóstych liter depesz.

Zjawiskiem uderzającym jest, że cykle tej samej długości występują zawsze do pary. W zinterpretowaniu tego zjawiska pomocną będzie następująca informacja: W Berlinie istniało towarzystwo akcyjne wyrabiające maszyny do szyfrowania dla celów handlowych. Maszyny te też nazywały się "Enigma", a więc tak samo jak maszyny używane przez wojsko niemieckie. Wszystko więc wskazywało na to, że maszyny wojskowe są tego samego lub podobnego typu co maszyny stosowane w handlu. Z tych względów Biuro Szyfrów sprowadziło taką maszynę i postawiło do mej dyspozycji. Nie zamierzam tej maszyny opisywać szczegółowo, nadmienię tylko, że z wyglądu zewnętrznego przypominała maszynę do pisania. Miała 26 klawiszy oznaczonych literami, a za klawiszami znajdowała się tablica z 26 okienkami, pod którymi były żarówki, jak w kieszonkowych latarkach. Tablica miała układ następujący



We wnętrzu maszyny znajdowało się kilka na jednej osi umieszczonych bębenków, przez które przebiegał prąd elektryczny zasilany z bateryjki. Za każdym uderzeniem klawisza jeden z bębenków, a niekiedy dwa lub kilka obracało się, a jednocześnie jedna z żarówek umiszczonych pod tablicą zapalała się oświetlając literę w okienku. Maszyna była tak skonstruowana, że jeżeli uderzało się w klawisze kolejne litery kleru, to w okienkach pokazywały się kolejne litery szyfru, a jeżeli przy tej samej początkowej pozycji bębenków uderzało się kolejne litery szyfru, to w okienkach pokazywały się kolejne litery kleru. Albo innymi słowy, jeżeli w pewnej pozycji bębenków uderzenie klawisza a spowodowało zaświecenie się lampki b, to w tej samej pozycji bębenków uderzenie klawisza b spowodowało zaświecenie się lampki a. Można by to nazwać prawem wzajemności. Drugą cechą maszyny było, że uderzenie klawisza a w różnych pozycjach bębenków powodowało zapalanie się coraz to innych lampek z wyjątkiem lampki oznaczonej literą a. Tę cechę można by nazwać prawem wyłączności.

Nie ulegało wątpliwości, że opisane cechy maszyny handlowej występowały również w maszynie wojskowej "Enigma". Teraz dopiero stało się zrozumiałym, dlaczego cykle tej samej długości pojawiają się zawsze w liczbie parzystej. Weźmy bowiem przypadek szczególny. Wśród początków depesz wymienionych na str. 18. znajduje się też taki początek

auq amu

W początku tym pierwsza i czwarta litera są równe. Oznacza to, że uderzenie pewnego klawisza różnego od a powoduje zapalenie się lampki a zarówno w pierwszej jak i czwartej pozycji. Ale w takim razie na mocy prawa wzajemności uderzenie klawisza a musi spowodować zapalenie się jednej i tej samej lampki w pozycji pierwszej i czwartej. Oprócz jednoliterowego cyklu (a) musi zatem wystąpić

jeszcze drugi cykl jednoliterowy. Istotnie jest nim cykl (s). Od razu też wiadomo, że uderzenie klawisza a spowodowało zaświecenie się lampki s i uderzenie klawisza s spowodowało zaświecenie się lampki a. W podobny, choć już nie tak zupełnie prosty sposób można wyjaśnić występowanie parzystej liczby cykli dwu-, trzy- i więcejliterowych, przy czym zawsze jest tak, że uderzenie klawisza oznaczonego literą znajdującą się w jednym cyklu powoduje zapalenie się lampki oznaczonej literą znajdującą się w drugim cyklu tej samej długości. Można też wykazać, że jeżeli w określonej pozycji bębenków uderzenie klawisza a powoduje zapalenie się lampki b, to uderzenie klawisza znajdującego się w cyklu na prawo /względnie na lewo/ od a powoduje zapalenie się lampki znajdującej się w cyklu na lewo /względnie na prawo/ od b. Pojęcia "prawo" i "lewo" należy rozumieć szerzej niż w języku potocznym : jeżeli jakaś litera znajduje się na prawym krańcu cyklu, to przez literę na prawo od niej stojącą należy rozumieć literę znajdującą się na lewym krańcu cyklu, itd./.

W oparciu o te wiadomości zrozumiałym staje się dalsze nasze postępowanie zmierzające do rozszyfrowania kluczy. Wiemy już, że jeżeli szyfranci - tak jak przypuszczamy - kilka razy wybrali jako klucz depeszy litery aaa, to trzeba klucz ten szukać wśród początków depesz zaczynających się na literę s. Ponieważ początek syx scw występuje /na str.18./ aż pięć razy, więc prawdopodobnym jest, że jest to właśnie zaszyfrowany klucz aaa. Zresztą pozostałe początki rozpoczynające się na literę s nie wchodzą w grę. Początek sjm spo nie może oznaczać klucza aaa, gdyż litery a i j w A_2A_5 /na str.21./ wchodzą do dwóch cykli niejednakowej długości. Początek sug smf też nie może oznaczać klucza aaa, między innymi dlatego, ponieważ litery a i g w A_3A_6 wchodzą do jednego i tego cyklu. Zakładamy więc, że początek syx scw oznacza klucz aaa. Napiszmy teraz odpowiednie cykle w ten sposób jedne pod drugimi, aby

z cykli wchodzących w skład A_1A_4 pod literą a znalazła się litera s, z cykli wchodzących w skład A_2A_3 pod literą a znalazła się litera y i z cykli wchodzących w skład A_5A_6 pod literą a znalazła się litera x, przy czym ze zrozumiałych względów w dolnych rzędach kolejność liter została odwrócona

a
s

axt
ygc

abviktjgfcqny
xlherzudomspw

Nieco spostrzegawczości i trochę zmysłu kombinatoryjnego wystarczy, aby i pozostałe cykle tak sobie podporządkować

a bc dvpfkxgzyo
s rw iethlqnumj

axt blfqveoum d
ygc jhnrziwsp k

abviktjgfcqny
xlherzudomspw

by spośród początków podanych na str. 18. można było utworzyć możliwie jak najwięcej kluczy kształtu BBB, CCC, itd. Przy takim podporządkowaniu początki podane na str. 18 dają następujące klucze:

auq amn :	SSS	khb xjv :	LLL	taa cxb :	PYX
bnh chl :	RFV	ldr hde :	KKK	use nwh :	ZUI
bct cgj :	RTZ	maw uxp :	YYY	vii poh :	EEE
cik bzt :	WER	nxd qtu :	GGG	vqz pvr :	ERT
ddb vdv :	IKL	nlu qfz :	GHJ	wtm rao :	CCC
ejp ips :	VBN	obu dlz :	JJJ	wki rkk :	CDE
fbr kle :	HJK	pvj feg :	TZU	xrs gnm :	QQQ
gpb zsv :	NML	qga lyb :	XXX	xoi guk :	QWE
hno thd :	FFF	rjl wpx :	BBB	xyw gcp :	QAY
hxv tti :	FGH	rfc wqq :	BNM	ypc osq :	MMM
ikg jkf :	DDD	syx scw :	AAA	zzy yra :	UVW
ind jhu :	DFG	sjm spo :	ABC	zef yoc :	UIO
jwf mic :	OOO	sug smf :	ASD	zsj ywg :	UUU
		tmn eby :	PPP		

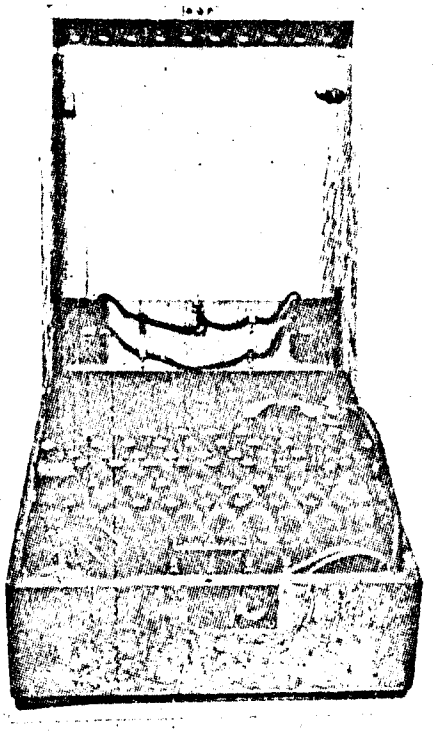
Tak więc istotnie przy obranym przez nas podporządkowaniu sobie cykli wystąpiło bardzo wiele kluczy składających się z trzech równych liter lub z trzech kolejnych liter. W pierwszej chwili dziwić może pojawienie się również takich kluczy jak PYX, QWE, RFV. Wystarczy jednak spojrzeć na tablicę na str. 21., by zrozumieć, że niektórzy szyfranci wybierali sobie jako klucze trzy litery znajdujące się w tej tablicy bądź obok siebie, bądź w jednej linii ukośnej. To spostrzeżenie ma o tyle pewne znaczenie, że wkrótce zabroniono szyfrantom używania kluczy składających się z trzech równych lub trzech kolejnych liter. Wówczas metodę odtwarzania kluczy oparto na posługiwaniu się przez szyfrantów takimi właśnie kluczami jak PYX, QAY itp. Zresztą w rzeczywistości sprawa rekonstrukcji kluczy nie przedstawiała się tak prosto, jak z podanego przykładu można by wnioskować. Kluczy charakterystycznych tak dużo znów nie było. Nie zawsze też w początkach depesz występowały wszystkie litery alfabetu, i wówczas trudności pojawiały się już przy składaniu cykli. Cykle mogły przyjmować wszystkie długości od jednej do trzynastu liter, jak to widać na przykładzie ze str. 21., ale mogły na przykład występować cztery cykle lub nawet sześć cykli czteroliterowych i wówczas ich wzajemne podporządkowanie sobie było trudniejsze. Dlatego też w późniejszej fazie pracy obmyślono inne metody prowadzące szybciej do celu. Chwilowo jednak umiejętność odtwarzania kluczy stanowiła ważny krok naprzód w kierunku rozwiązania szyfru maszynowego. Dzięki niej bowiem w danym dniu, w którym klucze złożono, wiedziano dla sześć kolejnych pozycji bębenków, jakie lampki zapalą się przy uderzeniu każdego klucza. Ale aby posunąć się dalej, potrzebne były dokładniejsze informacje o budowie maszyny, o sposobie posługiwania się nią, a poza tym potrzebna była - jak to później okażemy - znajomość pewnego działu algebry wyższej.

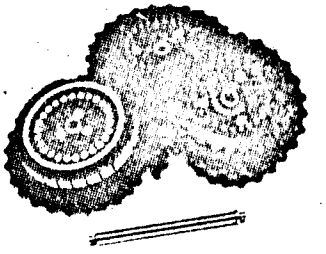
IV.

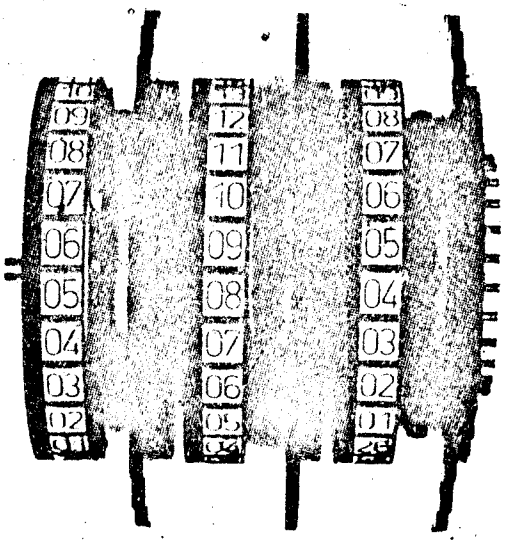
Gdyby maszyna "Enigma" używana przez wojsko niemieckie była tak samo skonstruowana jak maszyna służąca celom handlowym, wówczas przedstawiona poprzednio metoda odtwarzania kluczy byłaby wystarczającym instrumentem do całkowitego rozwiązania szyfru. Postaram się to wykazać później na przykładzie rozwiązanej w czasie wojny maszyny szwajcarskiej.

Niestety jednak maszyna wojskowa, choć miała niektóre cechy wspólne z maszyną handlową, różniła się jednak od niej zasadniczo. Dowiedziano się o tym z fotokopii tajnej niemieckiej instrukcji służbowej, która w tym czasie znalazła się w posiadaniu Biura Szyfrów /Pod instrukcją znajdował się podpis :Fellgiebel. Czyżby był to ten sam gen.Fellgiebel wmieszany w zamach na Hitlera i stracony?/. Z instrukcji wynikało, że maszyna nazywała się "Enigma", /co już wiedzieliśmy/ względnie "E eins" i że system szyfrowania nazywał aię Maschinenschlüsselverfahren, w przeciwstawieniu do przestawienia podwójnego zwanego obecnie Handschlüsselverfahren. Instrukcja zawierała też reprodukcję maszyny i niektórych jej części. Rysunki umieszone na stronie 27 dadzą - jak sądzę - pewne pojęcie o jej wyglądzie i budowie.

Po podniesieniu wieka drewnianej skrzyni ukazuje się drugie wieko metalowe. W wieku widać trzy szczeliny, z których wystają zębate krawędzie tarcz bębenków szyfrowych na tyle, aby można było je przesuwać ręką i w ten sposób nastawiać bębenki na żądaną literę. Litery te znajdują się na obwodach pierścieni bębenków i ukazują się w trzech niewielkich, pokrytych płytką szklaną okienkach znajdujących się obok szczelin. We wieku, bardziej z przodu, jest też umieszczone pole z lampkami, o którym była już mowa na str. 21. Klawiatura znajduje się z [illegible] poza [illegible]



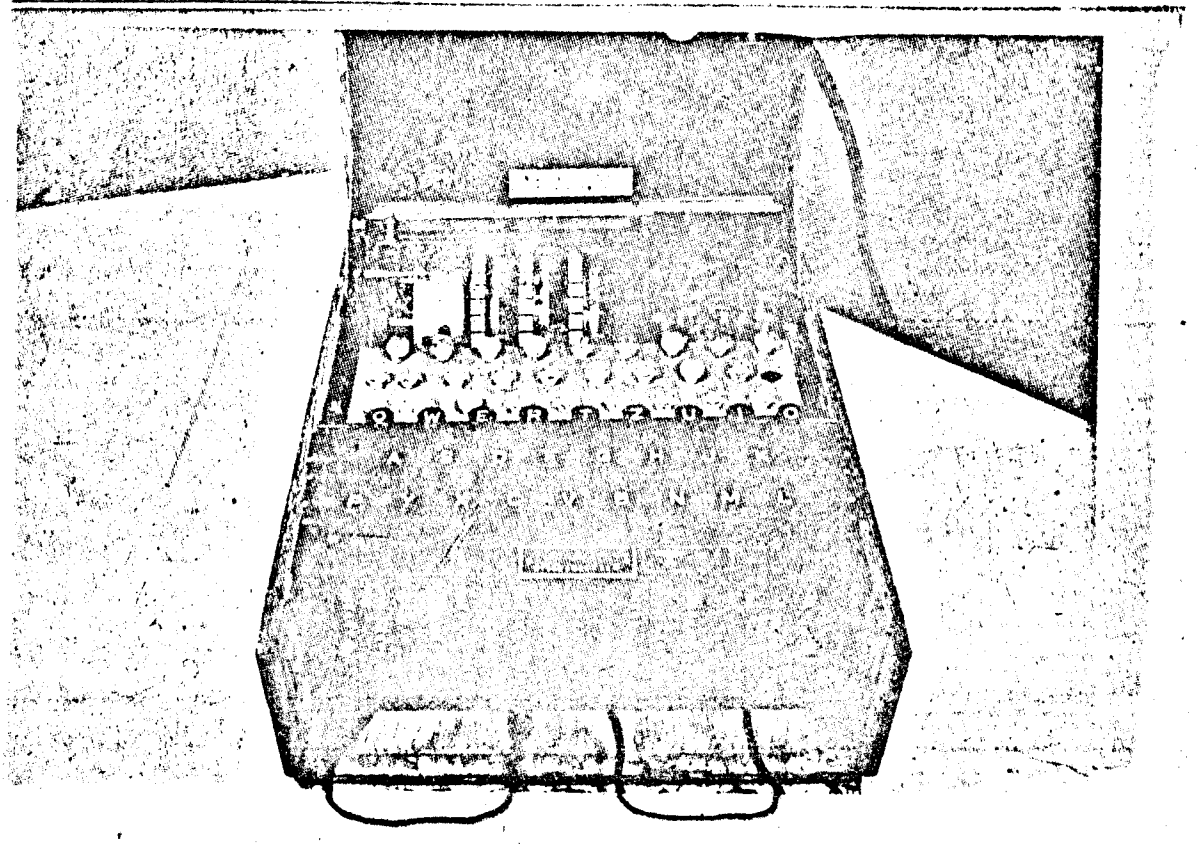



09
08
07
06
05
04
03
02
12
11
10
09
08
07
06
08
07
06
05
04
03
02

Po podniesieniu wieka metalowego widać umieszczone na jednej poziomej osi cztery bębenki. Trzy z nich nazywają się bębenkami do szyfrowania /Chiffrierwalzen/ i oznaczone są rzymski cyframi I, II, III. Ich kolejność można zmieniać. Z tego tytułu możliwych jest sześć kombinacji. Czwarty bębenek znajdujący się najbardziej na lewo nazywa się bębenkiem odwracającym /Umkehrwalze/. Na lewo od bębenka odwracającego znajduje się mała dźwignia, która - zależnie od położenia - bębenki alba przyciska do siebie, albo je zwalnia. Na lewo od dźwigni jest bateryjka zasilająca maszynę w prąd elektryczny o niskim napięciu. Po odpowiednim przestawieniu dźwigni można bębenki wraz z osią wyjąć i pojedyńczo zdjąć z osi. Bębenki do szyfrowania mają wygląd - z grubsza - taki jak przedstawiono na rysunkach na str. 27. na dole. Na prawo pokazano oddzielnie środkową część bębenków do szyfrowania. Jest to ebonitowy krążek, w który wbito z jednej strony 26 metalowych kontaktów stałych, a z drugiej strony 26 metalowych kontaktów sprężynujących. Izolowanymi drucikami przebiegającymi w odpowiednim wyżłobieniu wewnątrz krążka /jeden taki drucik narysowano/ połączone są w nieregularny sposób kontakty stałe z kontaktami ruchomymi. Ebonitowe krążki osadzone są na stałe w metalowych tarczach, na których znajdują się metalowe pierścienie z literami alfabetu. Pierścień jest przestawialny w stosunku do tarczy i krążka. Sposobu przestawiania pierścienia na rysunku nie uwidoczniono. Bębenek odwracający ma nieco inną budowę. Jego krążek ebonitowy z lewej strony nie ma żadnych kontaktów, a tylko z prawej strony kontakty ruchome połączone drucikami między sobą / w sposób nieregularny, podobnie jak w bębenkach do szyfrowania/. Poza tym bębenek odwracający nie ma ruchomego pierścienia ani liter na jego obwodzie. Bębenki do szyfrowania mają jeszcze na swych tarczach odpowiednie wcięcia /na rysunkach nie uwidocznione/ które powodują, że bębenek stojący na prawo przesuwa się za każdym na-

ciśnięciem klawisza o jedną literę naprzód, bębenek środkowy przesuwa się o jedną literę naprzód, gdy bębenek po prawej stronie wykona pełny obrót, a bębenek po lewej stronie przesuwa się o jedną literę naprzód, gdy bębenek środkowy wykona pełny obrót. Bębenek odwracający swej pozycji nie zmienia. Na prawo od bębenków do szyfrowania znajduje się jeszcze jeden - nieruchomy - krążek ebonitowy z 26 kontaktami stałymi, od których biegną druty do klawiszy wzgl. do lampek. Po umieszczeniu bębenków do szyfrowania w określonej kolejności na osi, po włożeniu osi do łożyska i po przyciśnięciu bębenków do siebie przez przestawienie dźwigni, kontakty ruchome jednego bębenka stykają się z kontaktami stałymi bębenka sąsiedniego i w ten sposób przez bębenek może przepływać prąd elektryczny, gdy na skutek naciśnięcia klawisza zamkniemy obwód.

Pod wiekiem metalowym, oprócz pola z żarówkami, o którym już wspominaliśmy, znajduje się jeszcze jedno urządzenie, które stanowi najistotniejszą różnicę w porównaniu z maszyną typu handlowego. Tym urządzeniem są tak zwane połączenia wtyczkowe./Steckerverbindungen/



Sześć sznurków /przewodów elektrycznych/ zakończonych każdy z obu stron wtyczkami podobnymi do wtyczek w centralkach telefonicznych wkłada się do odpowiednich gniazdek umieszczonych na desce z materiału izolacyjnego /ebonitu/ i oznaczonych literami od A do Z. Działanie połączeń wtyczkowych polega na tym, że prąd elektryczny, który normalnie przebiegałby od kolejnych klawiszy względnie lampek do kolejnych kontaktów nieruchomego, wejściowego krążka ebonitowego, obiera teraz inną drogę. Jeżeli dla przykładu gniazdko A połączymy sznurkiem z gniazdkiem F, wówczas prąd elektryczny nie przebiegnie od klawisza /wzgl. lampki/ A do kontaktu pierwszego, lecz do kontaktu szóstego /F jest szóstą literą alfabetu/ i na odwrót prąd elektryczny od klawisza /wzgl. lampki/ F nie przebiegnie do kontaktu szóstego, lecz do kontaktu pierwszego itp. Połączenia wtyczkowe stanowią więc coś w rodzaju dalszego bębenka szyfrującego, z tym tylko, że bębenek ten /który naturalnie nie ma kształtu bębenka, lecz płytki/ jest nieruchomy i zamienia tylko 12 liter, ale za to zamienia codziennie inne litery. Należy jeszcze wspomnieć, że kontakty na krążkach ebonitowych nie są wprawdzie numerowane, jednak dla orientacji pracowników zestawiających we fabryce bębenki jeden z kontaktów zaopatrzony jest w kropkę. Kontakt ten uważa się za pierwszy i od niego zaczyna się liczenie kolejnych kontaktów.

Tajna niemiecka instrukcja służbowa poza opisem maszyny podawała również sposób posługiwania się nią. Dowiedzieliśmy się więc, że szyfrant przed przystąpieniem do szyfrowania musi maszynę odpowiednio nastawić na właściwy klucz składający się z kilku części, które, z wyjątkiem jednej, szyfrantowi narzucone są z góry. Pierwszą narzuconą część klucza stanowi kolejność bębenków /Walzenlage/, którą podawano w formie trzech rzymskich cyfr, np. I, II, III albo II, I, III itp. Kolejność bębenków zmieniano jeden raz na kwartał. Następną częścią klucza jest ustawienie pierścieni [illegible]-

lung/, które podawano w formie trzech liter np. G,T,K. Ustawienie pierścieni polegało na umieszczeniu sprężynującego czopka w otworze znajdującym się na pierścieniu przy każdej literze każdego bębenka i powodowało zmianę położenia pierścienia bębenka w stosunku do krążka. Ustawienie pierścieni zmieniano raz na miesiąc. Dalszą częścią klucza były połączenia wtyczkowe /Steckerverbindungen/, które podawano w postaci sześć par liter np. A/P, B/L, C/Z, F/H, J/K, Q/U. Połączenia wtyczkowe zmieniano codziennie. Po uskutecznieniu połączeń wtyczkowych szyfrant zamykał metalowe wieko i nastawiał maszynę na ostatnią część narzuconego klucza, to jest doprowadzał maszynę do pozycji zasadniczej /Grundstellung/. Pozycja zasadnicza, którą zmieniano też codziennie i którą podawano w formie trzech liter, n.p. S,A,T, polegała na tym, że obracano wystające ze szczelin wieka zębate tarcze bębenków tak, aby w sąsiednich trzech okienkach ukazały się litery S, A, T. Teraz wreszcie szyfrant obierał sobie swój własny klucz /Spruchschlussel/, inny dla każdej depeszy, np. A,B,C, dwukrotnie te trzy litery wystukiwał, i kolejne litery, które się nad lampkami ukazywały, np. sjmspo, zapisywał jako początek depeszy. Potem szyfrant przestawiał zębate tarcze bębenków na litery A,B,C i rozpoczynał szyfrowanie właściwej treści depeszy.

Deszyfrowanie odbywało się podobnie. Po nastawieniu maszyny na wszystkie części narzuconego klucza deszyfrant wystukuje początek szyfrogramu, np. sjmspo i po sprawdzeniu, że nad lampkami ukaże się dwukrotnie ta sama trójka liter, np. A,B,C, nastawia w okienkach litery A,B,C i rozpoczyna deszyfrowywanie wystukując kolejne litery właściwego szyfrogramu, to jest od siódmej litery zaczynając /i oczywiście zapisując litery ukazujące się kolejno nad lampkami/.

Może warto jeszcze zastanowić się nad możliwościami, jakie daje maszyna do szyfrowania "Enigma". Każdy z bębenków s[illegible]ając

może przyjąć 26 różnych pozycji. Poza tym kolejność bębenków też się zmienia. Razem daje to 6·26·26·26 = 105456 możliwości. Jest to liczba duża wprawdzie, ale nie przyprawiająca jeszcze o zawrót głowy. Do astronomicznych cyfr dochodzi się dopiero wówczas, gdy weźmie się pod uwagę, na ile sposobów w bębenkach można połączyć ze sobą kontakty stałe z kontaktami ruchomymi lub ile istnieje różnych połączeń wtyczkowych. Zacznijmy od tych ostatnich. Łatwo obliczyć, że przy sześć połączeniach wtyczkowych ich liczba wynosi

$$\frac{26!}{2^6 \cdot 6! \cdot 14!} = 100391791500$$

Liczba możliwych bębenków odwracających wynosi

$$\frac{26!}{2^{13} \cdot 13!} = 7905875085625$$

Ale największa jest liczba możliwych bębenków szyfrujących, mianowicie

$$26! = 403292558134383869952000000$$

Ostatnią liczbę należało by podnieść jeszcze do trzecie potęgi /gdyż są trzy bębenki szyfrujące/ i pomnożyć przez dwie liczby poprzednie, aby wyczerpać wszystkie możliwości tkwiące w maszynie. Wielkość przytoczonych liczb dowodzi niezbicie, że jeżeli się jest w posiadaniu oryginalnej niemieckiej maszyny do szyfrowania wraz z bębenkami i jeżeli ponadto znane są połączenia wtyczkowe, wówczas można ewentualnie pokusić się o znalezienie właściwego położenia bębenków szyfrujących drogą prób. Natomiast o odtworzeniu drogą prób połączeń wtyczkowych lub wewnętrznych połączeń bębenków, a przecież na tym przede wszystkim polega całe zadanie, nie może być mowy. Dotego celu trzeba szukać innych dróg. Dróg takie istotnie znaleziono. Okazały się nimi metody matematyczne przedstawione na następnych kartkach.

V.

Jednym z działów algebry wyższej jest tak zwana teoria grup, w ramach której obok grup abstrakcyjnych omawia się zwykle grupy permutacji. Własnościom samych permutacji - a jedynie te nas tutaj interesują - współczesne podręczniki algebry na ogół niewiele poświęcają miejsca. Więcej na ten temat można znaleźć w podręcznikach starszych, ale są one trudniej dostępne. Dlatego uważałem za właściwe przedstawić tutaj własności permutacji w takim zakresie, w jakim są potrzebne dla zrozumienia dalszych wywodów odnoszących się do rozwiązania maszyny do szyfrowania "Enigma".

Określoną liczbę liter można ustawić obok siebie w różnym porządku. Jeżeli np. mamy sześć liter a, b, c, d, e, f, to można je ustawić w porządku

c e b d f a lub d c f b a e

lub na wiele innych sposobów. Przejście od jednego porządku do innego porządku nazywamy permutacją i oznaczamy w sposób następujący

$$S = \begin{pmatrix} c & e & b & d & f & a \\ d & c & f & b & a & e \end{pmatrix},$$

to znaczy w górnym wierszu permutacji piszemy porządek pierwotny, a w dolnym wierszu porządek nowy i całość zamykamy w nawiasach.

W permutacjach nie jest istotnym, jaki był pierwotny porządek i jaki jest nowy porządek liter, lecz istotnym jest jedynie, na co poszczególne litery permutacji zostały zamienione. W naszym przykładzie jest więc istotnym, że litera a zamienioną została na literę e, litera b na literę f, itd. Dlatego też w każdej permutacji można dowolnie zmieniać porządek liter w górnym wierszu, pod warunkiem, że jednocześnie zmieni się odpowiednio porządek liter w drugim wierszu. Permutację S można więc też przedstawić w postaciach:

$$S = \begin{pmatrix} e & c & b & a & d & f \\ c & d & f & e & b & a \end{pmatrix} = \begin{pmatrix} a & f & b & c & e & d \\ e & a & f & d & c & b \end{pmatrix} = \begin{pmatrix} c & f & b & d & a & e \\ d & a & f & b & e & c \end{pmatrix}, \text{ itd.,}$$

gdyż w każdej z nich a przechodzi na e, b na f, itd. Najczęściej permutację przedstawia się w takiej postaci, aby w górnym wierszu występowały litery w porządku alfabetycznym

$$S = \begin{pmatrix} a & b & c & d & e & f \\ e & f & d & b & c & a \end{pmatrix}.$$

Jeżeli jest nam jednak wygodniej, można też napisać

$$S = \begin{pmatrix} f & d & e & c & a & b \\ a & b & c & d & e & f \end{pmatrix},$$

gdzie litery dolnego wiersza występują w porządku alfabetycznym, lub w jakikolwiek inny sposób, byleby a przechodziło na e, b na f, itp.

Permutacje można podnosić do kwadratu lub do wyższych potęg. Przez podniesienie permutacji S do kwadratu rozumiemy dwukrotne wykonanie czynności wskazanych w permutacji S. Jeżeli więc w permutacji S litera a przechodzi na literę e, zaś litera e przechodzi na literę c, to w permutacji S^2 litera a przechodzi na literę c. I tak samo, skoro w permutacji S litera b przechodzi na literę f, zaś litera f przechodzi na literę a, więc w permutacji S^2 litera b przechodzi na literę a, itd.:

$$S^2 = \begin{pmatrix} a & b & c & d & e & f \\ c & a & b & f & d & e \end{pmatrix}$$

Podobnie przez S^3 rozumieć należy permutację, w której trzykrotnie wykonano czynności wskazane w permutacji S:

$$S^3 = \begin{pmatrix} a & b & c & d & e & f \\ d & e & f & a & b & c \end{pmatrix}$$

itd. Potęgę ujemną S^{-1} otrzymamy, jeżeli w permutacji S wiersz górny napiszemy jako dolny, a wiersz dolny jako górny

$$S^{-1} = \begin{pmatrix} e & f & d & b & c & a \\ a & b & c & d & e & f \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \\ f & d & e & c & a & b \end{pmatrix}.$$

Dalsze potęgi ujemne S^{-2}, S^{-3}, itd. otrzymamy, jeżeli czynności wskazane w permutacji S^{-1} wykonamy dwukrotnie, trzykrotnie, itd.:

$$S^{-2} = \begin{pmatrix} a & b & c & d & e & f \\ b & c & a & e & f & d \end{pmatrix}, \qquad S^{-3} = \begin{pmatrix} a & b & c & d & e & f \\ d & e & f & a & b & c \end{pmatrix}.$$

Permutację, w której wszystkie litery przechodzą na siebie same, a więc permutację, w której nic się nie zmienia, nazywamy permutacją identyczną albo identycznością albo jednością i oznaczamy przez I:

$$I = \begin{pmatrix} a & b & c & d & e & f \\ a & b & c & d & e & f \end{pmatrix}.$$

Dwie różne permutacje można przez siebie mnożyć. Wtedy iloczyn dwóch permutacji

$$S = \begin{pmatrix} a & b & c & d & e & f \\ e & f & d & b & c & a \end{pmatrix}, \qquad T = \begin{pmatrix} a & b & c & d & e & f \\ d & a & f & c & b & e \end{pmatrix}$$

rozumiemy permutację ST, w której wpierw wykonano czynności wskazane w permutacji S, a następnie czynności wskazane w permutacji T:

$$ST = \begin{pmatrix} a & b & c & d & e & f \\ b & e & c & a & f & d \end{pmatrix}.$$

Iloczyn ST jest na ogół różny od iloczynu TS:

$$TS = \begin{pmatrix} a & b & c & d & e & f \\ b & e & a & d & f & c \end{pmatrix} \neq ST = \begin{pmatrix} a & b & c & d & e & f \\ b & e & c & a & f & d \end{pmatrix}.$$

A zatem mnożenie permutacji nie podlega prawu przemienności.

Jeżeli jednak mnożymy przez siebie różne potęgi tej samej permutacji, wówczas prawo przemienności jest zachowane:

$$S^2S^3 = S^3S^2 = S5 = \begin{pmatrix} a & b & c & d & e & f \\ f & d & e & c & a & b \end{pmatrix}.$$

W szczególności z definicji potęgi ujemnej wynika, że zawsze jest

$$S^{-1}S = SS^{-1} = I$$

i podobnie

$$S^{-2}S^2 = S^2S^{-2} = I, \quad \text{itd.}$$

Poza tym jednak kolejności mnożenia permutacji nie wolno zmieniać. O tym należy pamiętać szczególnie wówczas, gdy chcemy znaleźć nieznaną permutację X. Jeżeli na przykład mamy równanie

$$AX = B,$$

wówczas dla znalezienia permutacji X należy obie strony równania lewostronnie przemnożyć przez A^{-1}:

$$A^{-1}AX = A^{-1}B$$
$$X = A^{-1}B$$

Podobnie dla rozwiązania równania

$$YA = B$$

należy obie strony równania prawostronnie pomnożyć przez A^{-1}:

$$YAA^{-1} = BA^{-1}$$
$$Y = BA^{-1}.$$

Istnieje jeszcze inny sposób przedstawiania permutacji, który w wielu wypadkach jest wygodniejszy, gdyż jest ekonomiczniejszy i ponadto uwidacznia niektóre wewnętrzne cechy permutacji. Polega on na tym, że wypisuje się dowolną literę górnego wiersza permutacji i na prawo od niej pisze się tę literę, która znajduje się pod nią w dolnym wierszu. Litery tej szuka się w górnym wierszu, patrzy, jaka się znajduje pod nią i tę literę wypisuje się na prawo od poprzednich dwóch liter jako trzecią literę. Tak postępujemy [illegible]

nie wypisujemy, lecz dotychczas napisane litery zamykamy w nawias i nazywamy cyklem. Jeżeli w ten sposób wszystkich liter permutacji jeszcze nie wyczerpaliśmy, wybieramy dalszą literę, która w pierwszym cyklu nie wystąpiła i postępując podobnie tworzymy drugi i dalsze cykle aż do wyczerpania wszystkich liter permutacji. W ten sposób można na przykład napisać:

$$S = \begin{pmatrix} a & b & c & d & e & f \\ e & f & d & b & c & a \end{pmatrix} = (a\ e\ c\ d\ b\ f)$$

$$T = \begin{pmatrix} a & b & c & d & e & f \\ d & a & f & c & b & e \end{pmatrix} = (a\ d\ c\ f\ e\ b)$$

$$Q = \begin{pmatrix} a & b & c & d & e & f \\ f & a & e & d & c & b \end{pmatrix} = (a\ f\ b)(c\ e)(d)$$

$$R = \begin{pmatrix} a & b & c & d & e & f \\ a & f & d & e & c & b \end{pmatrix} = (a)(b\ f)(c\ d\ e)$$

Dwie permutacje, w których występujące cykle mają takie same długości, nazywają się permutacjami podobnymi. Ilość i długość cykli charakteryzuje więc w pewnym stopniu permutację. W powyższych przykładach permutacje S i T są permutacjami podobnymi, gdyż w każdej występuje jeden cykl sześcioliterowy. Tak samo permutacje Q i R są podobne, gdyż w każdej z nich występuje jeden cykl trzyliterowy, jeden cykl dwuliterowy i jeden cykl jednoliterowy. Permutacje, dzięki przedstawieniu ich w postaci cyklu lub iloczynu cykli, można podzielić na klasy, zaliczając do jednej i tej samej klasy wszystkie permutacje podobne, a do różnych klas permutacje do siebie nie podobne.

W poszczególnych cyklach dozwolona jest cykliczna zmiana liter, to znaczy na pierwszym miejscu w cyklu można napisać jakąkolwiek literę cyklu, byleby kolejność liter była zachowana.

Cykle dwuliterowe nazywają się też transpozycjami. Jeżeli pomnożymy przez siebie dwie permutacje, z których każda składa się z samych transpozycji, wówczas w iloczynie występują cykle tej samej długości w liczbie parzystej. Przykład:

$$V = (a\ f)(b\ d)(c\ h)(e\ g)(i\ j)$$
$$W = (a\ e)(b\ h)(c\ j)(d\ i)(f\ g)$$
$$VW = (a\ g)(b\ i\ c)(d\ h\ j)(e\ f)$$

Jeżeli mamy permutację S przedstawioną w postaci iloczynu cykli, to permutację S^{-1} otrzymujemy, wypisując w cyklach litery w odwrotnej kolejności. Na przykład:

$$S = (a\ e\ c\ d\ b\ f), \qquad S^{-1} = (f\ b\ d\ c\ e\ a)$$
$$Q = (a\ f\ b)(c\ e)(d), \qquad Q^{-1} = (b\ f\ a)(e\ c)(d).$$

Permutacja S^{-1} nazywa się też odwrotnością permutacji S.

Permutacja składająca się z samych tylko transpozycji i cykli jednoliterowych jest równa swej odwrotności. Kwadrat takiej permutacji jest równy I /Identyczności/. Można to łatwo sprawdzić na przykładach, można też bezpośrednio wyprowadzić z wzoru $S = S^{-1}$. Przemnożenie obu stron wzoru przez S daje $S \cdot S = S^{-1} \cdot S$ czyli $S^2 = I$.

Niezmiernie ważnym pojęciem jest pojęcie przekształcenia. Jeżeli mamy dwie permutacje A i B i jeżeli utworzymy iloczyn $B^{-1}AB$, i iloczyn ten oznaczymy przez C

$$C = B^{-1} \cdot A \cdot B,$$

wówczas mówimy, że permutacja C jest przekształceniem permutacji A przy pomocy permutacji B. Z definicji przekształcenia wynika, że jeżeli C jest przekształceniem permutacji A przy pomocy B, wówczas A jest przekształceniem permutacji C przy pomocy permutacji B^{-1}. Przykład:

$$A = (a\ d\ f)(b\ e)(c)$$
$$B = (a\ b\ c\ d\ e\ f)$$
$$C = (b\ e\ a)(c\ f)(d)$$

Na tym przykładzie widać, że:

1 ermutacja A i przekształcona permutacja C są do siebi podobne.

2. Przekształconą permutację C można otrzymać, dokonując na literach permutacji A zmian wskazanych w permutacji B /t.zn. w danym przykładzie przez zastąpienie każdej litery literą po niej w alfabecie następującą z tym, że po literze f następuje litera a/.

Stąd bardzo ważny wniosek następujący:

Jeżeli mamy do rozwiązania równanie

$$C = X^{-1}A \cdot X$$

z niewiadomą permutacją X, to równanie takie tylko wówczas jest rozwiązalne, gdy dane permutacje C i A są do siebie podobne. Rozwiązanie otrzymujemy, jeżeli pod cyklami permutacji A napiszemy cykle tej samej długości permutacji C i otrzymany w ten sposób dwuwiersz traktować będziemy jako permutację napisaną sposobem tradycyjnym /nie cyklicznym/. Rozwiązanie nie jest jednoznaczne, gdyż rozwiązań otrzymujemy tyle, ile jest możliwości cyklicznych zmian liter w cyklach. W naszym przykładzie rozwiązań jest sześć, gdyż niezależnie od siebie można w cyklu trzyliterowym dokonać trzech zmian cyklicznych, a w cyklu dwuliterowym dwóch zmian:

$$X_1 = \begin{pmatrix} a & d & f & b & e & c \\ b & e & a & c & f & d \end{pmatrix} = (a\ b\ c\ d\ e\ f)$$

$$X_2 = \begin{pmatrix} a & d & f & b & e & c \\ e & a & b & c & f & d \end{pmatrix} = (a\ e\ f\ b\ c\ d)$$

$$X_3 = \begin{pmatrix} a & d & f & b & e & c \\ a & b & e & c & f & d \end{pmatrix} = (a)(d\ b\ c)(f\ e)$$

$$X_4 = \begin{pmatrix} a & d & f & b & e & c \\ b & e & a & f & c & d \end{pmatrix} = (a\ b\ f)(d\ e\ c)$$

$$X_5 = \begin{pmatrix} a & d & f & b & e & c \\ e & a & b & f & c & d \end{pmatrix} = (a\ e\ c\ d)(b\ f)$$

$$X_6 = \begin{pmatrix} a & d & f & b & e & c \\ a & b & e & f & c & d \end{pmatrix} = (a)(d\ b\ f\ e\ c)$$

Tylko rozwiązanie X_1 jest identyczne z permutacją B ze str.38.

Przekształcenia jednej permutacji przy pomocy drugiej można

dokonać również wtedy, gdy obie permutacje, to znaczy przekształcona i przekształcająca lub jedna z nich przedstawione są w postaci niecyklicznej. W tym wypadku zmian wskazanych w permutacji przekształcającej należy dokonać zarówno w górnym jak i w dolnym wierszu permutacji przekształconej. Pokażemy to na przykładzie takiego rodzaju, z jakim w dalszym ciągu będziemy mieli do czynienia, to znaczy na przykładzie permutacji obejmującej 26 liter. Jako permutację przekształcającą przyjmujemy permutację specjalnego typu przedstawioną w postaci jednego cyklu

$$P = (a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z),$$

to znaczy permutację zamieniającą każdą literę na literę następującą po niej w alfabecie z tym, że po literze z następuje litera a. Jako permutację przekształconą przyjmujemy permutację:

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ k & j & p & z & y & d & t & i & o & h & x & c & s & g & u & b & r & n & w & f & m & v & e & q & l & a \end{pmatrix}$$

Otrzymamy wówczas

$$P^{-1}CP = \begin{pmatrix} b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & a \\ l & k & q & a & z & e & u & j & p & i & y & d & t & h & v & c & s & o & x & g & n & w & f & r & m & b \end{pmatrix}$$

Widzimy, że wszystkie litery w permutacji $P^{-1}CP$ są istotnie zaawansowane alfabetycznie o jedną literę w stosunku do permutacji C. Gdybyśmy permutację C przekształcili nie przez P, lecz przez P^{-1}, to znaczy gdybyśmy utworzyli PCP^{-1}, to otrzymalibyśmy

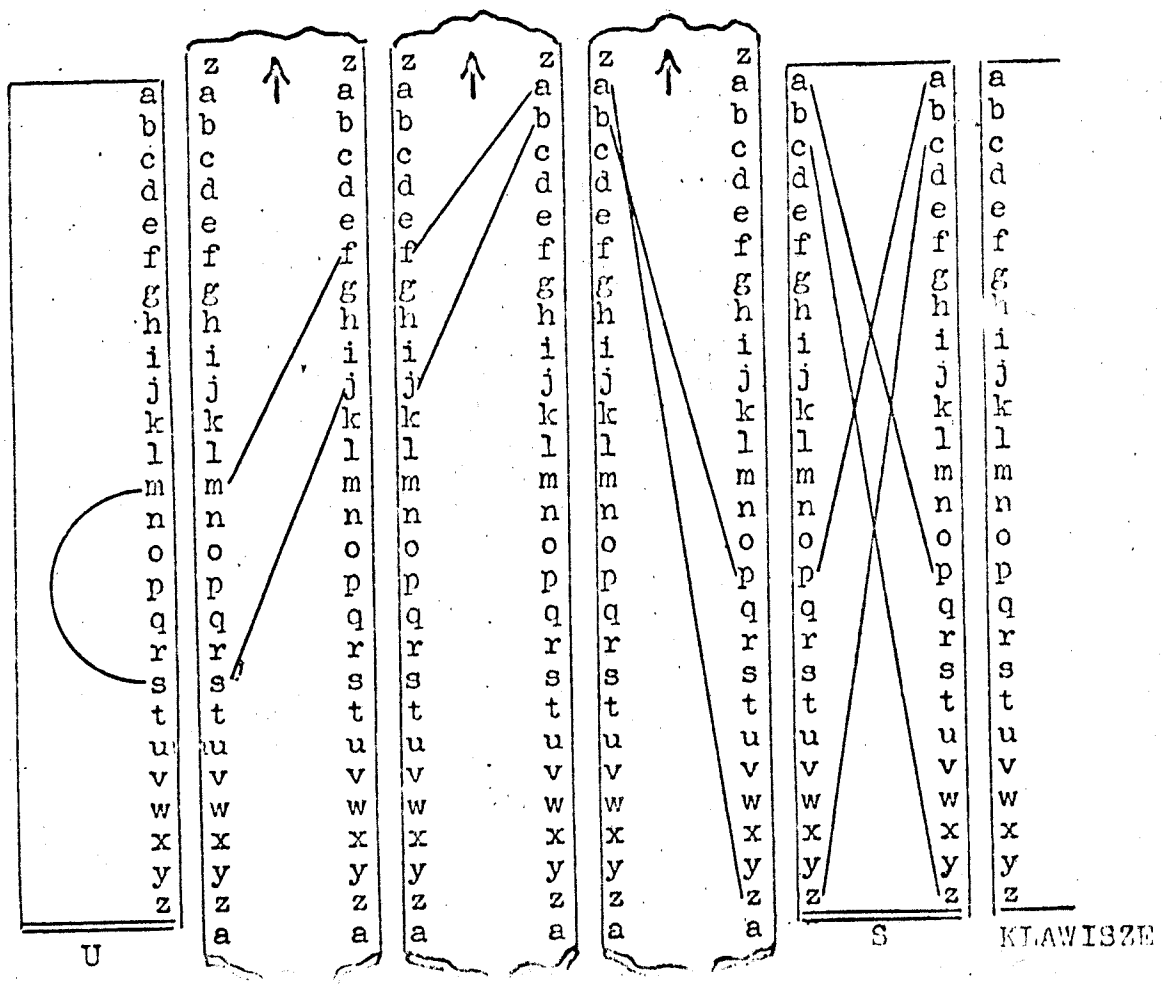
$$PCP^{-1} = \begin{pmatrix} z & a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y \\ j & i & o & y & x & c & s & h & n & g & w & b & r & f & t & a & q & m & v & e & l & u & d & p & k & z \end{pmatrix},$$

w której wszystkie litery są alfabetycznie cofnięte o jedną literę w stosunku do permutacji C.

Ponieważ z permutacją, w której każdą literę zamienia się na literę po niej następującą w alfabecie, będziemy mieli często do czynienia, przeto będziemy ją stale oznaczać tą samą literą P.

VI.

Po zapoznaniu się z podstawowymi własnościami permutacji powracamy obecnie do maszyny "Enigma". Wiemy już, jaki jest jej wygląd i na czym polega jej działanie, ale dla lepszego uzmysłowienia sobie procesów zachodzących w niej w czasie szyfrowania wskazanym jest zastąpić trzywymiarową konstrukcję jakimś dwuwymiarowym jej modelem. Odnosi się to zwłaszcza do tej części maszyny, w której następuje właściwy proces szyfrowania, to jest do bębenków. Wyobraźmy sobie zatem, że zamiast bębenków mamy suwaki. A ponieważ niektóre bębenki, mianowicie bębenki szyfrujące mogą się obracać, przeto musimy przyjąć, że odpowiadające im suwaki rozciągają się w obie strony dostatecznie daleko, aby także w razie przesunięcia suwaków można było śledzić przebieg prądu elektrycznego poprzez ich wewnętrzne połączenia.

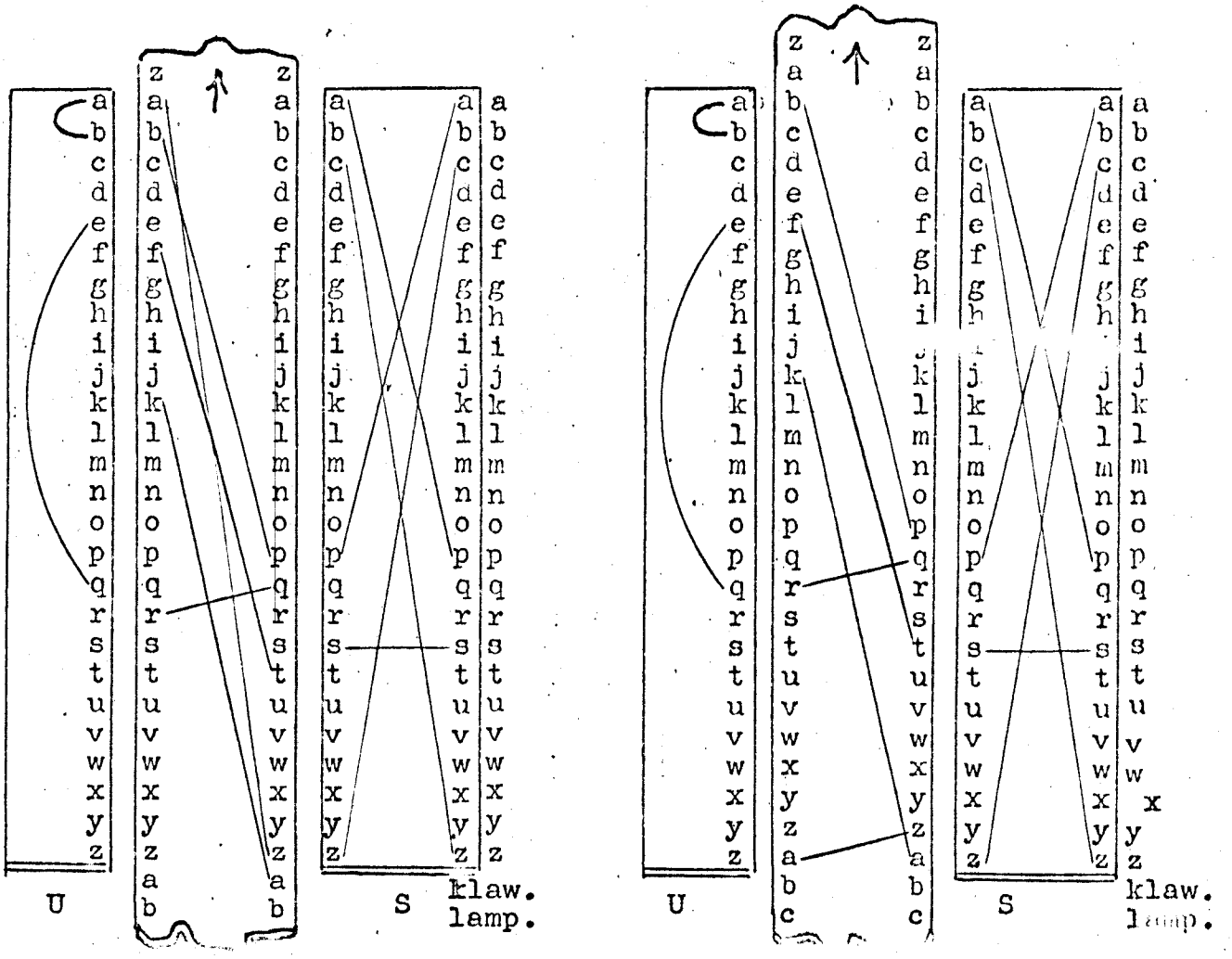


Na schemacie przedstawionym na str. 41. pokazanych jest tylko kilka wewnętrznych połączeń bębenków i kilka połączeń wtyczkowych, w wypadku bowiem narysowania wszystkich połączeń rysunek stałby się bardzo nieprzejrzysty. Kolumna liter po prawej stronie ma oznaczać klawisze wzgl. lampki. Na lewo od niej znajduje się nieruchomy suwak S /Steckerverbindungen/ mający przedstawiać połączenia wtyczkowe. Wspomnieliśmy już na str. 30., że połączenia wtyczkowe odgrywają taką samą rolę co nieruchomy, lecz codziennie zmieniany bębenek szyfrujący. Zwracamy też uwagę na symetryczność połączeń wtyczkowych: jeżeli od litery a biegnie połączenie do kontaktu wyjściowego p, to i nawzajem od litery p biegnie połączenie do kontaktu wyjściowego a, itd. Na lewo od S znajdują się trzy ruchome suwaki C_1, C_2 i C_3 /Chiffrierwalzen/ reprezentujące bębenki szyfrujące, a wreszcie na lewo od nich jest suwak nieruchomy U /Umkehrwalze/ przedstawiający bębenek odwracający.

Cały schemat przedstawia jakąś pozycję bębenków, fikcyjnie przyjętą jako początkową, a kolejne litery na suwakach oznaczają numerację /wyrażoną nie liczbami lecz literami/ ruchomych lub stałych kontaktów na ebonitowych krążkach. Na schemacie można śledzić, jak w danej pozycji suwaków /czyli bębenków/ prąd od klawisza a biegnie poprzez połączenia wtyczkowe, bębenki szyfrujące, bębenek odwracający i z powrotem przez bębenki szyfrujące i połączenia wtyczkowe do lampki c. Taką samą drogą, w odwrotnej kolejności, biegłby prąd od klawisza c do lampki a. W rzeczywistości prąd biegłby dopiero po zamknięciu obwodu, a obwód zamyka się przez naciśnięcie klawisza, ale wówczas bębenek /czyli suwak C_1/ przesunie się o jedną literę w kierunku strzałki i cały obraz przebiegu prądu ulega zmianie. Przebieg prądu i zmiany przebiegu prądu spowodowane przesunięciem bębenka /suwaka/ C_1 wyrazimy przy pomocy permutacji. Przedtem jednak uprościjmy nieco nasz schemat ze str.41.

Z opisu maszyny wiemy, że bębenek C_1 przesuwa się za każdym

uderzeniem klawisza o jedną literę. Bębenek C_2 natomiast przesunie się o jedną literę po wykonaniu przez bębenek C_1 pełnego obrotu, to znaczy po 26 uderzeniach. Kiedy przesunięcie bębenka C_2 nastąpi, tego dokładnie nie wiemy, gdyż zależy to od wcięcia znajdującego się na pierścieniu bębenka C_1, a pozycji tego wcięcia /na razie/ nie znamy. Bębenek C_3 przesuwa się jeszcze o wiele rzadziej. Nas interesują w tej chwili początki depesz czyli ich sześć pierwszych liter. Prawdopodobieństwo, ażeby w czasie wystukiwania sześciu liter nie nastąpiło przesunięcie bębenka C_2, jest dosyć duże, gdyż wynosi 21 : 26 = 80,77 %. Uprościmy sobie znakomicie nasze zadanie, jeżeli przyjmiemy, że w rozpatrywanym przez nas dniu przesunięcie bębenka C_2, a zatem i C_3 nie nastąpiło. Bębenki U, C_3 i C_2 w tym wypadku nie przesunęły się wzajemnie i dlatego możemy te trzy bębenki traktować jako jeden fikcyjny bębenek odwracający. Sprowadziliśmy więc zadanie do rozwiązania maszyny o tylko trzech bębenkach S, C i U.



Rysunek po lewej stronie stanowi odpowiednik do schematu ze str. 41., w którym bębenki U, C_3 i C_2 zastąpiono przez jedan fikcyjny bębenek odwracający U. Przedstawia on zatem przebieg prądu w pozycji wyjściowej, czyli przed naciśnięciem jakiegokolwiek klawisza. Rysunek po prawej stronie przedstawia przebieg prądu po pierwszym naciśnięciu klawisza, czyli po przesunięciu się bębenka /wzgl. suwaka/ C o jedną literę.

Wyraźmy teraz wszystko przy pomocy permutacji i działaniach na permutacjach. Zacznijmy od rysunku po lewej stronie.

Połączenia wtyczkowe powodują zamianę niektórych liter na inne litery. Stanowią zatem pewną permutację S. Tak samo połączenia wewnętrzne bębenka C powodują zmianę liter. Stanowią więc dalszą permutację, którą oznaczymy przez C. Potem prąd biegnie poprzez połączenia wewnętrzne bębenka U, które oznaczymy odpowiednio jako permutację U. Dalej prąd wraca poprzez połączenia bębenka C, ale już w odwrotnym kierunku. Litery ulegają zatem permutacji C^{-1}. W końcu prąd biegnie ponownie poprzez połączenia wtyczkowe, na skutek czego litery ulegają permutacji S^{-1}. Ogółem więc litery alfabetu w pozycji wyjściowej bębenków ulegają kolejnym permutacjom S, C, U, C^{-1}, S^{-1}. Kolejne wykonanie kilku permutacji nazywaliśmy iloczynem permutacji. Jeżeli więc ostateczną zamianę liter na skutek przebiegu prądu poprzez wszystkie połączenia wtyczkowe i bębenki w pozycji wyjściowej oznaczymy przez A_0, to możemy napisać równość:

$$A_0 = SCUC^{-1}S^{-1}.$$

Dla ścisłości należy dodać, że zamiast S^{-1} można też napisać S, gdyż połączenia wtyczkowe zamieniają niektóre litery parami, a innych liter nie zamieniają zupełnie. Permutacja S składa się więc z samych transpozycji i cykli pojedyńczych i jako taka równa jest swej odwrotności /patrz str.38./. Z tych samych względów można by

też napisać U^{-1} zamiast U, bo permutacja U składa się wyłącznie z transpozycji.

Przechodzimy teraz do rysunku po prawej stronie. Początek jest taki sam. Litery alfabetu ulegają permutacji S. Ale teraz następuje zmiana. Na skutek przesunięcia się suwaka litera a nie trafia już na literę a, b na b, itd., lecz obecnie litera a trafia na literę b, litera b na c, itd. Litery alfabetu ulegają więc permutacji, która każdą literę zastępuje przez jej następną. Taką permutację umówiliśmy się /patrz str. 40./ oznaczać literą P. Potem następuje permutacja C, a potem, jak to na rysunku można odczytać, następuje permutacja P^{-1}. Następną permutacją jest U, a potem następują wszystkie poprzednie permutacje w odwrotnej kolejności i w odwrotnej potędze. Jeżeli więc efekt pierwszego uderzenia w klawisze oznaczymy jako permutację A_1, wówczas możemy napisać równość

$$A_1 = SPCP^{-1}UPC^{-1}P^{-1}S^{-1}$$

Łatwo sobie uzmysłowić, że efekt drugiego uderzenia w klawisze, a więc ponowne przesunięcie się suwaka w górę, doprowadza do równości

$$A_2 = SP^2CP^{-2}UP^2C^{-1}P^{-2}S^{-1}$$

i podobnie następne przesunięcie do równości

$$A_3 = SP^3CP^{-3}UP^3C^{-1}P^{-3}S^{-1}$$

itd., itd. Z każdym dalszym uderzeniem klawiszów, a więc z każdym dalszym obróceniem się bębenka C permutacja P występować będzie w coraz to wyższej /dodatniej lub ujemnej/ potędze, podczas gdy pozostałe permutacje S, C i U występują zawsze w tej samej postaci.

Jeżeli w określonym dniu przy pomocy metody przedstawionej na str. str. 16 - 25 uda się odtworzyć klucze, wówczas dla sześć ko-

lejnych pożycji bębenków znany jest efekt przebiegu prądu, to znaczy wiadomym jest, jakie lampki zapalą się przy uderzeniu każdego klawisza /patrz str.26./, innymi słowy, znane są wówczas permutacje A_1, A_2, A_3, A_4, A_5 i A_6. Permutacja P i jej potęgi są nam oczywiście też znane, nieznane natomiast są permutac[illegible] C [illegible] U. Zadanie nasze sprowadziliśmy zatem do rozwiązania układu sześciu równań z trzema niewiadomymi permutacjami. Ponieważ w stosunku do mno[illegible]żenia permutacji prawo przemienności /patrz str. 35./ nie zachodzi, przeto rozwiązanie tego układu równań jest niezwykle trudne lub może nawet niemożliwe.

Szczęśliwym zbiegiem okoliczności Biuro Szyfrów jednocześnie z fotokopią instrukcji o posługiwaniu się maszyną "Enigma" znalazło się w posiadaniu fotokopii kompletu kluczy za okres dwóch miesięcy. Jeżeli dobrze pamiętam, były to klucze za wrzesień i październik 1932 roku. Za ten więc okres były m.i. znane połączenia wtyczkowe, a tym samym permutacja S, dzięki czemu stało się możliwym uproszczenie naszego układu sześciu równań. Przez odpowiednie prawo- i lewostronne pomnożenie obu stron równań przez permutacje znane doprowadzamy nasz układ równań do następującej postaci

$$B_1 = P^{-1}S^{-1}A_1SP = CP^{-1}UP\,C^{-1}$$
$$B_2 = P^{-2}S^{-1}A_2SP^2 = CP^{-2}UP^2C^{-1}$$
$$B_3 = P^{-3}S^{-1}A_3SP^3 = CP^{-3}UP^3C^{-1}$$
$$B_4 = P^{-4}S^{-1}A_4SP^4 = CP^{-4}UP^4C^{-1}$$

Ostatnich dwóch równań nie piszemy, gdyż nie będą nam w dalszym ciągu potrzebne. Lewe strony równań zawierają same wielkości znane. Oznaczyliśmy je dla skrócenia odpowiednio przez B_1, B_2, B_3 i B_4. Permutacje B składają się, jak łatwo widać, z samych transpozycji /bo U składa się z samych transpozycji, a permutacje B jako przekształcone z U są podobne do U/. Ponieważ manipulowanie permutacjami składającymi się z samych transpozycji jest w naszym wypadku [illegible] niedogodne, przeto zastępujemy [illegible]

innym, pozornie bardziej skomplikowanym układem otrzymanym przez utworzenie iloczynów B_1B_2, B_2B_3, B_3B_4 :

$$B_1B_2 = CP^{-1}UP^{-1}UP^2C^{-1}$$
$$B_2B_3 = CP^{-2}UP^{-1}UP^3C^{-1}$$
$$B_3B_4 = CP^{-3}UP^{-1}UP^4C^{-1}$$

Układ ten, po pewnych elementarnych przekształceniach, można też przedstawić w postaci następującej:

$$\begin{cases} B_1B_2 = CP^{-1}UP^{-1}UP^2C^{-1} = B_1B_2 \\ B_2B_3 = CP^{-1}C^{-1}(CP^{-1}UP^{-1}UP^2C^{-1})CPC^{-1} = CP^{-1}C^{-1}(B_1B_2)CPC^{-1} \end{cases}$$

$$\begin{cases} B_2B_3 = CP^{-2}UP^{-1}UP^3C^{-1} = B_2B_3 \\ B_3B_4 = CP^{-1}C^{-1}(CP^{-2}UP^{-1}UP^3C^{-1})CPC^{-1} = CP^{-1}C^{-1}(B_2B_3)CPC^{-1} \end{cases}$$

Teraz możemy zastosować metodę wskazaną na str. 39. Przez podpisanie na wszystkie możliwe sposoby permutacji B_2B_3 przedstawionej w postaci cykli pod permutacją B_1B_2 przedstawioną w postaci cykli otrzymamy szereg permutacji, wśród których jedna powinna być permutacją CPC^{-1}. Ale ten sam rezultat otrzymamy, podpisując permutację B_3B_4 na wszystkie możliwe sposoby pod permutację B_2B_3. Ta permutacja, która w obu szeregach się powtórzy, będzie szukaną permutacją CPC^{-1}. I jeżeli teraz pod znaną nam permutacją P napiszemy permutację CPC^{-1}, to w wyniku otrzymamy permutację C^{-1}, a stąd, przez prostą zamianę górnego i dolnego wiersza, permutację C czyli wewnętrzne połączenia bębenka szyfrującego C.

To, z natury rzeczy dość abstrakcyjne, żonglowanie wzorami, równaniami i przekształceniami zilustrujemy teraz na przykładzie. Na str. 24. podaliśmy początki depesz z jednego dnia i odpowiadające im klucze. Otrzymane tam wyniki możemy też przedstawić w postaci permutacji A_1 do A_6. Ograniczymy się jednak do podania tylko czterech pierwszych permutacji, gdyż są one, jak to okazaliśmy, wystarczające dla uzyskania zamierzonego wyniku. Podajemy je też od razu w postaci cykli jako ekonomiczniejszej i dla naszych

celów dogodniejszej:

$$A_1 = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)$$
$$A_2 = (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz)$$
$$A_3 = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)$$
$$A_4 = (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy)$$

Podajemy też permutację S, gdyż zgodnie z naszyni założeniami uważamy połączenia wtyczkowe jako znane:

$$S = (ap)(bl)(cz)(fh)(jk)(qu)(d)(e)(g)(i)(m)(n)(o)(r)(s)(t)(v)(w)(x)(y)$$

Dla wygody podajemy również permutację P i jej potęgi:

$$P = (abcdefghijklmnopqrstuvwxyz)$$
$$P^2 = (acegikmoqsuwy)(bdfhjlnprtvxz)$$
$$P^3 = (adgjmpsvybehknqtwzcfilorux)$$
$$P^4 = (aeimquycgkosw)(bfjnrvzdhlptx)$$

Potęg ujemnych permutacji P nie podajemy, gdyż, jak to podaliśmy na str. 38., wystarczy /w myśli/ odwrócić porządek liter w cyklach permutacji P i jej potęg dodatnich, by otrzymać potęgi ujemne. Mając powyższe dane możemy utworzyć permutacje B:

$$B_1 = P^{-1}S^{-1}A_1SP = (ax)(bu)(ck)(dr)(ej)(fw)(gi)(lp)(ms)(nz)(oh)(qt)(vy)$$
$$B_2 = P^{-2}S^{-1}A_2SP^2 = (ar)(bv)(co)(dh)(fl)(gk)(iz)(jp)(mn)(qy)(su)(tw)(xe)$$
$$B_3 = P^{-3}S^{-1}A_3SP^3 = (as)(bz)(cp)(dq)(eo)(fw)(gj)(hl)(iy)(kr)(mu)(nt)(vx)$$
$$B_4 = P^{-4}S^{-1}A_4SP^4 = (ap)(bf)(cu)(dv)(ei)(gr)(ho)(jn)(ky)(lx)(mz)(qs)(tw)$$

oraz iloczyny permutacji B_1B_2, B_2B_3 i B_3B_4 :

$$B_1B_2 = (aepftybsnikod)(cgzmuvqwljxrh)$$
$$B_2B_3 = (akjcevzydlwnu)(bxopgrsmtfhqi)$$
$$B_3B_4 = (aqvloikgnwbmc)(dspuzftjryehx)$$

To, że we wszystkich trzech równaniach długości cykli są takie same, wskazuje, że widocznie w obrębie sześciu pierwszych uderzeń klawiszów nie nastąpiło przesunięcie się środkowego bębenka szyfrującego i że prawdopodobnie nie popełniliśmy błędów przy mnożeniu

przez siebie permutacji. Wiemy przecież, że permutacje B_1B_2, B_2B_3 i B_3B_4 mają być do siebie podobne.

Zgodnie z receptą podaną na str. 47. powinniśmy teraz pod cykle permutacji B_1B_2 podpisać na wszystkie możliwe sposoby cykle permutacji B_2B_3 i podobnie pod cykle permutacji B_2B_3 p dpisać na wszystkie możliwe sposoby cykle permutacji B_3B_4. Możemy tak postąpić, gdyż zbyt wiele możliwości nie ma. Ale zadanie można sobie w różny sposób ułatwić, n.p. pamiętając o tym, że otrzymany wynik, to jest permutacja CPC^{-1} jako podobna do permutacji P musi się składać z jednego tylko cyklu 26-literowego. Można też posługiwać się przesuwanymi paskami papieru. W każdym razie kilka prób wystarczy, aby przekonać się, że cykle można podpisać pod sobą tylko w sposób następujący:

$$\begin{matrix} B_1B_2 = \\ B_2B_3 = \end{matrix}\begin{pmatrix}(aepftybsnikod)(cgzmuvqwljxrh)\\ (ydlwmuakjcevz)(xopgrsmtfhc\ldots\end{pmatrix} = CPC^{-1}$$

$$\begin{matrix} B_2B_3 = \\ B_3B_4 = \end{matrix}\begin{pmatrix}(ydlwmuakjcevz)(xopgrsmtfhqib)\\ (uzftjryehxdsp)(qvloikgnwbmca)\end{pmatrix} = CPC^{-1}$$

bo tylko przy tym sposobie na permutację CPC^{-1} otrzymujemy w obu wypadkach ten sam wynik:

$$CPC^{-1} = (ayuricxqmgovskedzplfwtnjhb)$$

Dalszy ciąg jest prosty. Podpisując pod permutacją P permutację CPC^{-1} na wszystkie możliwe sposoby, a sposobów takich jest 26, otrzymamy 26 wariantów dla permutacji C^{-1}. Jeden z wariantów jest na przykład

$$C^{-1} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ z & p & l & f & w & t & n & j & h & b & a & y & u & r & i & c & x & q & m & g & o & v & s & k & e & d \end{pmatrix}$$

Zamieniając wiersz górny i dolny otrzymamy:

$$C = \begin{pmatrix} z & p & l & f & w & t & n & j & h & b & a & y & u & r & i & c & x & q & m & g & o & v & s & k & e & d \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \end{pmatrix}$$

a po alfabetycznym uporządkowaniu górnego wiersza otrzymujemy wreszcie

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ k & j & p & z & y & d & t & i & o & h & x & c & s & g & u & b & r & n & w & f & m & v & e & q & l & a \end{pmatrix}$$

Jest to, jak wspomnieliśmy, jeden z 26 możliwych wariantów. Pozostałe nie różnią się od niego w sposób istotny. Otrzymamy je kolejno wszystkie, zastępując w dolnym wierszu każdą literę przez literę po nią w alfabecie następującą, n.p.:

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ l & k & q & a & z & e & u & j & p & i & y & d & t & h & v & c & s & o & x & \cdot & \cdot & \cdot & \cdot & f & \cdot & b \end{pmatrix}$$

albo

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & l & r & b & a & f & v & k & q & j & z & e & u & i & w & d & t & p & y & h & o & x & g & s & n & c \end{pmatrix}$$

itd., itd. Każdemu wariantowi permutacji C odpowiada jeden określony wariant permutacji U, który można znaleźć n.p. z podanego na str. 45. wzoru

$$B_1 = CP^{-1}UPC^{-1}$$

przez odpowiednie prawo- i lewostronne pomnożenie

$$U = PC^{-1}B_1CP^{-1}.$$

W istocie rzeczy jednak permutacja U specjalnie nas nie interesuje, gdyż przedstawia nie rzeczywisty bębenek odwracający, lecz fikcyjny składający się z bębenków szyfrujących C_2, C_3 i U rzeczywistego.

Dalszym naszym zadaniem było więc odtworzenie połączeń wewnętrznych pozostałych bębenków. Nie będę szczegółowo opisywał, jak to się odbyło. Przypomnę tylko, że Biuro Szyfrów było w posiadaniu fotokopii kluczy z dwóch miesięcy należących do różnych kwartałów /wrzesień i październik 1932r./. A ponieważ kolejność bębenków

zmieniała się raz na kwartał, więc metodę przedstawioną na poprzednich stronicach można było zastosować do znalezienia połączeń wewnętrznych dwóch różnych bębenków, i to na podstawie materiału szyfrowego z jednego tylko dnia w każdym z obu miesięcy. Łatwo zrozumieć, że pozostały materiał szyfrowy [illegible] z tego okresu był wystarczający do znalezienia połączeń reszty bębenków i wszelkich innych szczegółów ich budowy, jak momentów ich przesuwania się itp., tak że jeszcze przed końcem 1932 roku można było odczytać całkowicie materiał szyfrowy z tego okresu.

Był to niewątpliwie niemały sukces, zwłaszcza jeżeli weźmie się pod uwagę, że ani francuskie ani angielskie biura szyfrów - jak się to dalej okaże - pomimo długoletnich tradycji i doświadczeń w dziedzinie kryptologii i daleko większych niż polskie Biuro Szyfrów zasobów ludzkich i materialnych, nawet w roku 1938 jeszcze nie były w posiadaniu metody rozwiązania szyfru "Enigma" i dopiero dzięki współpracy z Polskim Biurem Szyfrów tę tajemnicę posiadły.

VII.

Odtworzenie wewnętrznych połączeń bębenków było ważnym, ale jeszcze nie końcowym etapem na drodze do całkowitego opanowania szyfru maszynowego. Mając już maszynę, należało z kolei opracować metody pozwalające odtworzyć, na podstawie samego materiału szyfrowego, wszystkie składniki klucza, które, jak to podano na str. 30 - 31, zmieniały się w różnych odstępach czasu.

Metod takich opracowano i stosowano cały szereg, różne w różnych okresach czasu, skomplikowane i prymitywne, kosztowne i niekosztowne, zmechanizowane i niezmechanizowane. Bo Niemcy, czy to wyczuwając, że ich szyfry czytamy, czy też dla samej zasady co pe-

ków szyfrowych, która początkowo wynosiła 3, podnieśli naprzód do 4, a potem do 5, przez co ogromnie wzrosła liczba możliwych kolejności bębenków. Samą kolejność bębenków, zmienianą pierwotnie co kwartał, zaczęli zmieniać co miesiąc, a wreszcie codziennie. Tak samo nastawienie pierścieni zmieniano codziennie, a liczba połączeń wtyczkowych, która początkowo była stała i wynosiła 6, w późniejszym okresie wahała się od 5 do 9. W ten sposób okres siedmiu lat od końca 1932 roku do wybuchu wojny w roku 1939 stanowił nieustanny pojedynek pomiędzy niemieckim i polskim biurem szyfrów, z którego stale wychodziliśmy zwycięsko.

Szczegółowy opis wszystkich stosowanych wówczas metod zająłby dużo miejsca. Poza tym niektóre z tych metod zatarły się w mej pamięci do tego stopnia, że nie mam już możności ich zrelacjonowania. Konieczność więc zmusza mnie do ograniczenia się do przedstawienia tutaj tylko kilku z nich i do poświęcenia innym najwyżej krótkiej wzmianki.

Ponieważ początkowo zmiana kolejności bębenków odbywała się jeden raz na kwartał, przeto na razie nie stanowiła dla nas specjalnego problemu. Wystarczyło wyznaczyć ją jakąkolwiek drogą, by mieć spokój na trzy miesiące. I tak na przykład dzięki posiadaniu kluczy za miesiąc październik 1932 roku znana nam była kolejność bębenków także w listopadzie i grudniu tego roku. Również ze znalezieniem nastawienia pierścieni, zmienianego w początkowym okresie tylko jeden raz na miesiąc, nie było w tym czasie jeszcze większego kłopotu. Pozycja zasadnicza bębenków była wprawdzie zmieniana codziennie, ale potrzebną była właściwie tylko do szyfrowania i deszyfrowywania początków depesz, które i tak umieliśmy odtwarzać innym sposobem. W tych warunkach punkt ciężkości zadania przesunął się do codziennego odnajdywania połączeń wtyczkowych stanowiących jak gdyby dodatkowy bębenek szyfrujący. Do tego celu zastosowaliśmy między innymi następującą metodę:

Gdy przedstawialiśmy metodę odtwarzania początków depesz, umawialiśmy się, że cykle, jakie powstają /patrz str. 21./ z pierwszych i czwartych liter początków depesz, oznaczać będziemy przez A_1A_4, cykle, jakie powstają z drugich i piątych liter depesz, przez A_2A_5 i cykle, jakie powstają z trzecich i szóstych liter początków depesz przez A_3A_6. W oparciu o własności permutacji, które potem poznaliśmy, łatwo zauważymy, że oznaczenie A_1A_4 /jak również oznaczenia dalsze/ bynajmniej nie zostało dowolnie obrane, lecz że istotnie przedstawia iloczyn dwóch permutacji, z których pierwsza, A_1 stanowi efekt przejścia prądu elektrycznego od klawiszy do lampek po pierwszym uderzeniu klawisza, a druga, A_4 ten sam efekt po czwartym uderzeniu klawisza. Można to sprawdzić przez rzeczywiste pomnożenie permutacji A_1 przez permutację A_4 ze str. 48. i porównanie z wyrażeniem A_1A_4 na str. 41. Z drugiej strony ogólny wzór na permutację A_1 podany jest na str.45. Podajemy go tu ponownie

$$A_1 = SPCP^{-1}UPC^{-1}P^{-1}S^{-1}$$

jak również /poprzednio nie podany/ ogólny wzór na A_4

$$A_4 = SP^4CP^{-4}UP^4C^{-1}P^{-4}S^{-1}$$

Przez pomnożenie otrzymujemy:

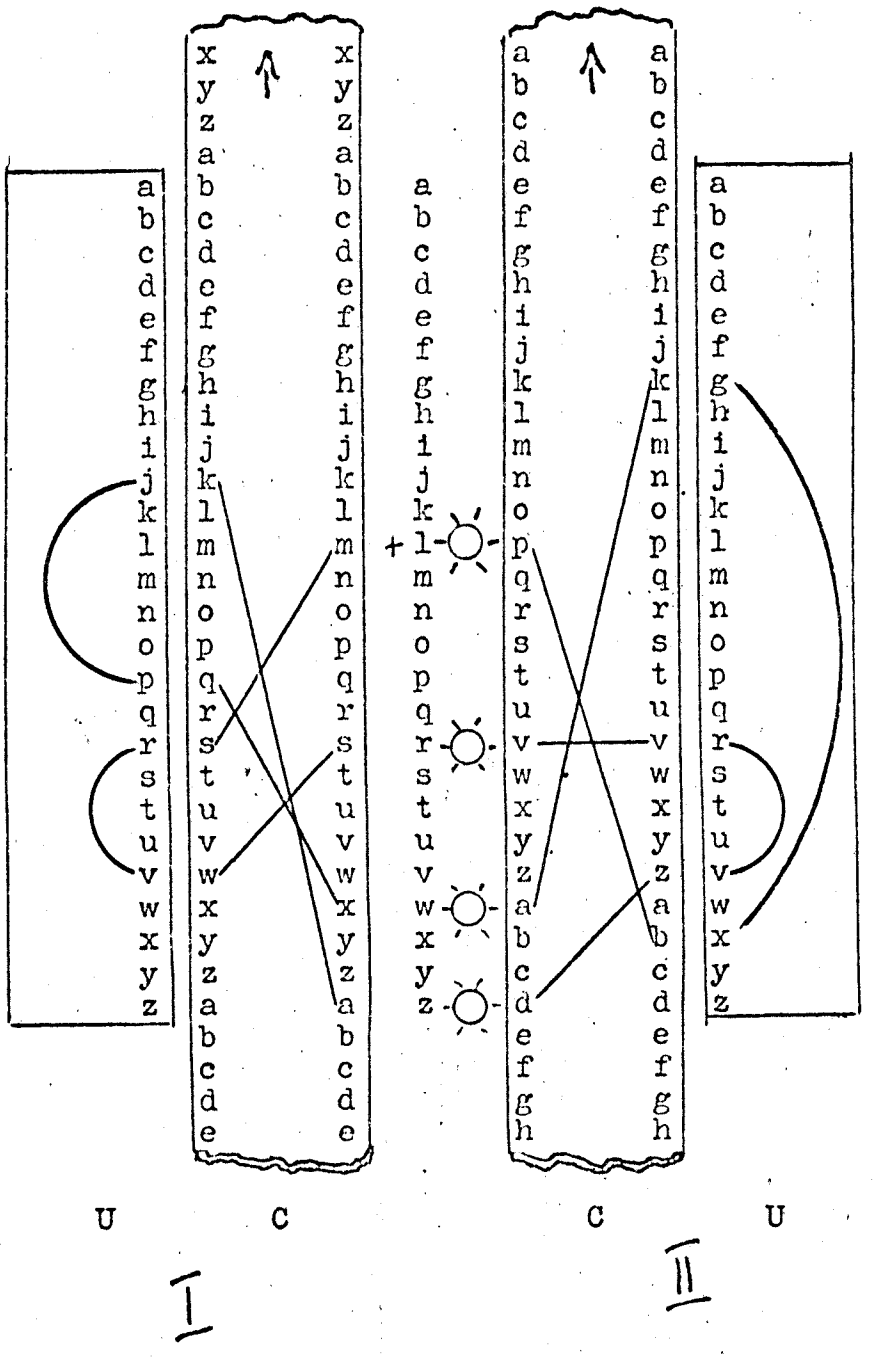
$$A_1A_4 = SPCP^{-1}UPC^{-1}P^3CP^{-4}UP^4C^{-1}P^{-4}S^{-1}$$

Iloczyn ten jest podobny, a więc składa się z tych samych cykli, co iloczyn

$$A_1'A_4' = PCP^{-1}UPC^{-1}P^3CP^{-4}UP^4C^{-1}P^{-4}$$

powstały z iloczynu A_1A_4 przez wyeliminowanie permutacji S, to jest połączeń wtyczkowych. W iloczynie $A_1'A_4'$ w zasadzie wszystko jest znane, pomijając pozycje bębenków szyfrujących i bębenka od-

wracającego /pamiętajmy, że bębenek odwracający jest fikcyjny i składa się z trzech bębenków, z których dwa są ruchome i jeden nieruchomy/. Ale tych pozycji nie jest znów tak bardzo dużo, bo dla każdej kolejności bębenków ilość ta wynosi 26·26·26 = 17576. Zbudowaliśmy /to jest firma AVA zbudowała/ więc specjalną maszynę składającą się w zasadzie z dwóch sprzężonych ze sobą maszyn "Enigma", tylko bez połączeń wtyczkowych, bez przestawialnych pierścieni, bez klawiszy, lecz z przełącznikami przy każdej żarówce. Maszynę nazwaliśmy cyklometrem, a jej działanie obrazuje poniższy rysunek:



Dla uzyskania większej przejrzystości na rysunku kolejność bębenków w części II jest odwrócona, tak że bębenek odwracający części II znajduje się teraz po prawej stronie. Między obiema częściami cyklometru znajduje się układ żarówek z przełącznikami. Bębenek C części II jest przesunięty o trzy litery w stosunku do bębenka C części I. W ten sposób, jeżeli pozycję bębenków w części I oznaczymy przez A_1, to pozycję bębenków w części II należy odpowiednio oznaczyć przez A_4. Jeżeli teraz przy jakiejkolwiek żarówce, na przykład przy żarówce l włączymy źródło prądu przez przestawienie przełącznika, wówczas prąd będzie przebiegać na przemian przez część I i część II cyklometru, aż po pewnej ilości przebiegów wróci do żarówki l. Jednocześnie zapalą się te żarówki, które znalazły się na drodze prądu. Ich liczba jest zawsze parzysta i jest równa podwójnej liczbie liter któregoś z cykli permutacji A_1A_4. W naszym przykładzie zapalą się cztery żarówki l, r, w, z, odpowiadające dwom cyklom dwuliterowym (bc), (rw) permutacji A_1A_4 ze str.21. Litery są oczywiście częściowo inne na skutek połączeń wtyczkowych, których w cyklometrze nie ma. Po przestawieniu innego przełącznika zapalą się znów inne żarówki, z których liczby można wnioskować o długości dalszego cyklu permutacji A_1A_4. W ten sposób przy pomocy cyklometru, obracając kolejno bębenkami i licząc zapalające się żarówki, można określić długość cykli permutacji A_xA_{x+3} dla wszystkich 17576 pozycji bębenków przy danej kolejności bębenków. Łatwo domyśleć się, że cyklometr był zaopatrzony w opornicę, w przeciwnym bowiem wypadku, wobec nieró..nej il ści zapalających się żarówek, albo żarówki nie zapalałyby się, albo zaraz by się przepalały.

Należało jeszcze w jakikolwiek sposób ponumerować wszelkie możliwe kształty, jakie permutacje A_xA_{x+3} przedstawione w postaci cyklicznej mogą przyjąć, aby każdej pozy i bębenków podporządkować pewną liczbę, na przykład

permutacji	(13)(13)	podporządkować liczbę 1
"	(12)(12)(1)(1)	" " 2
"	(11)(11)(2)(2)	" " 3
"	(11)(11)(1)(1)(1)(1)	" " 4
.....		
"	(1)(1)(1)(1)...(1)(1)	" " 101

gdyż istotnie różnych klas jest 101./Zagadnienie "partitio numerorum" addytywnej teorii liczb/.

Pisząc przy każdej pozycji bębenków odpowiadającą tej pozycji liczbę i dwie liczby odpowiadające dwom następnym pozycjom otrzymamy to, co nazwaliśmy charakterystyką danej pozycji bębenków, na przykład

pozycja	a a a	charakterystyka 7, 6, 9
"	a a b	" 6, 9, 1
"	a a c	" 9, 1, 3
"	a a d	" 1, 3,12
.....		
.....		
"	z z z	" 10, 1, 1

W ten sposób dla każdej kolejności bębenków stworzyliśmy sobie kartotekę charakterystyk składającą się z 17576 pozycji. Takich kartotek mieliśmy 6,odpowiednio do 6 różnych kolejności bębenków /przy trzech bębenkach szyfrujących/. Tych samych charakterystyk w obrębie jednej kartoteki było zazwyczaj kilka, niekiedy kilkanaście, rzadziej kilkadziesiąt.

Jeżeli teraz przy pomocy metody wskazanej na str. 21. utworzymy z początków depesz określonego dnia iloczyny A_1A_4, A_2A_5, A_3A_6, i określimy właściwą dla tego dnia charakterystykę, to wystarczy odszukać ją w kartotece i znając odpowiadającą jej pozycję bębenków utworzyć iloczyny /na maszynie "Enigma", nie na cyklometrze/ $A_1'A_4'$, $A_2'A_5'$, $A_3'A_6'$ i drogą porównania zn[illegible] połączenia wtyczkowe. Najlepiej wyjaśni to przykład:

Niech iloczynom A_1A_4, A_2A_5 i A_3A_6 podanym na str. 21. odpowiada charakterystyka 6,9,1. W kartotece naszej stwierdzamy, że charakterystyka 6,9,1 występuje w pozycji bębenków a,a,b. Na maszynie "Enigma" w pozycji bębenków a,a,b wystukujemy cały alfabet i otrzymujemy

$$A_1' = (at)(bj)(cq)(di)(ev)(fh)(gn)(ko)(lr)(my)(ps)(ux)(wz).$$

Tak samo wystukujemy cały alfabet przy pozycji bębenków a,a,e i otrzymujemy

$$A_4' = (ae)(bx)(cn)(dk)(fj)(gu)(ht)(lw)(mo)(ps)(qy)(rz)(iv).$$

Przez pomnożenie otrzymujemy

$$A_1'A_4' = (ahjxgcyodv)(eikmqnubft)(lz)(p)(rw)(s).$$

Ale permutacja $A_1'A_4'$ jest przekształcona z permutacji A_1A_4 przy pomocy permutacji S, jak to wynika ze wzorów podanych na str. 53. Należy więc cykle permutacji $A_1'A_4'$ napisać na wszystkie możliwe sposoby pod cykle permutacji A_1A_4. Ponieważ zaś permutacja S jest szczególnego rodzaju, gdyż składa się z samych tylko transpozycji i cykli pojedyńczych, przeto zadanie nasze jest niezwykle ułatwione i nie ma nawet potrzeby uciekać się do porównywania $A_2'A_5'$ i $A_3'A_6'$ z permutacjami A_2A_5 i A_3A_6, by po kilku próbach otrzymać

$$S = \begin{pmatrix}(dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)\\(dvahjxgcyo)(eikmqnubft)(lz)(rw)(p)(s)\end{pmatrix}$$

czyli

$$S = (ap)(bl)(cz)(fh)(jk)(qu),$$

gdyż cykli jednoliterowych (d), (e), itd nie musimy wypisywać.

W tym więc wypadku połączenia wtyczkowe znaleźliśmy bez trudu. Jednak nie zawsze sprawa ta przedstawia się tak prosto. Jeżeli w kartotece identycznych charakterystyk z charakt[illegible] dan[illegible]

dnia jest dużo, wówczas odnalezienie pośród nich właściwej pozycji bębenków staje się czynnością dość pracochłonną. Ale to jeszcze nie wszystko. Może się okazać, że właściwej pozycji bębenków wogóle nie znajdziemy. Cała kartoteka została przecież sporządzona przy założeniu, że w obrębie początków depesz nie ma przesunięcia bębenka środkowego. Dzieje się tak wprawdzie w 21 przypadkach na 26, niemniej jednak materiał szyfrowy z kilku dni w każdym miesiącu pozostaje niedostępny dla tej metody. Można by kartotekę rozciągnąć i na te przypadki, wymagałoby to jednak pięciokrotnego powiększenia kartoteki, co nie tylko pochłonęłoby dużo czasu dla jej sporządzenia, ale co przede wszystkim znacznie zmniejszyłoby jej użyteczność na skutek o wiele większej ilości identycznych charakterystyk. Dlatego korzystano jeszcze z innych dróg.

Metoda "kartoteki" opierała się przede wszystkim na tej własności, że połączenia wtyczkowe nie mają wpływu na kształt cykli w iloczynach A_1A_4, A_2A_5 i A_3A_6. Metoda "siatki", którą teraz przedstawimy, wykorzystuje okoliczność, że połączenia wtyczkowe pozostawiają część liter bez zmian.

Z równań podanych na str. 45. można przez prawo- i lewostronne pomnożenie wyliczyć U:

$$U = PC^{-1}P^{-1}S^{-1}A_1SPCP^{-1}$$
$$U = P^2C^{-1}P^{-2}S^{-1}A_2SP^2CP^{-2}$$
$$U = P^3C^{-1}P^{-3}S^{-1}A_3SP^3CP^{-3}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Permutacja U jest nam wprawdzie nieznaną, wiemy jednak, że jeżeli w obrębie początków depesz nie nastąpi przesunięcie środkowego bębenka, wówczas U jest to samo dla wszystkich sześć równań. Jeżeli w obrębie początków depesz nastąpi przesunięcie środkowego bębenka, wówczas U przyjmie dwie wartości, jedną przed, drugą po przesunięciu bębenka środkowego. W każdym razie co najmniej trzy pierwsze albo trzy ostatnie U są ze sobą identyczne. Przyjmijmy na przykład że trzy

pierwsze U są identyczne. Zakładamy, że potrafimy odtworzyć klucze metodą wskazaną na str. 24., czyli że znane nam są permutacje A_1, A_2 i A_3. Każda z tych permutacji składa się z 13 transpozycji. Ponieważ permutacja S nie zmienia wszystkich liter, przeto możemy się spodziewać, że w każdej z permutacji A kilka transpozycji pozostaje niezmienionych pomimo przekształcenia przez S. Jeżeli więc utworzymy wyrażenia

$$P\,C^{-1}P^{-1}A_1P\,CP^{-1}$$
$$P^2C^{-1}P^{-2}A_2P^2CP^{-2}$$
$$P^3C^{-1}P^{-3}A_3P^3CP^{-3}$$

przez opuszczenie w równaniach na U permutacji S, to wyrażenia te już nie będą ani równe U ani równe między sobą, ale niektóre transpozycje będą się jednak we wszystkich trzech wyrażeniach powtarzać. Kłopot polega wszakże na tym, że chociaż znamy połączenia wewnętrzne bębenka C, to nie znamy jego pozycji. Ale różnych pozycji bębenka C jest tylko 26 i wszystkie permutacje odpowiadające kolejnym pozycjom bębenka C otrzymamy, przekształcając permutację C przez P^{-1}, P^{-2}, ..., P^{-25}. Permutacja $P^{26}CP^{-26}$ znów równa się C, gdyż, jak łatwo się przekonać:

$$P^{26} = P^{-26} = I \text{ /Identyczność/.}$$

Należy zatem utworzyć wspomniane wyżej wyrażenia:

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ k & j & p & z & y & d & t & i & o & h & x & c & s & g & u & b & r & n & w & f & m & v & e & q & l & a \end{pmatrix}$$

$$PCP^{-1} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ i & o & y & x & c & s & h & n & g & w & b & r & f & t & a & q & m & v & e & l & u & d & p & k & z & j \end{pmatrix}$$

$$P^2CP^{-2} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ n & x & w & b & r & g & m & f & v & a & q & e & s & z & p & l & u & d & k & t & c & o & j & y & i & h \end{pmatrix}$$

.....

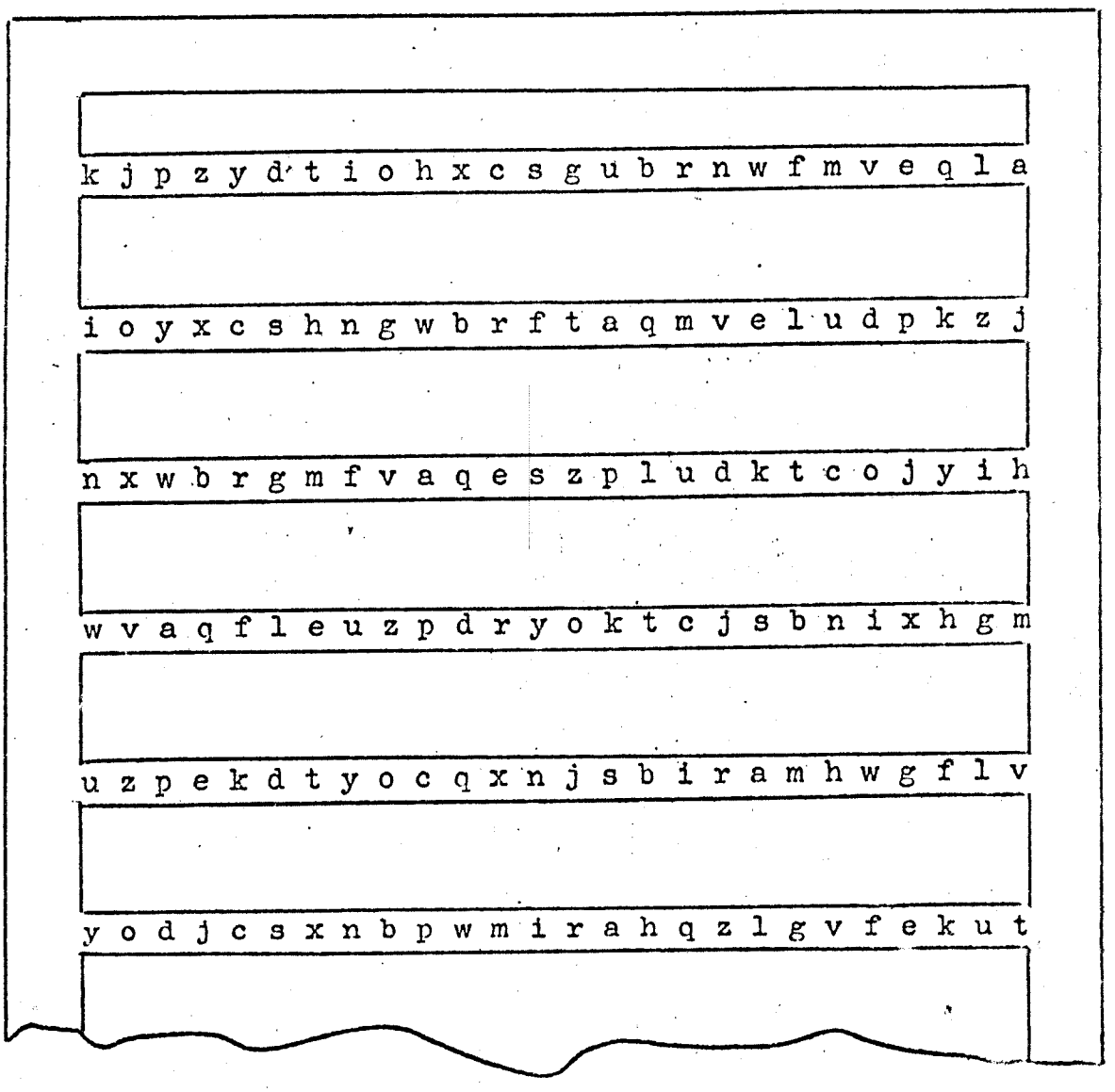
$$P^{25}CP^{-25} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & l & k & q & a & z & e & u & j & p & i & y & d & t & h & v & c & s & o & x & g & n & w & f & r & m \end{pmatrix}$$

i przekształcać przy pomocy tych wyrażeń kolejno A_1, A_2 i A_3, aż

w pewnym momencie niektóre transpozycje się powtórzą. Jeżeli dla przykładu jako A_1, A_2, A_3 weźmiemy permutacje podane na str.48., wówczas nastąpi to już przy drugiej próbie. Jest mianowicie:

$$PC^{-1}P^{-1}A_1PCP^{-1} = (aw)(br)(cd)(ei)(fz)(ql)(uj)(xg)(sn)(ht)(ov)(mk)(yp)$$
$$P^2C^{-1}P^{-2}A_2P^2CP^{-2} = (ni)(ax)(wt)(bq)(rv)(gz)(my)(fz)(sl)(pj)(ud)(ck)(oh)$$
$$P^3C^{-1}P^{-3}A_3P^3CP^{-3} = (wh)(vr)(ay)(qe)(fz)(lk)(ui)(pn)(dj)(ot)(cs)(bm)(xg)$$

Widzimy, że powtarzają się transpozycje $(fz), (xg), (rv)$. W praktyce szukanie powtarzających się transpozycji odbywało się nieco inaczej. Z podanych na stronie poprzedniej permutacji C przekształconych przy pomocy kolejnych potęg permutacji P^{-1} wypisano raz na zawsze na podłużnej tekturze z otworami /stąd nazwa metody "siatki"/ tylko dolne wiersze:



Pod siatkę podkładano ćwierć arkusza papieru kratkowanego z wypisanymi permutacjami A_1, A_2, A_3 itd. w postaci niecyklicznej z tym, że między górnym a dolnym wierszem każdej permutacji pozostawiano odpowiedni odstęp.

a b c d e f g h i j k l m n o p q r s t u v w x y z

A_1 s r w i v h n f d o l k y g j t x b a p z e c q m u

---

a b c d e f g h i j k l m n o p q r s t u v w x y z

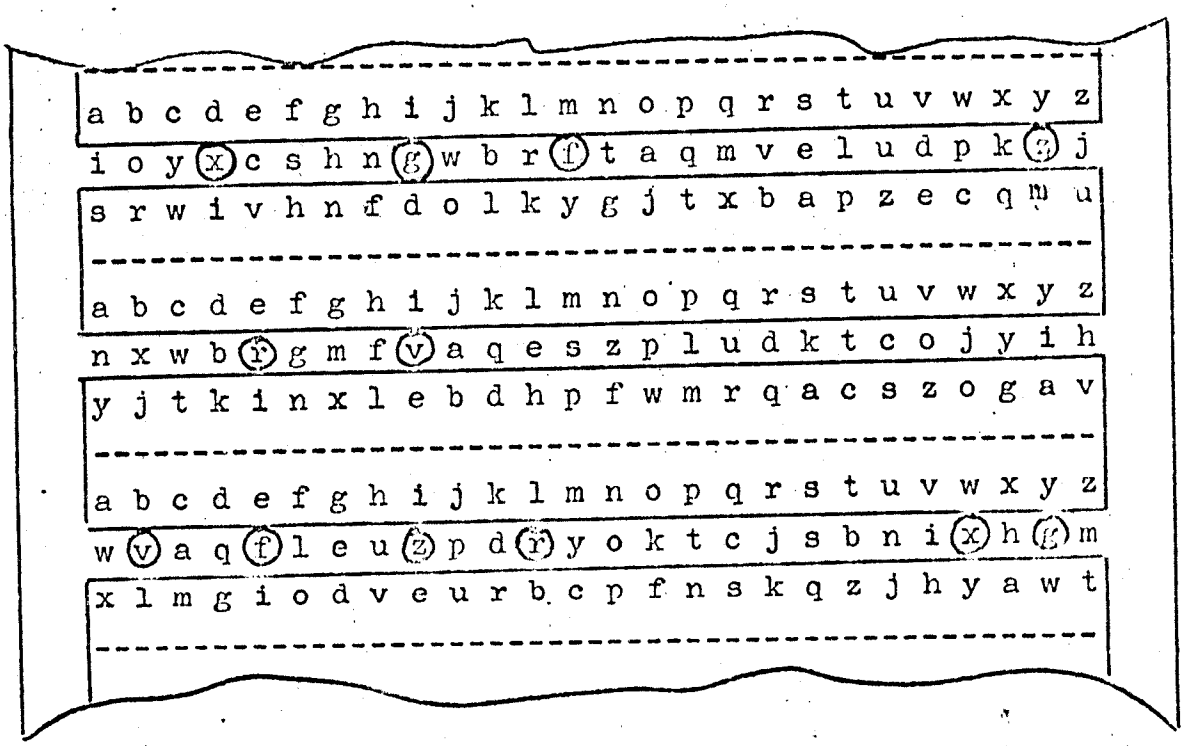
A_2 y j t k i n x l e b d h p f w m r q a c s z o g a v

---

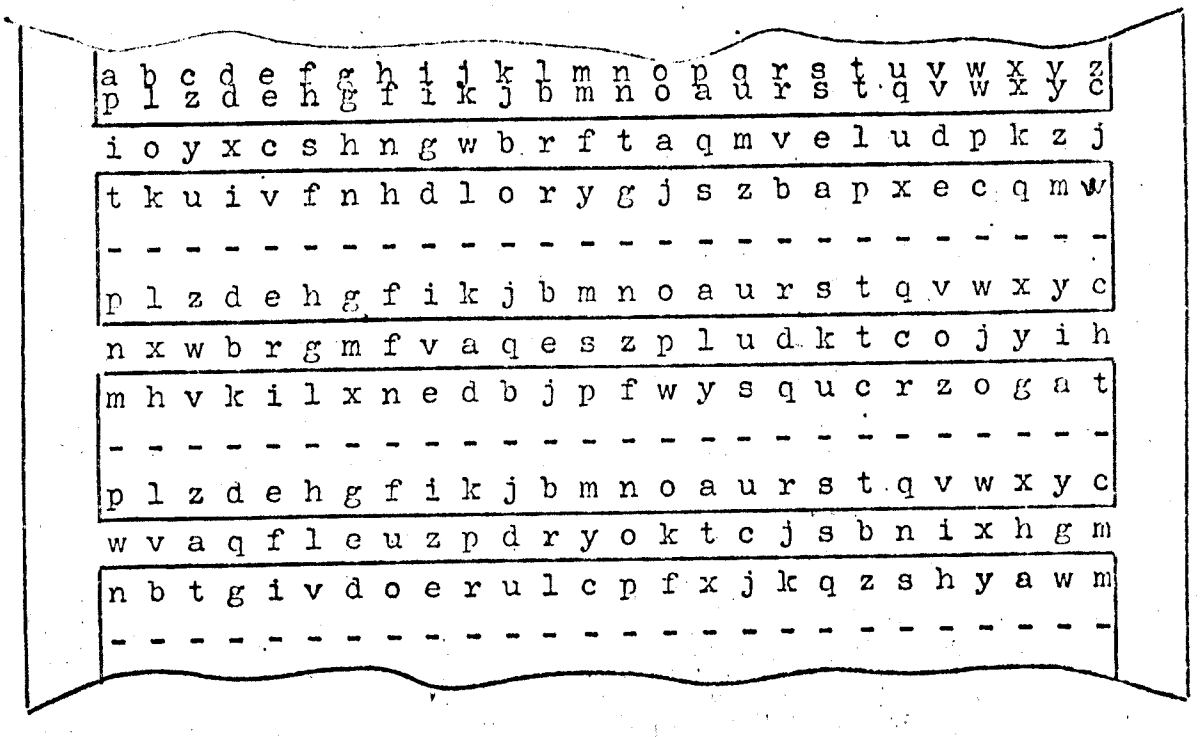
a b c d e f g h i j k l m n o p q r s t u v w x y z

A_3 x l m g i o d v e u r b c p f n s k q z j h y a w t

Przesuwając siatką nad ową ćwiartką papieru jednocześnie w myślach sprawdzano, jakie transpozycje powstawały między górnym i dolnym wierszem permutacji A_1, A_2, A_3 i jeżeli w pewnej pozycji siatki natrafiano na transpozycje powtarzające się, to na tej pozycji się zatrzymywano.



Zakładamy, że powtarzające się transpozycje $(fz), (xg), (rv)$ są to transpozycje, które nie uległy przekształceniu przez permutację S i, które zatem są transpozycjami należącymi do permutacji U. Ostatnia faza naszego zadania polega na tym, aby w oparciu o wspomniane trzy transpozycje tak poprzestawiać jednocześnie górne i dolne litery w każdej z trzech permutacji A_1, A_2, A_3, aby wszystkie transpozycje powstające pomiędzy górnymi i dolnymi wierszami permutacji A_1, A_2, A_3 były te same. Przy odpowiedniej rutynie udaje się to zazwyczaj po kilku próbach. W naszym przypadku końcowy obraz powinien wyglądać następująco:



Transpozycje, które utworzyły się między górnymi i dolnymi wierszami permutacji A_1, A_2, A_3 są teraz istotnie we wszystkich trzech przypadkach takie same:

$(ab), (cd), (eq), (fz), (gx), (ht), (il), (jp), (ku), (my), (ns), (ow), (rv)$

a w permutacjach A_1, A_2, A_3 uległy przestawieniu następujące pary liter:

$$(ap), (bl), (cz), (fh), (jk), (qu)$$

które są zatem szukanymi połączeniami wtyczkowymi S.

Stosując metodę"siatki" znaleźliśmy jednocześnie z połączeniami wtyczkowymi również położenie prawego bębenka szyfrującego, gdyż jego pozycja odpowiada pozycji siatki, przy której wystąpiły powtórzenia się transpozycji. Dla znalezienia pozycji pozostałych dwóch bębenków szyfrujących trzeba dokonać 26·26 = 676 prób polegających na tym, że bierze się początek, to jest sześć pierwszych liter dowolnej depeszy i wystukuje się je na maszynie "Enigma" przy wszystkich możliwych pozycjach lewego i środkowego bębenka, aż w pewnej pozycji wystuka się dwa razy tę samą trójkę liter /którą zresztą znamy dzięki metodzie odtwarzania kluczy depesz/.

Opisując metodę"siatki" zakładaliśmy, że w obrębie trzech pierwszych uderzeń klawiszy nie nastąpi przesunięcie bębenka środkowego. Czy to przesunięcie nastąpi przy dalszych uderzeniach klawisza, to można oczywiście łatwo sprawdzić. Ale jeżeli takie uderzenia nastąpi, wówczas przesunięcie to dodatkowo nas informuje, jakie jest nastawienie pierścienia prawego bębenka, gdyż przesunięcie bębenka środkowego uzależnione jest od wcięcia umiejscowionego na pierścieniu bębenka prawego. Nastawienie pierścieni pozostałych dwóch bębenków znajduje się znów drogą prób, czego już nie będziemy szczegółowo opisywać. W każdym razie przy pomocy metody "siatki" można znaleźć nie tylko połączenia wtyczkowe, lecz od czasu do czasu również nastawienie pierścieni i to od razu na okres całego miesiąca, gdyż w takich odstępach czasu zmieniano początkowo nastawienie pierścieni.

Siatek należało naturalnie sporządzić tyle, ile było bębenków szyfrujących, to jest początkowo trzy, a później pięć. Metodę "siatki" można było stosować również wtedy, gdy kolejność bębenków była nieznaną. Należało w takim wypadku "przymierzać" po kolei wszystkie siatki, co wymagało wprawdzie więcej czasu i więcej pracy, ale co jednak mieściło się w granicach wykonalności.

VIII.

Skoro prócz wewnętrznych połączeń bębenków szyfrujących mieliśmy też sposoby na odtwarzanie wszystkich składników klucza obowiązującego w danym dniu, nic już nie stało na przeszkodzie w bieżącym odczytywaniu całego obfitego materiału szyfrowego, nadawanego przez niemieckie wojsko. Przez krótki okres czasu, na przełomie lat 1932 i 1933, czyniłem to sam wraz ze swymi dwoma kolegami, których mi w międzyczasie przydzielono do pomocy, ale wkrótce już uruchomiono do tego celu biuro z pięcioma czy sześcioma pracownikami, których wyłącznym zadaniem było odczytywanie wszystkich niemieckich depesz przy pomocy klucza przez nas codziennie dostarczanego. Potrzebne maszyny "Enigma" wyprodukowała firma AVA w liczbie kilkudziesięciu sztuk. Tak wielka liczba maszyn była potrzebna zarówno ze względu na ich stosunkowo krótki żywot spowodowany intensywną eksploatacją, jak i z uwagi na przewidziany w wypadku wojny znaczny wzrost liczby pracowników odczytujących depesze. Na kilka lat przed wojną, prawdopodobnie w roku 1937, przeniesiono całą naszą komórkę z gmachu Sztabu Głównego przy Placu Saskim do nowo wybudowanego pomieszczenia w lesie pyrskim. W tym też okresie lub może nieco później odkomenderowano do naszego pokoju czterech oficerów /rtm.Żukotyński, kpt. Tuszyński, kpt. Hillebrandt, kpt. Czwartacki/ dla zapoznania się z naszymi metodami pracy.

O treści odczytanych depesz niewiele mogę powiedzieć, gdyż, jak już przed chwilą wspomniałem, poza okresem początkowym i wypadkami sporadycznymi, ich odczytywaniem nie zajmowałem się ani ja ani moi dwaj koledzy. W każdym razie nie były to depesze ćwiczebne. Z okresu puczu Roehma pamiętam depeszę rozpoczynającą się od słów: An alle Flughäfen Deutschlands, i kończących się na słowach: .....führer Roehm tot oder lebendig zur Stelle bringen.

Nie tylko zresztą wojsko lądowe używało szyfru maszynowego. Również marynarka wojenna przeszła na system Enigma z tym, że z samego początku zamiast 3 bębenków używała 5 bębenków szyfrujących. Z odczytanych treści depesz dowiedzieliśmy się, że marynarka wojenna posługiwała się trzema rodzajami kluczy: Marineschlüssel, Stabsschlüssel i Admiralsschlüssel. Ale o ile pamiętam, mogliśmy z braku materiału odczytywać na ogół tylko depesze zaszyfrwane kluczem Marineschlüssel i jedynie wyjątkowo też depesze zaszyfrowane przy pomocy Stabsschlüssel.

Również formacje hitlerowskiego Sicherheitsdienst posługiwały się maszyną Enigma, lecz czyniły to w sposób wyjątkowo wyrafinowany, gdyż niezależnie od tego, że klucze były i tak inne od kluczy wojska i marynarki, to jeszcze pierwotną treść depeszy wpierw zaszyfrowywano przy pomocy kodu i dopiero tak spreparowaną depeszę powierzano szyfrantowi dla wtórnego zaszyfrowania maszyną Enigma. Ale jeżeli o nas chodzi, na nic to się nie zdało: rozwiązaliśmy i kod i klucze maszyny. Z odczytanych depesz pamiętam jedną, w której wspomina się, że niektórzy francuscy ministrowie prawdopodobnie nie byliby nieczuli na dźwięk pieniądza i ewentualnie zgodziliby się na współpracę z SD. Imiennie wymieniano niejakiego ministra Marchandeau.

Przez bardzo krótki okres czasu pojawił się inny rodzaj szyfru maszynowego. Z odczytanych w tym okresie depesz zaszyfrowanych zwykłą maszyną Enigma wynikało, że nowy szyfr był to szyfr maszynowy oparty wprawdzie na zasadzie podobnej co maszyna Enigma, lecz że zastosowana maszyna była maszyną samopiszącą, zwaną "E zwo". Miała osiem bębenków do szyfrowania i używana była na szczeblu Wehrkreiskommando. Wycofano ją wnet z obiegu, gdyż zbyt często się psuła. Zapewne i ją [illegible]oby się rozwiązać, gdyby była dłużej w użyciu i gdyby więcej [illegible] materiału szyfrowego. W każdym razie mieliśmy i t[illegible] intere[illegible]e wyniki.

Wprowadzane przez stronę niemiecką częste zmiany w sposobie posługiwania się szyfrem maszynowym zmuszały stronę polską do szukania coraz to innych dróg dla przezwyciężenia powstających trudności. Zwłaszcza przejście od nastawiania pierścieni raz na miesiąc do codziennego nastawiania pierścieni okazało się bardzo skutecznym utrudnieniem naszej pracy. Zadanie polegało przecież nie tyle na rozwiązywaniu, ile na szybkim rozwiązywaniu niemieckich szyfrów wojkowych. Dlatego też dążyliśmy do maksymalnego, jak na owe czasy, zmechanizowania wykonywanych przez nas czynności. W tym właśnie celu zaprojektowaliśmy, a firma AVA zbudowała, maszynę stanowiącą agregat sześciu maszyn "Enigma". Dziś już nie pamiętam ani szczegółów konstrukcyjnych agregatu ani dokładnego jego działania, ale w każdym razie zbudowany był w ten sposób, że bębenki szyfrujące sześciu maszyn, z których agregat się składał, obracały się samoczynnie pod napędem elektrycznym, przybierając w ciągu około dwóch godzin kolejno wszystkie możliwe 17576 pozycji bębenków. Gdy bębenki znalazły się w pozycji mogącej stanowić szukane rozwiązanie, zapalało się światełko, a jednocześnie motor automatycznie się zatrzymywał. Takich agregatów, nazwanych przez nas "bombami" zbudowano sześć sztuk, odpowiednio do sześć różnych kolejności, jakie trzy bębenki szyfrujące mogą przyjmować. W ten sposób, puszczając jednocześnie w ruch wszystkie "bomby", najdalej po dwóch godzinach powinno się otrzymać wynik. Cena owych sześciu bomb wynosiła podobno około 100.000 złotych przedwojennych /wobec wybuchu wojny nie zapłaconych/. Wprowadzenie przez Niemców czwartego, a potem piątego bębenka szyfrującego w znacznym stopniu ograniczyło przydatność "bomb".

Jeszcze mniej niż metoda "bomb" utkwiła w mej pamięci inna metoda, chociaż włożyliśmy w nią bardzo dużo pracy. [illegible], nazwana przez nas metodą "płacht", polegała na nakładaniu na siebie w specjalny sposób dużych arkuszy papieru, z których w każdym było

około 1000 dziurek rozmieszczonych w specjalny sposób. Rozwiązanię otrzymywano, gdy w końcu poprzez dziesięć czy jedenaście płacht tylko jedna dziurka przeświecała. Płacht takich potrzebowaliśmy sześć kompletów po 26 sztuk każdy. Fabrykacja płacht odbywała się w niesłychanie prymitywny sposób. Braliśmy arkusze papieru milimetrowego wielkości około 60 cm x 60 cm i z braku odpowiedniego perforatora wycinaliśmy w nich mozolnie przy pomocy ostrzy do golenia kwadratowe dziurki wielkości 5 mm x 5 mm. Wybuch wojny przeszkodził w całkowitym wykończeniu wszystkich kompletów. Ale jakie było prawidło robienia tych dziurek, jakie było prawidło nakładania poszczególnych płacht i do czego one służyły, tego nie mogę już sobie w żaden sposób więcej przypomnieć.

W wyniku sojuszu zawartego z Wielką Brytanią i Francją doszło do współpracy Sztabów Głównych i II Oddziałów. Nie ulega wątpliwości, że angielski i francuski II Oddział otrzymywały od polskiego II Oddziału odczytane niemieckie depesze nie w stanie surowym, lecz jedynie ich istotną treść w postaci jakichś biuletynów informacyjnych opracowanych przez specjalistów. Tym niemniej sama już ogromna ilość materiału dostarczanego w tej formie musiała zdradzić Brytyjczykom i Francuzom, że posiedliśmy tajemnicę szyfru "Enigma". Toteż proponowali współpracę również w dziedzinie szyfrów. Strona polska podobno początkowo odpowiedziała odmownie. Gdy jednak stosunki polsko-niemieckie zaczęły się coraz bardziej zaostrzać, strona polska ustąpiła i na wiosnę 1939 roku doszło do spotkania wszystkich trzech stron w gmachu naszej placówki w lesie pyrskim. Ze strony brytyjskiej przybył niejaki komandor Knox i jeszcze jedna osoba, której nazwiska już nie pamiętam, a ze strony francuskiej mjr. Bertrand i kpt. Bracquenier. Bardzo pojętni okazali się zwłaszcza Brytyjczycy. Szybko zorientowali się, jak znaleźliśmy wewnętrzne połączenia bębenków i szybko też pojęli, jak działają nasze "płachty" i "bomby". Powiedzieli, że brytyjskie Biuro Szyfrów natychmiast

przystąpi do sporządzenia takich samych "płacht" i takich samych "bomb". Przekonaliśmy się wkrótce, że słowa dotrzymali. Na zakończenie spotkania każda z delegacji otrzymała od nas w prezencie po jednej maszynie "Enigma".

Po tym spotkaniu normalna praca trwała jeszcze około pół roku aż do chwili wybuchu wojny.

IX.

Ogłoszono powszechną mobilizację, ale wskutek wyreklamowania mych dwóch kolegów i mnie przez II Oddział pozostaliśmy nadal pracownikami cywilnymi. Praca w Biurze Szyfrów miała się odtąd odbywać dniem i nocą bez przerwy na trzy zmiany. W rzeczywistości było tak tylko przez jeden czy dwa pierwsze dni. Potem, wobec szybkiego posuwania się wojska niemieckiego, zaczęto niszczyć część akt i przygotowywać się do ewakuacji. Już w dniu 6. września 1939 roku znaleźliśmy się wraz ze sprzętem i resztą akt w pociągu, t.zw. eszelonie "F" w drodze do Brześcia nad Bugiem. Gdy tam po kilku dniach jazdy przybyliśmy, zostaliśmy odkomenderowani do Kwatery Głównej, wobec czego opuściliśmy pociąg ewakuacyjny i dalszą drogę odbyliśmy samochodami. Poszczególne etapy tej drogi są znane: Łuck, Dubno, Krzemieniec i wreszcie pod Kutami przez most nad Dniestrem do Rumunii. Po drodze stopniowo niszczono sprzęt i resztę akt. Władze rumuńskie oddzieliły osoby cywilne od wojskowych, wyznaczając im inny kierunek drogi. W ten sposób straciliśmy kontakt z naszymi przełożonymi. Samochód nasz zarekwirowano, a nam polecono udać się do obozu znajdującego się w pobliżu dworca kolejowego miejscowości, której nazwy już nie pamiętam. Ostatniego polecenia władz rumuńskich nie wykonaliśmy jednak, lecz poszliśmy na dworzec i pierwszym pociągiem pojechaliśmy do Bukaresztu. Tu zameldowaliśmy się u płk. Żakrzewskiego, attaché wojskowego naszej ambasady i po przedstawieniu mu faktu na-

szej współpracy z brytyjskim i francuskim Biurem Szyfrów uzyskaliśmy zgodę na skontaktowanie się z ambasadą brytyjską lub francuską dla możliwie jak najszybszego kontynuowania naszej działalności kryptologicznej.

Do ambasady brytyjskiej przybyliśmy raczej w nie najodpowiedniejszym momencie, gdy na dziedziniec ambasady właśnie wjeżdżał autokar z personelem ambasady brytyjskiej z Warszawy. Ambasador brytyjski w Bukareszcie też był na dziedzińcu, ze zrozumiałych względów dość zaaferowany, a gdy mu przedstawiłem cel naszego przybycia, oświadczył, że przed podjęciem jakichkolwiek kroków musi wpierw zwrócić się do Londynu. Ponieważ liczyliśmy się z możliwością, że w nawale spraw wogóle o nas zapomni i ponieważ nie chcieliśmy przedłużać naszego pobytu w Bukareszcie, udaliśmy się jeszcze na wszelki wypadek do ambasady francuskiej, gdzie - widocznie uprzedzeni o możliwości naszego zgłoszenia się - w błyskawicznym tempie postarali się dla nas o paszporty z wszelkimi wizami i o bilety kolejowe, tak że już około 25. września znaleźliśmy się w Paryżu. Później cała sprawa wywołała jeszcze mały konflikt dyplomatyczny, gdyż władze wojskowe brytyjskie, powołując się na nasze zgłoszenie się w ambasadzie w Bukareszcie, domagały się od władz francuskich naszego wydania, na co się jednak nie zgodzono.

Wznowienie naszej pracy nieprędko jednak nastąpiło. Kierownik francuskiego Biura Szyfrów, mjr Bertrand, nasz obecny gospodarz, rozpoczął starania, aby w obozach w Rumunii szukano naszych przełożonych, ppłka Langera i mjra Ciężkiego i aby ich po odnalezieniu z tych obozów wyciągnięto. Trwało to dość długo i dopiero po szeregu tygodni nasi przełożeni przybyli do Paryża. Potem całą naszą grupę, do której przyłączyło się jeszcze parę osób z innych komórek naszego Biura Szyfrów, tak że razem było nas już kilkanaście osób, ulokowano w małym zameczku odległym o 1 km od miasteczka Graetz [illegible] daleko Paryża. Zamek nazywał się Vignolles.

Różne prace organizacyjne zabrały dalszych parę tygodni. W międzyczasie francuskie Biuro Szyfrów, w oparciu o dostarczony im przed wojną pierwowzór, zbudowało kilka sztuk maszyn "Enigma", a na podstawie rysunków technicznych, wykonanych przez pracownika "AVA"-y, który też znalazł się w naszej grupie, zrekonstruowało nasz cyklometr, zaś Anglicy nadesłali nam komplet "płacht", pięknie wykonanych na arkuszach specjalnie na ten cel wydrukowanych, nieco mniejszego formatu niż nasze i przez to wygodniejsze .. manipulowaniu. "Bomb" nam nie przysłali, to jest zrozumiałe, ale kpt. Bracquenier, nasz znajomy z czasów spotkania w Pyrach, a obecnie nasz stały współpracownik, oświadczył, że w czasie pobytu w Londynie, jeszcze przed naszym przyjazdem do Francji, "bomby" te oglądał. Opisywał też, jak w Londynie dziesięć czy dwanaście Angielek przy pomocy odpowiednich urządzeń perforowało owe "płachty", które my w swoim czasie mozolnie ręcznie przy pomocy "żyletek" dziurkowaliśmy. Tak więc spotkanie w lesie pyrskim przyniosło ten rezultat, że nasz wieloletni wkład pracy nie przepadł całkowicie, lecz że mogliśmy dalej, chociaż na obczyźnie, zwalczać wroga bronią, jaką dysponowaliśmy. Jeżeli broni tej nie umiano, być może, w całej pełni wykorzystać, to już nie nasza w tym była wina.

Praca nasza, gdy wreszcie się zaczęła, była bardzo gorączkowa. Pracowaliśmy na zmianę dniem i nocą, zwłaszcza jednak nocą. Telegrafiści francuscy przekazywali nam niemieckie depesze za pośrednictwem dalekopisu natychmiast, bieżąco tak jak je odbierali. Zmiana kluczy następowała o północy, a nas najwięcej właśnie interesowały pierwsze depesze nadane po zmianie klucza. Zauważono bowiem, że niektórzy niemieccy szyfranci, po dokonaniu zmian klucza i po zamknięciu metalowego wieka maszyny wybierali sobie jako klucz depeszy /Spruchschlüssel/ te litery, które były widoczne w okienkach wieka. Nie zauważali, naiwni, że litery te, jeżeli nie poruszyli ..enków szyfrujących, były równe lub w przybliżeniu ró.. nau..

wieniu pierścieni /bo chcąc nastawić pierścienie na daną literę, trzeba tak obrócić bębenki, aby żądana litera znalazła się na wierzchu, a więc pod okienkiem lub niedaleko okie[illegible] W[illegible]en sposób byliśmy najczęściej już w niewiele minut po północy w posiadaniu kluczy i mogliśmy resztę depesz danego dnia czytać tak samo szybko jak niemieccy adresaci depesz. Lojalność każe przyznać, że spostrzeżenie o pierwszych kluczach po północy zawdzięczaliśmy Anglikom.

Jeszcze jedno zresztą spostrzeżenie zawdzięczaliśmy Anglikom, którego ze względu na niewystarczający materiał i na nawał pracy sami nie mogliśmy dokonać, ale które jako interesujące z punktu widzenia kryptologicznego pragnę tu przedstawić. W opisywanym okresie, to jest na początku 1940 roku pojawił się nowy szyfr, na który nie zwracaliśmy specjalnej uwagi, gdyż byliśmy całkowicie zaabsorbowani rozwiązywaniem szyfru maszynowego. Zresztą otrzymywaliśmy zaledwie kilka depesz dziennie w tym szyfrze. Był to jakiś niewielki kod, dokładnie już nie pamiętam, czy dwu- czy może trzyliterowy, który najwidoczniej służył do przekazywania krótkich meldunków meteorologicznych między samolotami a ziemią. Litery wchodzące w skład kodu były codziennie zmieniane, tak jak gdyby kod poddawano wtórnemu zaszyfrowaniu. Otóż Anglicy, którzy zapewne więcej otrzymywali materiału szyfrowego i bez porównania więcej mieli ludzi do pracy, spostrzegli, że Niemcy dla dokonywania wtórnego zaszyfrowania kodu posługiwali się zmienianymi codziennie połączeniami wtyczkowymi maszyny "Enigma", czyli że codziennie zmieniali litery w kodzie w sposób wskazany przez połączenia wtyczkowe. Był to kardynalny błąd ze strony niemieckiej, gdyż w ten sposób nie trzeba nawet rozwiązać kod, by bez trudu odnaleźć codziennie połączenia wtyczkowe. Wystarczy przypomnieć, że połączenia wtyczkowe zamieniały tylko część liter, i to w ten sposób, że jeżeli literę a zamieniano na b, to jednocześnie literę b zamieniano na a.

W ramach współpracy z Anglikami odbywało się naturalnie też regularne wzajemne zawiadamianie /przy pomocy dalekopisu poprzez Kanał/ o obowiązujących w danym dniu kluczach maszynowych i kto był wcześniej w posiadaniu klucza na dany dzień, ten natychmiast informował o tym drugą stronę. Dzięki temu w czasie całej kampanii norweskiej nie było bodaj depeszy przez Anglików lub przez nas nie odczytanej i to z tak rekordową szybkością, że zawsze pozostało wystarczająco czasu /tylko nie zawsze były środki/ na podjęcie wszelkiej wskazanej kontrakcji. W pamięć wbiła mi się szczególnie jedna depesza, która nie dotyczyła wprawdzie okresu kampanii norweskiej, lecz okresu nieco wcześniejszego i która odsłoniła całą bezsilność aliantów wobec niemieckich ataków powietrznych. Wspomniana depesza podawała dokładne szczegóły tak zwanego "Unternehmen Paula" czyli planu bombardowania zakładów samochodowych Renaulta w Paryżu. Depesza podawała, ile bombowców i ile myśliwców weźmie udział w tej akcji, wzdłuż jakiej trasy, na jakiej wysokości, którego dnia i o której godzinie polecą. Termin akcji wyznaczony był na około osiem dni naprzód. Przekazaliśmy oczywiście treść depeszy /jak zresztą treść każdej depeszy przez nas odczytanej/ natychmiast naszym francuskim gospodarzom, ale o żadnej kontrakcji nie usłyszeliśmy. Obserwowaliśmy natomiast - ponieważ trasa przelotu biegła nad naszym zamkiem - jak w oznaczonym dniu i o oznaczonej godzinie samoloty w zwartym szyku przelatywały nad naszymi głowami w kierunku Paryża.

Gdy rozpoczął się niemiecki atak na Francję, przeniesiono nas na pewien okres czasu z Graetzu do samego Paryża na ul. 2 bis Tourville, gdzie mieścił się francuski II Oddział i gdzie dniem i nocą jeszcze bardziej gorączkowo niż przedtem, pracowaliśmy. Odczytywane depesze przepisywano natychmiast w 5 czy 6 egzemplarzach na maszynie na papierze przebitkowym żółtego koloru i owe "feuillets jaunes" były wprost rozchwytywane przez wyższych oficerów francuskich

którzy czatowali na nie pod drzwiami naszego pokoju, a niektórzy z nich nawet nocowali w gmachu, byleby jak najszybciej wejść w posiadanie tych żółtych kartek. Klęski Francji to nie odwróciło.

Wobec posuwania się wojsk niemieckich musieliśmy wkrótce pracę naszą przerwać, nas zaś umieszczono w zarekwirowanym autobusie paryskim, który, podobnie jak w czasie kampanii wrześniowej w Polsce, wiózł nas etapami coraz bardziej na południe, naprzód do La Ferté, potem do Bon Encontre i wreszcie do Tuluzy. Stąd, po zawieszeniu broni, nastąpił odlot dwoma samolotami przez Morze Śródziemne do Afryki Północnej, naprzód do Oranu, a potem do Algieru, gdzie pozostaliśmy około trzech miesięcy.

X.

Pobyt nasz w Algierze miał charakter przejściowy. Mieliśmy tam pozostać tak długo, aż znane będą warunki zawieszenia broni i życie we Francji powróci do pewnej normy. Liczono się bowiem z możliwością, że Niemcy w warunkach zawieszenia broni zażądają naszego wydania. Pracować w tym czasie nie mogliśmy, ponieważ podsłuch radiowy nie był jeszcze zorganizowany. Tak minęło kilka miesięcy. Wreszcie uznano, że sytuacja we Francji na tyle się ustabilizowała, że pobyt nasz w strefie nieokupowanej stał się możliwy, wobec czego w pierwszych dniach października 1940 roku przewieziono nas statkiem pod przybranymi nazwiskami jako Francuzów z Algieru do Marsylii. Ja na przykład otrzymałem dowód osobisty na nazwisko Pierre Raneau, professeur au lycée de Nantes, i tym dowodem osobistym legitymowałem się do końca roku 1942, to jest do chwili opuszczenia Francji.

Po kilku dniach pobytu w Marsylii umieszczono nas w zameczku Les Fouzes odległym o 1 km od miasteczka Uzès niedaleko Nîmes. Praca nasza miała teraz charakter konspiracyjny. Jednym z pierwszych zadań, jakie nasz szef, ppułk. Langer, sobie postawił, było na-

zanie łączności z Oddziałem II Sztabu Naczelnego Wodza, znajdującego się obecnie w Londynie. Potrzebny sprzęt nadawczo-odbiorczy dostarczyli Francuzi, kilka osób naszej grupy wyszkolono na radiotelegrafistów, a do utajnienia przekazywanych wiadomości służyła maszyna do szyfrowania polskiej konstrukcji typu LCP /Langer, Ciężki, Palluth/, której dwa egzemplarze zachowano przed zniszczeniem w czasie ucieczki do Rumunii we wrześniu 1939 roku. Grupa nasza, po nawiązaniu łączności otrzymała kryptonim "grupa 300". Sprzęt na zamku Les Fouzes przechowywano w taki sposób, by go móc szybko i bezpiecznie ukryć w wypadku niepożądanej wizyty. Niebezpieczeństwo dekonspiracji było, jak się wkrótce okaże, bardzo poważne.

Przede wszystkim jednak należy odnotować niezwykle tragiczny wypadek, który się zdarzył, jeżeli mnie pamięć nie myli, w pierwszej połowie 1941 roku. Z powodów, które nie są mi znane, Francuzi postanowili utworzyć w Algierze ekspozyturę naszej komórki i w tym celu kilka osób naszej grupy pojechało tam statkiem na kilka miesięcy. Gdy wracali, Lamoricière - tak się nazywał ich statek - dostał się w burzę, uległ katastrofie i w pobliżu wysp Balearów zatonął. Większość pasażerów straciła życie, w tym trzech Polaków naszej grupy : kpt. Graliński, którego wymieniałem na początku /str. 14./ niniejszych wspomnień, mój najbliższy kolega i współpracownik Jerzy Różycki i jeszcze jeden pracownik nazwiskiem Smoleński. Zginął też ich opiekun na statku, oficer francuski, którego nazwiska nie pamiętam.

Zadanie nasze polegało oczywiście w dalszym ciągu na rozwiązywaniu niemieckich szyfrów i szyfry te rozwiązywaliśmy. Ale okres spędzony na południu Francji nie utrwalił się zbyt dobrze w mej pamięci. W każdym razie nie jestem pewien kolejności naszych dalszych zajęć kryptologicznych. Nie pamiętam też, czy zajmowaliśmy się jeszcze szyfrem "Enigma". Przypuszczam jednak, że mieliśmy za mało materiału szyfrowego i że musieliśmy zaniechać zajmowania się tym

~~szyfrem. Był nawet taki okres, kiedy wogóle nie mieliśmy żadnego niemieckiego materiału szyfrowego.~~" Prawdopodobnie Francuzi, po klęsce swego kraju, musieli dopiero zorganizować konspiracyjny podsłuch radiowy. Tymczasem dostarczyli nam dwa rodzaje szyfrogramów szwajcarskich. Jeden rodzaj był to jakiś kod handlowy, który bez trudu rozwiązaliśmy. W depeszach była mowa o różnych transakcjach zawieranych między Szwajcarią a krajami Bliskiego Wschodu. Dla Francuzów informacje te mogły być interesujące.."

"Drugim rodzajem szyfru był szwajcarski maszynowy szyfr wojskowy. Pobieżna analiza wykazała, że w przeciwieństwie do szyfru maszynowego niemieckiego, gdzie każda depesza miała swój własny klucz, w szyfrze szwajcarskim wszystkie depesze z jednego dnia miały ten sam klucz, czyli że rozpoczynano szyfrowanie wszystkich depesz z tej samej pozycji wyjściowej. Umożliwiało to nam odczytywanie depesz bez znajomości maszyny, w oparciu o same tylko cechy językowe, mniej więcej na tej samej zasadzie, według której rozwiązuje się zwykłe literówki, z tą jednak różnicą, że tutaj wszystkie pierwsze litery depesz stanowiły jedną literówkę, wszystkie drugie litery depesz drugą literówkę o odmiennym kluczu, itd." Cechy językowe były zresztą częściowo zatarte. Po odczytaniu depesz z jednego dnia wyszło na jaw, dlaczego tak jest. Okazało się mianowicie, że tylko część pierwotnych tekstów depesz była w języku niemieckim, inne były w języku francuskim i jeszcze inne w języku włoskim. Stanowiło to pewne utrudnienie w odczytywaniu depesz." Jednocześnie jednak, już w czasie prób odczytywania pierwszych depesz, ujawniła się pewna cecha maszyny, która trochę ułatwiała odtwarzanie kluczy (...) ~~poszczególnych literówek~~. Była to ta sama cecha, którą posiadała również ~~maszyna~~ "Enigma" i która polegała na tym, że jeżeli uderzenie klawisza X dawało literę Y, to i nawzajem uderzenie klawisza Y dawało literę X. Jednym słowem, było to tzw. prawo wzajemności ~~ze str. 23~~. Dzięki tej cesze, każda hipoteza, którą w czasie prób znalezie-

nia poszczególnych literówek robiliśmy, ustalała od razu dwie litery. Fakt, iż maszyna szwajcarska miała podobne własności co maszyna niemiecka, nasuwał przypuszczenie, że jest oparta na takich samych lub podobnych zasadach co tamta. Dlatego też próbując ją rozwiązać zastosowaliśmy te same metody, jakie użyliśmy dla rozwiązania maszyny "Enigma". Rolę początków depesz odegrały teraz pierwsze litery szyfrogramów, zaś permutacjom A_1, A_2, A_3.... odpowiadały teraz literówki otrzymane w wyniku odczytania początkowych fragmentów kleru. Ponieważ wykazaliśmy w swoim czasie /str. 47./, że dla znalezienia wewnętrznych połączeń ostatniego bębenka szyfrującego wystarczą cztery równania A_1, A_2, A_3, A_4, więc w obecnym wypadku dla znalezienia tych połączeń też byłyby potrzebne cztery kolejne literówki. Okazało się, że obrana droga istotnie prowadziła do celu i że w ten sposób rozprawiliśmy się również ze szwajcarską maszyną do szyfrowania. Nie będę podawać szczegółowej drogi rozwiązania na konkretnym przykładzie, gdyż byłoby to niemal dosłownym powtórzeniem tego, co już przedstawiliśmy na str. 41, - 50. Jedyna różnica polegałaby na tym, że permutacja S /połączenia wtyczkowe/ zostałaby obecnie wyeliminowaną z naszych rozważań. Szwajcarska maszyna okazała się bowiem zwykłą maszyną do szyfrowania "Enigma" typu handlowego, naturalnie z innymi połączeniami wewnętrznymi bębenków, które trzeba było sukcesywnie odtwarzać. Nie było też kłopotów ze zmiennym nastawianiem pierścieni, gdyż w maszynach "Enigma" typu handlowego pierścieni nastawialnych nie ma. Tym niemniej, dla znalezienia pozycji ostatniego bębenka, nie mieliśmy innej metody jak codzienne odnajdywanie metodą literówkową początkowych fragmentów treści depesz. Pozycję pozostałych bębenków uzyskiwano drogą prób. Szwajcarzy zostali, o ile mi wiadomo, poinformowani przez Francuzów o wadach niemieckiej maszyny "Enigma" typu handlowego i o niebezpieczeństwie, że ich depesze mogą być czytane również przez Niemców.

Przed opuszczeniem dziedziny szyfrów nieniemieckich nie chcę pominąć całkowitym milczeniem pewnego epizodu z mej działalności kryptologicznej, który nie przyniósł mi żadnego uznania z niczyjej strony. Z zasady nie interesowałem się polskimi systemami szyfrowymi i nigdy nie próbowałem ich rozwiązać. Ponieważ jednak wiedziałem, że grupa nasza utrzymuje łączność radiową z "Hotelem Rubens" /ówczesną siedzibą Sztabu Naczelnego Wodza/ w Londynie, więc poprosiłem któregoś dnia o udostępnienie mi jakiegokolwiek zaszyfrowanego meldunku - i po upływie około dwóch godzin przedstawiłem szefowi grupy odczytaną treść meldunku. Konsternacja była niemała, jednak dla łączności z Londynem nadal posługiwano się maszyną do szyfrowania ICP, z tym tylko, że uprzednio poddawano treść przekazywanej korespondencji dodatkowemu zaszyfrowaniu innym systemem. Jaką metodą doszedłem do rozwiązania w tak krótkim czasie polskiej maszyny do szyfrowania, tego już dzisiaj nie pamiętam.

Powracając do szyfrów niemieckich chcę w pierwszej kolejności omówić szyfr, którym zajął się wymieniony na str. 2. p.A. Palluth i który go też pięknie rozwiązał. Depesz zaszyfrowanych tym systemem było bardzo niewiele, ale na pierwszy rzut oka było widać, że był to szyfr przestawieniowy. Później, po jego rozwiązaniu, okazało się, że była to odmiana przestawienia pojedyńczego. Szyfrowanie odbywało się w sposób następujący:

Szyfrantowi podaje się rząd kilkunastu liczb, np.

7 3 10 6 2 13 9 5 12 1 4 11 8

i prócz tego oddzielnie jeszcze jedną liczbę, np. 5. Na kratkowanym papierze szyfrant wypisuje wspomniany rząd liczb w jednym wierszu po jednej liczbie w każdej kratce, po czym rysuje kontur, tak jak pokazano na przykładzie na następnej stronie, po czym wewnątrz konturu wykreśla co piątą kolejną kratkę. Tych kratek wykreśla tyle, ile wynosi długość tekstu do zaszyfrowania, postępuje w ten sposób

pewien regularny deseń, tak jak niekiedy przy hafcie krzyżykowym.

7	3	10	6	2	13	9	5	12	1	4	11	8
				x					x			
	x					x					x	
			x					x				
x					x					x		
		x					x					x
				x								

Gdyby szyfrantowi razem z kluczem podano nie liczbę 5, lecz np. liczbę 4, wówczas wykreśliłby oczywiście nie co piątą, lecz co czwartą kratkę i deseń wypadłby inny.

Następna czynność szyfranta polega na wpisaniu do otrzymanej tablicy właściwego tekstu w poziomych wierszach po jednej literze do każdej kratki. Gdyby np. szyfrant miał zaszyfrować tekst:

Ich weiss nicht, was soll es bedeuten, dass ich so traurig bin.,

wówczas utworzyłaby się taka tablica:

7	3	10	6	2	13	9	5	12	1	4	11	8
I	C	H	W	x	E	I	S	S	x	N	I	C
H	x	T	W	A	S	x	S	O	L	L	x	E
S	B	E	x	D	E	U	T	x	E	N	D	A
x	S	S	I	C	x	H	S	O	T	x	R	A
U	R	x	I	G	B	I	x	N	S	T	O	x
P												

Ostatnią czynnością szyfranta jest przepisanie w poziomych grupach po 5 liter pionowych kolumienek tablicy, poczynając od kolumienki LETS znajdującej się pod liczbą 1 klucza i kończąc na kolumience ESEB znajdującej się pod liczbą 13 klucza. W ten sposób otrzymuje gotowy szyfrogram:

LETSA DCGCB SRNLN TSSTS WWIII HSUPC EAAIU RIHTE SIDRO SOONE ESEB

Jak się odbywa deszyfrowanie, łatwo można się domyśleć a ni ma potrzeby czynności tej opisywać. Zresztą więcej niż czynność deszyfrowania interesuje nas metoda dekryptażu tego szyfru. Niestety metody takiej nie ma, a raczej jest tylko jedna: benedyktyska cierpliwość połączona z niestrudzoną pracowitością polegając na ciągłym przykładaniu i odrzucaniu i ponownym przykładaniu fragmentów szyfrogramu przy najrozmaitszych hipotezach co do desenia i długości klucza. Spróbujemy tę pracę na konkretnym przykładzie naszkicować. Niech więc dany będzie następujący szyfrogram:

IRUDMECNTTEESHPAIMLEZEIHICOUEEHDEZZUELTEWSNSNNSQUDERNRFE

w którym odstępy między grupami pięcioliterowymi usunęliśmy, żeb nas nie wprowadzały w błąd. Szukamy jakiegoś punktu zaczepienia. Widzimy, że w szyfrogramie występuje litera P, która w zasadzie w języku niemieckim jest literą rzadką. Zakładamy, że na końcu s frogramu jest słowo STOP, bo litera O też występuje i to jeden r Jeżeli nasza hipoteza jest słuszną, to litery O i P znajdują się na końcu kolumienek, z których utworzona jest tablica, jaką chcc zbudować. Szyfrogram więc odpowiednio przedzielamy

IRUDMECNTTEESHP | AIMLEZEIHICO | UEEHDEZZUELTEWSNSNNSQUDERNRFE

a literę O i kilka liter poprzednich jak i literę P i kilka lite poprzednich piszemy w dwóch pionowych kolumienkach obok siebie

H E
I S
C H
O P

Widzimy, że obok bigramu OP utworzył się piękny bigram CH. W szy gramie występuje jeszcze raz litera C, która wymaga litery H jak następnej. Ponieważ przed bigramem OP winna znaleźć się litera T więc na lewo od kolumienki HICO stawiamy kolumienkę CNTT, a w szy gramie naszym po literach CNTT utworzyć musimy dalszą cezurę

IRUDMECNTT | EESHP | AIMLEZEIIICO | UEEHDEZZUELTEWSNSNNSQUDERNRFE

Teraz jednak widzimy, że kolumienki powinny być nie tak długie, bo litera E przed literami ESHP nie może stać samotna

EIE
CHE
NIS
TCH
TOP

Ale trigram TCH nie podoba nam się. Może więc między dwoma TT w kolumience ECNTT jest pole przekreślone ?

E
CIE
NHE
TIS
xCH
TOP

Ale teraz jeden z bigramów CH się rozleciał. Trzeba więc i w środkowej kolumience umieścić pole przekreślone

EI
CHE
NxE
TIS
xCH
TOP

Nie skończyliśmy jeszcze ze słowem STOP. Ale jakiekolwiek S spróbujemy umieścić przed literą T, to zawsze przed dolnym bigramem CH wypadnie spółgłoska różna od S. Tym niemniej jednak kolumienka NSNNS świetnie się zgadza z górnym bigramem CH, zwłaszcza jeżeli i w tej kolumience uwzględnimy pole przekreślone

NEI
SCHE
NNxE
xTIS
NxCH
STOP

Teraz jednak deseń utracił symetrię, którą można by przywrócić

przez umieszczenie w samym środku nowej kolumienki i przez drobne zmiany w pozostałych kolumienkach

xE Ex
Nx IE
SCxHE
NN xS
xT Ix
Nx CH
STxOP

Deseń już się wykrystalizował. Ale i długość klucza da się też już określić, jeżeli szyfrogram odpowiednio przedzielimy

IRUDM|ECNTT|EESHP|AIMLEZ|EIHICO|UEEHDEZZUELTEWS|NSNNS|QUDERNRFE

Nasuwają się teraz dalsze punkty zaczepienia, wiemy np., że po literze Q winna nastąpić litera U, itp. Ale myśl przewodnia naszego postępowania jest już jasną i nie ma chyba potrzeby doprowadzić rozwiązanie do końca. Nie może też być żadnych złudzeń co do tego, że w rzeczywistości sprawa była daleko bardziej skomplikowana i że odczytanie jednej depeszy zajmowało p. Palluthowi nieraz kilka dni pracy.

Interesującą była treść przekazywanych depesz. Okazało się, że ich nadawcami byli niemieccy agenci, którzy uchodząc za zwykłych podróżnych obserwowali ruch statków w portach francuskich i algerskich i poczynione spostrzeżenia zgłaszali swej centrali w Stuttgarcie, która wyposażyła ich w walizkowe stacje nadawcze. Tego rodzaju działalność w strefie nieokupowanej, w świetle warunków zawartego zawieszenia broni, była podobno nielegalną i gdy z odczytanej depeszy wynikło, że określonego dnia wszyscy agenci mają się stawić w Marsylii, francuska policja,przez nas zawczasu poinformowana, urządziła na nich obławę i przychwyciła ich, przy czym walizkowe stacje nadwcze służyły jednocześnie jako znak rozpoznawczy i jako dowód winy, gdyż mieściły się w walizkach tego samego koloru i kształtu.

W ostatnim okresie naszego pobytu w nieokupowanej strefie Francji mieliśmy do czynienia jeszcze z dwoma rodzajami szyfru. Oba szyfry były podstawieniowe i oba były oparte na podobnych zasadach, jednak stopień trudności ich rozwiązania był różny. Trudniejszym o azał się szyfr, który dostał się do naszych rąk wcześniej i który też pierwszy został przez nas rozwiązany. Powinniśmy więc, chcąc zachować porządek chronologiczny, podać wpierw opis szyfru trudniejszego. Jednak ze względów metodycznych wydaje się celowym odłożenie omówienia szyfru trudniejszego na koniec i przedstawienie obecnie szyfru łatwiejszego.

Jak Niemcy szyfr łatwiejszy nazwali, nie wiemy. Nie szedł drogą radiową, lecz przekazywany był w obrębie strefy nieokupowanej drogą telegraficzną i nam dostarczany przez francuską służbę łączności współpracującą z Ruchem Oporu. W ramach warunków zawieszenia broni przysługiwało Niemcom prawo inwigilowania i likwidowania przy współudziale policji Laval'owskiej potajemnych stacji radiowych, które w tym czasie ogromnie się rozmnożyły i utrzymywały łączność głównie z Wielką Brytanią. Centra nasłuchu niemieckiego mieściły się w miastach Pau, Marseille i, jeżeli mnie pamięć nie myli, Toulon. Dokonywane przez te stacje spostrzeżenia co do długości fal, dni i godzin nadawania oraz kierunku, w którym potajemne stacje radiowe się znajdowały, były wzajemnie wymieniane drogą szyfrowanych telegramów, a odpisy tych właśnie telegramów trafiały do naszych rąk.

Szyfrowanie depesz odbywało się w następujący sposób: Przede wszystkim szyfrant otrzymywał klucz w postaci kwadratu o 25 poletkach, do którego wpisanych było w sposób nieregularny 25 liter alfabetu łacińskiego z pominięciem litery J. Następnie szyfrant odpowiednio preparował tekst podlegający zaszyfrowaniu. Preparowanie polegało na zastępowaniu w tekście litery j, jeżeli występowała, ez ii oraz przez podzielenie całego tekstu na bigramy. Je li

liczba liter tekstu była nieparzysta, należało na końcu tekstu dorzucić literę x. Dalszy tok postępowania najlepiej zilustruje przykład. Przypuśćmy, że dostarczony klucz ma postać następującą:

V	F	T	O	K
Q	B	E	I	X
Y	H	N	D	S
L	W	A	M	Z
R	P	G	U	C

a tekst, który ma być zaszyfrowany, niechaj brzmi:

Schön ist die Jugend, sie kommt nicht mehr.

Po spreparowaniu tekst przyjmie postać:

sc ho en is td ie ii ug en dx si ek om mt ni ch tm eh rx

Umawiamy się jeszcze, że przy opisie niniejszego szyfru i szyfru następnego litery kleru oznaczać będziemy małymi literami, a litery szyfru dużymi literami. Taka umowa pozwoli na znaczne skrócenie opisu i uniknięcie dwuznaczności. Szyfrowanie odbywa się bigram po bigramie. Reguły szyfrowania brzmią:

Jeżeli obie litery bigramu kleru znajdują się w jednej i tej samej kolumnie klucza, to jako litery szyfru obieramy litery stojące na prawo od liter kleru, przy czym litera stojąca na prawo od pierwszej litery bigramu kleru będzie tworzyć drugą literę bigramu szyfru, a litera stojąca na prawo od drugiej litery bigramu kleru będzie tworzyć pierwszą literę bigramu szyfru. Przykład:

bigramowi en odpowiada bigram DI

Przez litery stojące na prawo od liter skrajnie prawej kolumny rozumiemy odpowiednie litery znajdujące się w skrajnie lewej kolum-

bigramowi sc odpowiada bigram RY

Jeżeli obie litery bigramu kleru znajdują się w jednym i tym samym wierszu klucza, to jako litery szyfru obieramy litery stojące nad literami kleru, przy czym litera stojąca nad pierwszą literą bigramu kleru będzie tworzyć drugą literę bigramu szyfru, a litera stojąca nad drugą literą bigramu kleru będzie tworzyć pierwszą literę bigramu szyfru. Przykład:

bigramowi ie odpowiada bigram TO

Przez litery stojące nad literami górnego wiersza rozumiemy odpowiednie litery znajdujące się w dolnym wierszu. Przykład:

bigramowi ft odpowiada bigram GP

Jeżeli bigram kleru składa się z dwóch jednakowych liter, to jako bigram szyfru obieramy ziterowaną literę znajdującą się nad ziterowaną literą kleru. Przykład:

bigramowi ii odpowiada bigram OO

Jeżeli obie litery kleru są różne i nie znajdują się ani w tej samej kolumnie ani w tym samym wierszu, wówczas jako litery bigramu szyfru obieramy litery, które wraz z literami kleru tworzą pozostałe wierzchołki prostokąta, przy czym jako pierwszą literę bigramu szyfru obieramy wierzchołek znajdujący się w tym samym wierszu co pierwsza litera bigramu kleru, a jako drugą literę bigramu szyfru obieramy wierzchołek znajdujący się w tym samym wierszu co druga litera bigramu kleru. Przykład:

bigramowi ho odpowiada bigram DF

Podane reguły pozwalają zaszyfrować każdy tekst. Przykładowi kleru podanego na str. 83. odpowiada szyfr:

RY DF DI XD ON TO OO AM DI SI DX XT ZK AO DE PS OA BN CQ

który, po zebraniu liter w grupy po pięć przyjmie postać:

RYDFD IXDON TOOOA MDISI DXXTZ KAODE PSOAB NCQ

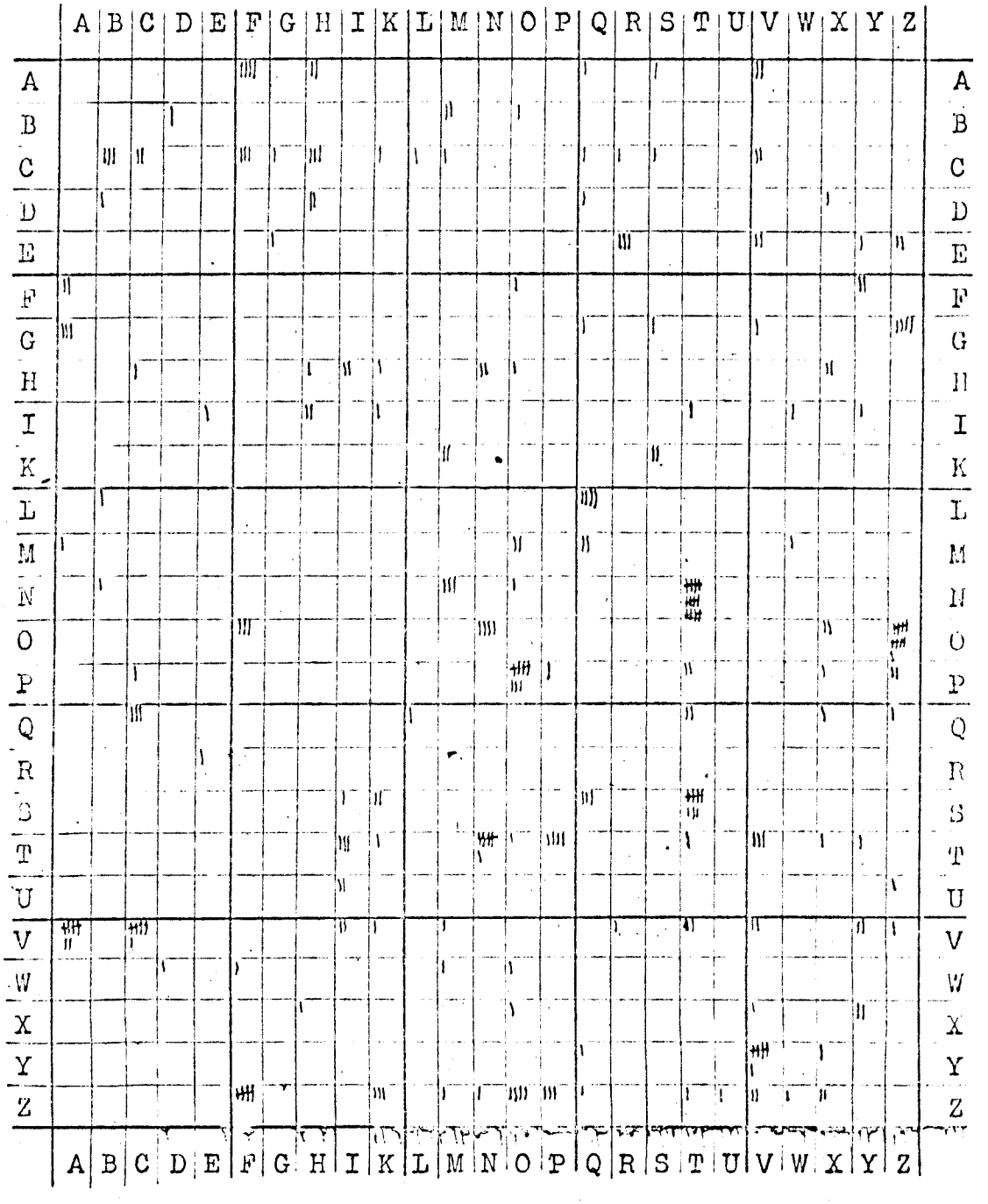
Nie widzimy potrzeby szczegółowego formułowania reguł na deszyfrowanie, gdyż łatwo można się ich domyśleć, a szkoda jest miejsca na podawanie ich in extenso. Chcemy od razu przejść do naszkicowania na konkretnym przykładzie sposobu dekryptażu szyfru. Zwróćmy jednak uwagę na pewne konsekwencje wynikające z tych reguł. Jeżeli mianowicie pewien bigram szyfru XY daje bigram kleru qs, to zawsze i na odwrót bigram szyfru YX daje bigram kleru sq, a ponadto w dwóch wypadkach na trzy bigram szyfru QS daje bigram kleru xy i bigram szyfru SQ daje bigram kleru yx. Pamiętając o tej zasadzie ułatwimy sobie nieco rozwiązanie szyfru.

Przypuśćmy, że chcemy rozwiązać następujący szyfrogram, który dla ułatwienia już podano w rozbiciu na bigramy:

VA ZO YV EG ST NT HH OF AF HO OZ EV KS VA CH VA BD ZK LB IY ZV HN
EZ TI DH OX IW VA ZO HN HI NT CH QZ RE SI BM IE IK WF HI MA UI TY
DX ZF PO LQ ST OZ NT ON KS GZ PX VC ZW XV ZF BO TN GS ZK TV MO EZ
TI DH OX QX LQ YQ CK QB EY NO ZQ QL CH QT NT VA ZO CF AH NT VA CV
GA CF AH VA AF ER SQ ST DQ ZM SK VI CB VY CM ZF YV VA KM WO PO OZ
GZ ZU ER TI CB VC AF CS GQ TK DB VT TN TN SK NT TN PK VI PO NT TP
XY GZ ON PO TP XY QT NM PO NT WM PZ ZN ZX EV TV VR ZK TV TP ZO QB
FO ER NT GA UI VC IH ZP ZP VV ST CG PT LQ ST OZ ZV NT VC OF AQ MV
ST GV ON PT NT CV YV VC NB YV AF PO OZ CF PP OZ QB PO IT YV ZF TP
HK ST WD OZ ZP MQ UZ XO VT NT ON NT OF NT YX ZF PO SQ ST TX CB OZ
NM PO TT MO NT VM CC PC HC AS BM AV TN LQ PZ AV KM CQ FY FA ZT VV
GA FA XH YV MQ TN CR OZ SQ VY OZ NM VK IH CC OZ HX FY VC HX CL GZ

Szyfr jest, jak wiemy, rodzajem bigramówki i musimy rozwiązać go tak samo, jak rozwiązuje się bigramówki, to znaczy, musimy rozpocząć od sporządzenia tablicy frekwencji bigramów. Alfabety po boku oznaczają pierwsze, alfabety na górze i dole oznaczają drugie lite

ry bigramów, kreseczki oznaczają częstość, z jaką bigramy w szyfrze wystąpiły.



Ale sporządzenie tablicy frekwencji bigramów, to jeszcze nie wszystko. Trzeba jeszcze wyłowić w szyfrogramie i zaznaczyć, najlepiej kolorowymi ołówkami, wszelkiego rodzaju ~~wszelkie rodzaju~~ zdublowania, okulary, powtórzenia, jednym słowem to wszystko, co może nam nasunąć przypuszczenia co do treści. W szyfrogramie podkreśliliśmy tylko jedno powtórzenie, ale powtórzeń jest znacznie cej. Grupa VA ZO powtarza się trzy razy. Same bigra... VA i ...O

też są częste. Bardzo częstym jest bigram OZ, a bigram AV też dwa razy wystąpił. Szukamy więc na grupę VA ZO określenia czteroliterowego, które samo jest częste, które składa się z częstych bigramów i którego bigramy, jeżeli porządek liter w nich odwrócimy, też są częste. Takim jest w języku niemieckim słowo eine. Zakładamy za tem, że

VA oznacza ei
ZO " ne
AV " ie
OZ " en

Jednak to nam niewiele jeszcze daje. Najczęstszym w szyfrze jest bigram NT i bigram TN też często występuje. Zakładamy więc, że

NT oznacza er
TN " re

i jednocześnie ryzykujemy hipotezę, że

ER oznacza nt
RE " tn

Ponieważ bigram ST jest bardzo frekwentny, zaś bigram TS wogóle nie występuje, przeto zakładamy, że

ST oznacza ch
TS " hc.

Wszystkie poczynione przez nas założenia wpisujemy do tablicy bigramów, nawet wówczas, gdy dany bigram wogóle w szyfrze nie wystąpił, np. nasze założenie, że TS oznacza hc, gdyż będzie to potrzebne przy składaniu klucza. Poczynione założenia podpisujemy też pod bigramy szyfru, aby móc sprawdzić, czy nie prowadzą do niedorzeczności, i aby tworzyć dalsze założenia. Przy poczynionych dotychczas założeniach szyfrogram wyglądać będzie następująco:

VA ZO YV EG ST NT HH OF AF HO OZ EV KS VA CH VA BD ZK LB IY .. ..
ei ne ch er en ei st ei

EZ TI DH OX IW VA ZO HN HI NT CH QZ RE SI BM IE IK WF HI MA UI TY
ei ne er st tn

DX ZF PO LQ ST OZ NT ON KS GZ PX VC ZW XV ZF BO TN GS ZK TV MO EZ
ch en er re

TI DH OX QX LQ YQ CK QB EY NO ZQ QL CH QT NT VA ZO CF AH NT VA CV
st er ei ne er ei

GA CF AH VA AF ER SQ ST DQ ZM SK VI CB VY CM ZF YV VZ KM WO TO OZ
ei nt ch ch.

GZ ZU ER TI CB VC AF CS GQ TK DB VT TN TN SK NT TN PK VI PO NT ..
nt re re er .. er

XY GZ ON PO TP XY QT NM PO NT WM PZ ZN ZX EV TV VR ZK TV TP ZO QB
er ne

FO ER NT GA UI VC IH ZP ZP VV ST CG PT LQ ST OZ ZV NT VC OF AQ ..
nt er ch ch en er

ST GV ON PT NT CV YV VC NB YV AF PO OZ CF PP OZ QB PO IT YV ZF ..
ch er en en

HK ST WD OZ ZP MQ UZ XO VT NT ON NT OR NT YX ZF PO SQ ST TX CB OZ
ch en er er er ch. en

NM PO TT MO NT VM CC PC HC AS BM AV TN LQ PZ AV KM CQ FY FA ZT VV
er ts ie re ie

GA FA XH YV MQ TN CR OZ SQ VY OZ NM VK IH CC OZ HX FY VC HX CL GZ
re en en en

Widzimy, że już zaczynają zarysowywać się pierwsze fragmenty treści. I tak na przykład znajdująca się w piątym wierszu grupa

VA AF ER SQ ST
ei nt ch

z pewnością oznacza słowo eigentlich, przez co określone są cztery dalsze bigramy AF, FA, SQ, QS, a może nawet, z pewnym ryzykiem, piąty bigram EG. Ale nie będziemy kontynuować naszych poszukiwań, gdyż chcieliśmy tylko wskazać kierunek postępowania. Wolimy założyć, że treść szyfrogramu została już całkowicie odczytaną, aby móc przejść do następnego i ostatniego etapu rozwiązywania szyfru, to jest do odtwarzania klucza. Do tego celu służy tablica bigramów na następnej stronie. Zostały w niej ujęte wszystkie bigramy występujące w przykładowym szyfrogramie, jak również, o czym wzmiankowaliśmy na str. 87., odwrócenie tych bigramów, nawet jeżeli w szyfrogramie nie występują, a więc obok występującego np. bigramu GA ujęty został

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A						ge	uz	it				izhdsz				dzihlaim		ic			ie					A
B			tl	mh							sh		rf	rd			kt	ht			se		ul	ub		B
C		lthm	tt			we	wa	stmb		rt					le		nt				sc				on	C
D							fa		va															na		D
E																										E
F	egzuti		ewawtstr		af av			itasr	atsy	rsys		so	nu rv	rmln		du		iw cahr	ahcr	gm	if ea	lp gs	gi	ng om	euáu co	F
G				bm																						G
H																										H
I																										I
K																										K
L	zi	hsdhprdr	zs			un		vrmr		os nl		vovn	ovfu	nvufndl		isdi dn			erzreb		ez	us uk	urfb		evoeoened	L
M																										M
N																										N
O																										O
P			el																							P
Q	zd	hi	altkth	mi	tn		ud wi		achamg	rhrc	si	id	re	rzbe		lib a		il hc	abch aa		h n he		gb g a	od r	ad or ef	Q
R																										R
S	ci																									S
T																										T
U																										U
V	ei		es		cs		fi		aesg			ze su		kurubf		bgdoda	nh		eh agarro	f	s ss hfinme		fh gr ut	ni rg	emcutu	V
W				lubu		pl		i g																		W
X																										X
Y					anno	gnue			mo																	Y
Z							ua			oc		ve	oeee	ndee	de					e	mc	ut				Z
	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

nie występujący bigram AG. Układ tablicy bigramów jest taki, że w każdym poletku górna litera oznaza pierwszą literę bigramu kleru, a dolna litera - drugą literę tego bi

Dalszy tok postępowania jest następujący: Wybieramy dowolną literę z bocznych alfabetów tablicy bigramów /szczególnie wygodnie jest wybrać literę występującą w języku niemieckim rzadko/ n.p. literę X i patrzymy, jakie litery występują kilkakrotnie w górnej części wiersza X. Będą to litery b oraz r. Potem patrzymy, jakie litery występują kilkakrotnie w górnych częściach wierszy B i R. Będą to litery t oraz r. Potem patrzymy, jakie litery występują kilkakrotnie w górnej części wiersza T. Będą to litery h oraz r. Potem patrzymy, jakie litery występują kilkakrotnie w górnej części wiersza H. Będą to litery t oraz r. Koło zamknęło się. Wnioskujemy, że w kluczu litery X, B, R, T, H znajdują się w jednym wierszu. Podobnie postępujemy wychodząc z innych liter i chociaż chwilami mogą powstać wątpliwości, do którego wiersza daną literę należy zakwalifikować, to jednak wnet ustalimy, że do poszczególnych wierszy klucza litery wchodzą w następujący sposób:

XBRTH QYAGI SWLKC DUZMO PVEFN

Dla ustalenia, jaka jest kolejność wierszy w kluczu, najlepiej jest wyjść z bigramów składających się z dwóch liter jednakowych. Ponieważ bigram CC daje bigram tt, przeto wiersz, w którym występuje litera C, znajduje się nad wierszem, w którym jest litera T. Ponieważ bigram HH daje bigram ii, przeto wiersz, w którym występuje litera H, znajduje się nad wierszem, w którym jest litera I. Tak postępując ustalamy kolejność wierszy

1. PVEFN 2. SWLKC 3.XBRTH 4. QYAGI 5. DUZMO

z tym, że możliwa jest jeszcze cykliczna zamiana wierszy.

Dla ustalenia składu liter wchodzących do poszczególnych kolumn klucza postępujemy podobnie, z tą tylko różnicą, że zamiast patrzeć na litery wchodzące do górnych części wierszy - patrzymy teraz na litery wchodzące do dolnych części wierszy. W ten sposób [illegible]

my, że skład poszczególnych kolumn klucza jest następujący:

Y	X	Q	E	V
N	U	L	A	S
O	G	P	Z	H
R	F	B	T	I
K	W	D	C	M

Kolejność kolumn znajdziemy szukając, jakie jeszcze litery występują w dolnych częściach wierszy Y, N, O, R, K poza literami Y, N, O, R, K. Wystarczy znaleźć jedną taką literę. Jeżeli to będzie np. litera F, wówczas wnioskujemy stąd, że kolumna YNORK znajduje się w kluczu na prawo od kolumny, w której występuje litera F. W taki sposób znajdziemy kolejność:

1.	2.	3.	4.	5.
Y	E	V	Q	X
N	A	S	L	U
O	Z	H	P	G
R	T	I	B	F
K	C	M	D	W

z tym, że możliwa jest zawsze cykliczna zamiana kolumn. Mając już kolejność wierszy i kolejność kolumn, bez trudu ustalamy, że następujący winien być kształt klucza:

N	E	V	P	F
K	C	S	L	W
R	T	H	B	X
Y	A	I	Q	G
O	Z	M	D	U

Być może, że uzyskany kształt klucza różni się od oryginału, tym niemniej jednak daje on te same wyniki, jakie dawałby oryginał klucza, co łatwo można wyrywkowo sprawdzić na tablicy bigramów ze str.89.

Nie pamiętam, czy klucze szyfru zmieniano codziennie, czy też w innych okresach czasu, dość że szyfr ten bieżąco rozwiązywaliśmy. Ponieważ treść depesz zawierała, jak o tym już wspomniałem, in-

macje o śledzonych przez Niemców tajnych stacjach i nieraz podawała wiadomość, że taka a taka stacja jest dojrzała do likwidacji /aushebereif/, więc odczytany przez nas materiał miał niewątpliwie wielkie znaczenie dla Ruchu Oporu, gdyż umożliwiał podjęcie kroków udaremniających dekonspirację stacji.

Nie było nam zbyt przyjemnie, gdy z przeczytanych depesz wynikało, że Niemcy zaczęli interesować się naszą własną stacją. Pozostaliśmy jednak na posterunku, aż pewnego dnia w październiku 1942 r., w czasie gdy stacja nasza pracowała, w pobliże naszego zameczku Les Fouzes zajechał wóz z anteną ramową na dachu, z którego wyskoczyło kilku drabów i otoczyło - - maleńki, samotnie stojący domek, odległy o kilkaset kroków od naszego zamku, ale leżący na tej samej co nasz zamek linii z wozem. Dlaczego Niemcy odstąpili potem od przeprowadzenia rewizji również u nas, nie wiadomo. W każdym razie jedynie zwykły zbieg okoliczności nas uratował. Nie potrzebuję dodawać, że następnego dnia już nas w zamku więcej nie było.

Zanim opuściliśmy teren Francji, przebywaliśmy jeszcze przez kilka miesięcy w strefie okupowanej przez Włochów / w międzyczasie nastąpił desant amerykański w Afryce Północnej i w odwet za to Niemcy i Włosi zajęli resztę Francji/, gdzie zdaniem naszych francuskich opiekunów byliśmy narażeni na mniejsze niebezpieczeństwo. Ale i tam zmienialiśmy dość często miejsce pobytu, po uprzednim podzieleniu się na kilka mniejszych grup. Przebywaliśmy w takich miejscowościach, jak Antibes, Nice, Cannes, w niektórych po kilka razy. Gdy przygotowania do naszej przeprawy przez Pireneje były dostatecznie zaawansowane, wróciliśmy znów do części Francji okupowanej przez Niemców. Ukrywaliśmy się w różnych miejscowościach, to na strychu domu /w Tuluzie/, to u przemytnika /w Perpignan/, to w domku podmiejskim /w Tuluzie/, to w eleganckim hotelu zajętym przez oficerów niemieckich, ale którego portier był w Ruchu Oporu /w Nar-

bonne/, to w podejrzanych hotelikach przygranicznych wyraźnie nastawionych na przemyt ludzi i towarów /Aix les Thermes, Tour de Carol/. Na stacji granicznej Tour de Carol, gdzie byłem już tylko z kol. H. Zygalskim, zatrzymywali nas kilkakrotnie i żandarmi francuscy i straż niemiecka, oglądając dokładnie nasze /podrobione/ dowody tożsamości i wypytując nas długo i szeroko o cel naszego pobytu w strefie granicznej. Wyszliśmy jednak cało z opresji i późnym wieczorem dnia 29.I.1943 r. rozpoczęliśmy przeprawę przez Pireneje z francusko-hiszpańskim przewodnikiem-przemytnikiem. Przekroczenie granicy francusko-hiszpańskiej nastąpiło niedaleko Andorry.

XI.

Zaraz po przejściu granicy przewodnik obrabował nas z reszty przedstawiających jakąś wartość przedmiotów, które mieliśmy jeszcze przy sobie /zegarek, aparat fotograficzny/, i pozostawił nas własnemu losowi. Już po kilku godzinach wpadliśmy w miejscowości Belver w ręce żandarmów hiszpańskich. Dalszych kilka miesięcy spędziliśmy w więzieniach, naprzód w Seo de Urgel, potem w Leridzie. Następnych kilka miesięcy przebyliśmy w Hiszpanii na wolności pod opieką Polskiego Czerwonego Krzyża, częściowo w Leridzie, częściowo w Madrycie. Tu dowiedzieliśmy się o losach pozostałych członków naszej grupy. Kilku wogóle nie opuściło Francji, kilku innych przedarło się podobnie jak my do Hiszpanii, czterech zaś, mianowicie ppułk. Langer, mjr. Ciężki, p. Palluth i pracownik "AVA'y, p. Fokczyński, przy próbie przejścia przez granicę wpadło w ręce niemieckie i dostało się do niewoli wzgl. do obozu. Po zakończeniu wojny ppułk. Langer i mjr. Ciężki, uwolnieni z Oflagu, znaleźli się w Londynie, pp. Palluth i Fokczyński natomiast zginęli od bomby alianckiej zrzuconej na obóz w Oranienburgu [illegible] tko przed k[illegible]

wojny. Tak więc straty naszej grupy, wraz z poprzednią stratą trzech osób, wynosiły około 30 % całego stanu.

Gdy w Madrycie zebrała się dostatecznie duża liczba uciekinierów z Francji, zorganizowano ich przerzut do Wielkiej Brytanii. Dnia 22.VII.1943 r. przewieziono nas pociągiem poprzez granicę hiszpańską do małego portu portugalskiego, gdzie cały nasz transport składający się z kilkuset osób załadowano na statek rybacki, z którego na pełnym morzu przeskakiwaliśmy na pokład brytyjskiego okrętu wojennego płynącego do Gibraltaru. Nas kilku, stanowiących resztę dawnej grupy "300", przewieziono po paru dniach samolotem do Wielkiej Brytanii.

Wcielony do wojska polskiego przydzielony zostałem wraz z paroma jeszcze osobami do Pułku Radia Sztabu Naczelnego Wodza. Dowództwo jednego z batalionów wchodzących w skład pułku mieściło się w Stanmore, a kompania podsłuchowa tegoż batalionu stacjonowała w Boxmore. Przy tej właśnie kompanii zorganizowano po naszym przybyciu na teren Wielkiej Brytanii małą komórkę rozwiązywania szyfrów pod nazwą plutonu eksploatacyjnego. Do jednej z dwóch sekcji, na które się dzieliła, wszedłem ja i kol. Zygalski, a prócz nas dwóch jeszcze kilka osób stanowiących pod względem kryptologicznym zupełnie surowy materiał. Komórka nasza, choć organizacyjnie należała do Pułku Radia, była ściśle powiązana z Oddziałem II Sztabu Naczelnego Wodza, którego przedstawiciele, pułk. Langenfeld i pułk. Gaweł, często nas odwiedzali.

W takich to zmienionych warunkach wznowiliśmy naszą pracę tak nagle przerwaną we Francji. Przez cały czas pobytu w Wielkiej Brytanii zajmowaliśmy się, o ile pamiętam, jednym tylko rodzajem szyfru, gdyż widocznie radiotelegrafiści tylko jeden rodzaj szyfrogramów odbierali. Był to szyfr, którym posługiwały się formacje SS. Nazywał się "Doppelwürfelverfahren". Rozwiązaliśmy go już na terenie Francji, ale główny okres jego eksploatacji przypadł na lata

naszej pracy w Anglii. Dlatego też jak również z uwagi na pewną złożoność szyfru opis szyfru i jego rozwiązania przesunęliśmy do chwili obecnej.

Szyfrant otrzymuje klucz w postaci dwóch kwadratów o 25 poletkach każdy, zwanych kwadratami A i B. Kwadraty umieszczone są obok siebie, kwadrat A z lewej, kwadrat B z prawej strony. Do poletek każdego kwadratu wpisanych jest w sposób nieregularny 25 liter alfabetu łacińskiego z wyłączeniem litery J, przy czym w kwadracie A litery są inaczej umieszczone niż w kwadracie B. Poza tym szyfrantowi podaje się na czas ważności klucza określoną liczbę jak 19 albo 22 albo 27 /czyli rzędu od kilkanaście do dwadzieściakilka/.

Szyfrant przed przystąpieniem do szyfrowania musi tekst odpowiednio przygotować. Przygotowanie to polega na wypisaniu tekstu na kratkowanym papierze dwuwierszami, przy czym długość każdego wiersza w dwuwierszu wynosi tyle, ile liczba podana szyfrantowi wraz z kluczem. Literę J, jeżeli występuje, zastępuje się przez II. Jeżeli liczba liter tekstu jest nieparzysta, dorzuca się na końcu tekstu literę X. Ostatni dwuwiersz tekstu może być krótszy niż pozostałe dwuwiersze.

Zasady szyfrowania zilustrujemy na przykładzie. Niech dostarczony klucz ma postać następującą

M	U	D	X	O
Z	B	S	K	C
N	W	L	F	I
V	G	A	P	R
E	Y	Q	H	T

"A"

H	D	X	L	Q
V	R	K	B	N
I	A	U	G	P
O	Y	C	Z	W
S	E	T	M	F

"B"

i niech podana wraz z kluczem liczba będzie na przykład 17, tekst zaś, który chcemy zaszyfrować, niech brzmi:

Wie die Alten sungen, so zwitschern jetzt die Jungen.

Po odpowiednim przygotowaniu tekst przyjmie postać:

w i e d i e a l t e n s u n g e n
s o z w i t s c h e r n i i e t z

t d i e i i
u n g e n x

Szyfrowanie odbywa się bigramami, przy czym przez bigram rozumie się tutaj dwie litery umieszczone nad względnie pod sobą w jednym dwuwierszu. Kolejne bigramy w tym znaczeniu są więc ws, io, ez, dw itd. Reguły szyfrowania są następujące:

Szukamy górną literę bigramu w kwadracie "A" klucza, a dolną literę bigramu w kwadracie "B" klucza. Jeżeli obie te litery znajdują się na tym samym poziomie, to jako litery szyfru obieramy litery stojące nad nimi, przy czym pierwszą literą bigramu szyfru będzie litera z tablicy "B", a drugą literą bigramu szyfru będzie litera z tablicy "A" klucza. Przykład:

bigramowi et odpowiada bigram CV

Przez litery stojące nad literami górnego wiersza rozumiemy odpowiednie litery najniższego wiersza. Przykład:

bigramowi dl odpowiada bigram MQ

Jeżeli obie litery kleru znajdują się na różnych poziomach, to jako litery bigramu szyfru obieramy litery tworzące wraz z literami kleru wierzchołki prostokąta, przy czym jako pierwszą literę bigramu szyfru obieramy literę z tablicy "B", a jako drugą literę bigramu szyfru obieramy literę z tablicy "A" klucza. Przykład

bigramowi ws odpowiada bigram IY.

zyfrowany przy pomocy tych reguł obrany przez nas te[illegible]

IY IR MV QA VC CV OQ UA SO YV AZ QD HW VZ YY CV GV TI QS BC YV PC UO

a po zebraniu liter w grupy po pięć:

IYIRM VQAVC CVOQU ASOYV AZQDH WVZYY CVGVT IQSBC YVPCU O.

Deszyfrowanie odbywa się w sposób podobny jak szyfrowanie z tym, że wszystkie czynności są teraz wykonywane w kolejności odwrotnej. Deszyfrant naprzód dzieli szyfrogram na odcinki po 34 litery / dlatego, bo 2 x 17 = 34; przy innym kluczu długość odcinków będzie inna/, a następnie każdy odcinek na bigramy. Potem bierze kolejne bigramy i szuka liter wchodzących do tych bigramów w kwadratach "A" i "B", przy czym obecnie pierwszej litery bigramu szyfru szuka w kwadracie "B", a drugiej litery w kwadracie "A". Jeżeli obie litery bigramu szyfru są na jednym poziomie, to jako litery kleru bierze litery stojące pod nimi, a jeżeli są na różnych poziomach, to jako litery kleru bierze litery tworzące z tamtymi wierzchołki prostokąta. Litery kleru wzięte z kwadratu "A" klucza pisze nad literami kleru wziętymi z kwadratu "B" klucza. A więc ponieważ bigram IY daje litery ws, przeto literę w pisze w górnym, a literę s w dolnym wierszu. Litery otrzymane z następnych bigramów piszę odpowiednio obok liter $\frac{w}{s}$ itd. Po dojściu do końca pierwszego odcinka deszyfrant zaczyna dwa nowe wiersze i tak postępuje dalej aż do końca szyfrogramu.

Inaczej oczywiście postępujemy przy próbie dekryptażu. Pierwszym warunkiem przed przystąpieniem do rozwiązania szyfru jest posiadanie dostatecznie dużego materiału szyfrowego. Omawiany rodzaj szyfru wymaga go niestety dość dużo. Trudno ściśle określić konieczne minimum, jednak z praktyki naszej wynika, że na ogół dobrze rozwiązuje się szyfr, gdy ma się do dyspozycji co najmniej 2000 liter materiału zaszyfrowanego jednym kluczem. Następnie musimy się znaleźć w dużym materiale powtórzenia, gdyż dzięki nim [illegible] mogli ob[illegible]

lić długość wierszy, jakimi ułożony był tekst przed zaszyfrowaniem. Może wydawać się dziwnym, że przy tym, bądź co bądź dość wyrafinowanym systemie szyfrowym powtórzenia się jeszcze zdarzają. Okazało się jednak, że powtórzenia były, i to nawet stosunkowo częste, a to z powodu stereotypowej treści wielu depesz. Przekonaliśmy się mianowicie, że w treści bardzo często występowały liczby, szczególnie przy określeniu czasu, n.p.

xvonxeinsnullnullnullxbisx

Jeżeli identyczne określenie czasu wystąpi w różnych depeszach lub dwa razy w tej samej depeszy, wówczas otrzymamy powtórzenie, które często zaczyna się lub kończy razem z wierszem, zależnie od tego, jak te same fragmenty treści są usytuowane we wierszach. Jeżeli n.p. usytuowanie tych samych fragmentów treści jest następujące:

1/.
```
..............xvo
nxeinsnullnullnul
lxbisx..........
................
```

2/.
```
............xvonx
einsnullnullnullx
bisx............
................
```

to jedno z powtórzeń znajdzie się na końcu wiersza, a jeżeli usytuowanie fragmentów jest inne, np. jak poniżej:

3/.
```
................
............xvonx
einsnullnullnullx
bisx............
```

4/.
```
................
..............xvo
nxeinsnullnullnul
lxbisx
```

to jedno z powtórzeń znajdzie się na początku wiersza. Przy jeszcze innych usytuowaniach tych samych fragmentów treści mogą nie wystąpić żadne powtórzenia w szyfrze albo też mogą wystąpić powtórzenia w środku wiersza. Tym niemniej jednak, zazwyczaj, mając kilka powtórzeń i licząc ilość liter od początku depeszy do początku lub końca powtórzeń i badając, czy niektóre z otrzymanych w ten sób liczb mogą być wielokrotnością długości wiersza, [illegible]

się zorientować, ile długość wiersza wynosiła.

Następnym etapem pracy, gdy długość wiersza już była znana, było przepisanie całego materiału szyfrowego na papierze kratkowanym, bigram po bigramie w ten sposób, że drugie litery każdego bigramu pisało się pod pierwszymi literami i że po otrzymaniu dwuwiersza długości poprzednio ustalonej rozpoczynało się pisanie następnego dwuwiersza. Pod każdym dwuwierszem pozostawiano miejsce, aby móc tam wpisać kler, w miarę jak robiono założenia odnośnie znaczenia poszczególnych bigramów.

Przed rozpoczęciem robienia takich założeń należało zapoznać się z frekwencją, z jaką poszczególne bigramy występują. Należało więc sporządzić tabelę frekwencji bigramów podobną do pokazanej na str. 86. Jest rzeczą zrozumiałą, że obraz frekwencji był teraz zupełnie inny niż w szyfrze poprzednim. Bo jeżeli na przykład w szyfrze poprzednim bigram oznaczający litery ee należał do bardzo rzadkich, to w szyfrze omawianym obecnie bigram oznaczający litery ee był najczęstszym ze wszystkich. Ogólnie można powiedzieć, że bigram oznaczający litery xy powinien wystąpić z frekwencją równą iloczynowi frekwencji litery x przez frekwencję litery y:

$$fr./xy/ = fr./x/ \cdot fr./y/$$

Dlatego też po sporządzeniu tabeli frekwencji bigramów stosunkowo łatwo było określić, który bigram oznacza litery ee i które bigramy oznaczają litery en lub ne. Ale przy dalszych poszukiwaniach powstawały trudności, gdyż dla określenia znaczenia następnych bigramów znajomość samej frekwencji już nie wystarczała i należało zakładać treść jednocześnie i w górnym i w dolnym wierszu, co oczywiście jest znacznie trudniejsze niż zakładanie treści w jednym tylko wierszu. Dlatego właśnie rozwiązywanie omawianego szyfru wymaga znacznie więcej materiału niż rozwiązanie szyfru poprzedniego. Znaczną pomoc w rozwiązywaniu stanowi znajomość [illegible]

Jak już wspomniałem, w treści depesz występowało bardzo dużo cyfr. Poza tym szablonowe były początki depesz, które niezmiennie brzmiały hssupfx albo hssupolfx albo hxssxuxpfx albo hoehererxssxundxpo lizeifuehrerx lub podobnie. Poza tym korzystaliśmy również z tej cechy szyfru, że jeżeli jakiś bigram np. PQ oznacza litery rs, to w czterech wypadkach na pięć bigram SR oznacza litery qp. Wszystko to dawało pewne punkty zaczepienia, ale nie zmieniało faktu, że całkowite odczytanie materiału zaszyfrowanego jednym kluczem trwało szereg godzin. Nie pamiętam dokładnie, jak często odbywała się zmiana klucza, ale prawdopodobnie następowało to co osiem godzin.

Ostatnim etapem pracy była rekonstrukcja klucza. Sprawa miała właściwie znaczenie drugorzędne, bo gdy do tej pracy przystępowano, to i tak cały materiał był już odczytany i posiadanie klucza stawało się zbędne. Nie chcę się nad tą sprawą zatrzymywać również i z tych względów, ponieważ było by to w pewnym stopniu powtórzeniem tego, co o sprawie rekonstrukcji klucza już podawaliśmy przy opisie szyfru poprzedniego. Wspomnę więc tylko, że w toku rozwiązywania szyfru sporządza się tabelę bigramów podobną do tabeli na str. 89., aby do niej wpisywać znaczenie każdego bigramu w miarę, jak się nam ono nasuwa. Potem tabela służy jeszcze do rekonstrukcji klucza. Ale gdy dla rekonstrukcji klucza szyfru poprzedniego potrzebne było przeanalizowanie górnych i dolnych liter tylko we wierszach tabeli, to dla rekonstrukcji klucza szyfru obecnie omawianego trzeba także przeanalizować górne i dolne litery w kolumnach tabeli. Górne litery wierszy dają bowiem wiersze kwadratu "A", a dolne litery wierszy dają kolumny kwadratu "B". Natomiast górne litery kolumn w tablicy frekwencji bigramów określają kolumny kwadratu "A", a dolne litery kolumn określają wiersze w kwadracie "B". Uporządkowanie wierszy i kolumn we właściwej kolejności w kwadratach "A" i "B" też nie sprawia większych trudności i dlatego od jego

wiania odstępujemy.

XII.

Opisany na poprzednich stronach szyfr zwany "Doppelwürfelverfahren" był jedyny i ostatnim niemieckim szyfrem, jakim się na terenie Wielkiej Brytanii zajmowaliśmy. Nie umiem dokładnie określić, kiedy nasza działalność kryptologiczna ustała, ale prawdopodobnie nastąpiło to już na wiele miesięcy przed końcem wojny, wskutek braku materiału szyfrowego. Komórkę naszą, nie mającą już racji bytu, rozwiązano, a jej pracowników przydzielono do różnych jednostek wojskowych, głównie na terenie Szkocji. Wraz z tymi jednostkami przebywałem jeszcze przez szereg miesięcy w różnych miejscowościach szkockich jak Glasgow, Kirkcaldy, Cardross, aż wreszcie we wrześniu 1946 roku, gdy rozpoczął się zaciąg do Polskiego Korpusu Przysposobienia i Rozmieszczenia, zgłosiłem się do powrotu do Kraju, który nastąpił w listopadzie tegoż roku drogą morską do Gdyni.

Za rozwiązanie szyfru maszynowego "Enigma" odznaczono mnie w roku 1938 Złotym Krzyżem Zasługi.

Za działalność we Francji w warunkach konspiracyjnych przyznano mi Srebrny Krzyż Zasługi z Mieczami.

W roku 1943 otrzymałem nominację na podporucznika w Korpusie Oficerów Łączności, a po kilkunastu miesiącach awans na porucznika.

I to byłoby już wszystko.

Bydgoszcz, w marcu 1967 roku.

M. Rejewski

/M.Rejewski/

S P I S R O Z D Z I A Ł Ó W