Z Archiwum Instytutu Zachodniego
DOKUMENTY
Nr 30/2021 21'05'21

Od Cezara przez Sanatorium do Sobieskiego, czyli odkrywanie metody i klucza szyfrowania w protokołach akcji „Iskra-Dog"

Autor: Krystian Sobański

Spis treści

W artykule opisano – dotąd niepublikowane – parametry szyfru użytego do utajnienia protokołów zebranych pod koniec II wojny światowej podczas akcji „Iskra-Dog". Odkryto je dzięki połączeniu doświadczeń autora z zakresu (dość prostych) metod szyfrowania z danymi zawartymi w protokołach akcji „Iskra-Dog" (danymi niejawnymi oraz ujawnionymi przez Edwarda Serwańskiego). W połączeniu z wynikami kwerendy na temat szyfrów używanych przez AK podczas II wojny światowej oraz z wynikami własnej analizy materiałów dostępnych w dokumentach zgromadzonych w Archiwum II Wojny Światowe IZ – umożliwiło to odtworzenie metody i klucza szyfrowania używanych podczas akcji „Iskra-Dog".

Mimo kilku publikacji[1] dotyczących tych protokołów i zawartych w nich informacji (częściowo rozszyfrowanych przez inicjatora akcji prof. E. Serwańskiego oraz jego współpracowników) – dotąd nie była publicznie znana ani metoda, ani klucz ich szyfrowania. To właśnie odkrycie tych faktów jest głównym osiągnięciem niniejszego opracowania. Niejako konsekwencją czy dodatkową korzyścią jest odszyfrowanie tej części protokołów, które dotąd pozostawały niejawne. Po śmierci E. Serwańskiego w 2000 r. ich odszyfrowanie było niemożliwe właśnie ze względu na nieznaną metodę i brak klucza szyfrującego.

Autor nie jest historykiem, lecz amatorem i dlatego w tym miejscu dziękuje za duże fachowe wsparcie, życzliwość oraz udostępnienie materiałów źródłowych z Archiwum IZ panu dr. Bogumiłowi Rudawskiemu.

Akcja „Iskra-Dog”

Tragiczne losy mieszkańców Warszawy nie zakończyły się wraz z upadkiem Powstania w 1944 r. Wygnani z Warszawy mieszkańcy zostali zgromadzeni w obozach przejściowych w Pruszkowie i okolicach. Ze zniszczonego miasta niemal każda rodzina wyniosła przede wszystkim wiele tragicznych doświadczeń po niemieckich zbrodniach dokonanych na cywilach. Edward Serwański, inicjator akcji, uznał, że te doświadczenia należy spisać i udokumentować formalnie jako protokoły, które po wojnie staną się dowodami przed sądem. Całą akcję zbierania tych zeznań zaplanowano i przeprowadzono w warunkach konspiracji przy współpracy członków podziemnej organizacji „Ojczyzna”. Aby zapewnić bezpieczeństwo zeznających, wszelkie dane osobowe zostały zaszyfrowane i zarchiwizowane. W ten sposób zebrano ponad 300 świadectw o okrucieństwach okupantów popełnionych podczas okupacji i pacyfikacji Powstania oraz tuż po nim. Część z tych materiałów istotnie wykorzystano w procesie sądowym i to bardzo znaczącym, tzn. w procesie norymberskim.

Po wojnie Edward Serwański wraz z Ireną Trawińską opracowali ankiety i już w 1946 r. opublikowali część z nich. W kolejnych latach wydali kolejne fragmenty tego zbioru w osobnych publikacjach. Nigdy nie opublikowano tych materiałów w całości. Po śmierci inicjatora akcji „Iskra-Dog” okazało się, iż nigdzie nie został opisany klucz ani metoda szyfrowania użyte do utajnienia danych osobowych. Nawet instrukcje kancelaryjne nie wspominają o takich szczegółach.

Do dziś Instytut Zachodni nie posiadał wiedzy o metodzie i kluczu zaszyfrowanych danych. Prof. Maria Rutowska odpowiadając w 2014 r. na pytanie dziennikarza „Gazety Wyborczej” Piotra Bojarskiego („Czy uda się też odszyfrować dane personalne

[1] Por. m.in. E. Serwański, I. Trawińska, *Zbrodnia niemiecka w Warszawie. 1944 r. Zeznania-zdjęcia*, Documenta Occupationis t. II, Poznań 1946; E. Serwański, *Dulag 121 – Pruszków: sierpień-październik 1944 roku*, Poznań 1946; E. Serwański, *Życie w powstańczej Warszawie: sierpień-wrzesień 1944. Relacje, dokumenty*, Warszawa 1965.

osób, które opowiedziały swoje historie w ankiecie?"), stwierdziła wówczas: „Nie mamy niestety żadnego klucza do szyfrów stosowanych przez ankieterów"[2].

To oznaczało, że część informacji zawartych w ankietach pozostała nieznana, a badacze byli zmuszeni do tego, by polegać jedynie na informacjach już uprzednio odszyfrowanych i podanych jawnym tekstem przez autora *Zbrodni niemieckiej w Warszawie*.

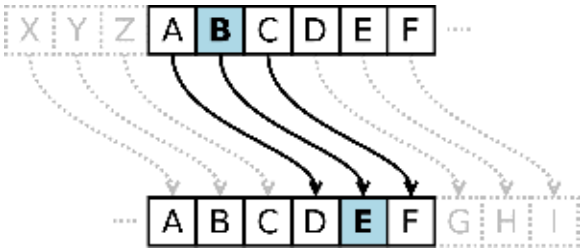
Wybrane klasyczne metody szyfrowania

Spośród naprawdę wielu metod szyfrowania (nawet tych najprostszych) zostaną tutaj omówione jedynie te oparte na ideach przydatnych podczas opisu szyfru z akcji „Iskra-Dog" i dlatego warto je poznać bliżej. Są to proste szyfry, jednak ciekawe również z perspektywy historycznej. Ich opisy są powszechnie dostępne, dlatego nie podano tutaj źródeł (z wyjątkiem rysunków skopiowanych, a nie utworzonych przez autora). Do każdej metody podano przykład.

Szyfr Cezara

Szyfr Cezara to prosty monoalfabetyczny szyfr podstawieniowy, który zastępuje każdą literę tekstu jawnego inną literą alfabetu. Jego nazwa pochodzi od Juliusza Gajusza Cezara (100 p.n.e. - 44 p.n.e.), który używał go w korespondencji. Jest to jeden z najprostszych szyfrów tego typu.

Każda litera tekstu jawnego jest zastępowana inną literą, która jest od niej oddalona o stałą liczbę pozycji w alfabecie. Jeśli algorytm wskazywałby na pozycję, która wychodzi poza ostatnią literę w alfabecie, to przechodzi się na początek alfabetu.



1. (rys. za Wikipedia3)

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

[2] P. Bojarski, *Szyfrowane powstańcze teczki. Sprzed 70. lat*, „Gazeta Wyborcza" 29.07.2014, https://poznan.wyborcza.pl/poznan/1,36001,16392915,Szyfrowane_powstancze_teczki__Sprzed_70__lat.html (dostęp: 1.12.2020)
[3] Por. https://pl.wikipedia.org/wiki/Szyfr_Cezara (dostęp: 31.12.2021).

Zatem wyraz ISKRA byłby tutaj zaszyfrowany do postaci: LVNUD

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

Szyfr Trithemiusa

Autorem tego szyfru jest niemiecki mnich Trithemius, żyjący na przełomie XV i XVI w. Jest to modyfikacja szyfru Cezara, w której kolejne litery tekstu jawnego są kodowane z użyciem innego alfabetu, przesuniętego o kolejną literę względem oryginalnego alfabetu. Zatem jest to jeden z pierwszych szyfrów polialfabetycznych.

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

2. Wzorcem dla przesuwanych kolejno alfabetów jest tzw. „tabula recta” (powyżej)

Każda kolejna litera tekstu jawnego jest kodowana przez kolejny wiersz tej tablicy. Po osiągnięciu 26 wiersza następuje powrót do 1 wiersza (wiersz 1 nie jest przesunięty w stosunku do oryginalnego alfabetu).

Zatem wyraz ISKRA byłby tutaj zaszyfrowany do postaci: ITMUE

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

Szyfr Vigenère'a

Jest to modyfikacja szyfru Trithemiusa, w której używa się jedynie wybranych wierszy z tablicy „tabula recta” – zatem kolejne litery tekstu jawnego NIE SĄ tutaj kodowane wg kolejnych przesunięć alfabetu. Wiersze, które są wybrane do szyfrowania, określa ustalone słowo kluczowe. Kolejne litery tego słowa wskazują wiersze konieczne do zakodowania wiadomości. Praktycznie jest zapisać litery słowa kluczowego pod literami wiadomości. Szyfr Viegenère’a przez długi czas uchodził za nieodszyfrowywalny. Złamany został dopiero przez brytyjskiego uczonego Ch. Babbage’a w XIX w.

Jeśli słowem kluczowym jest OJCZYZNA, to wiadomość „AKCJAISKRADOG” będzie miała niejawną postać: OTEIYHFKFJFNE

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

jawny	A	K	C	J	A	I	S	K	R	A	D	O	G
klucz	O	J	C	Z	Y	Z	N	A	O	J	C	Z	Y
zakodowany	O	T	E	I	Y	H	F	K	F	J	F	N	E

Szachownica Polibiusza

Kolejny z wybranych szyfrów wprowadza w końcu ideę używania cyfr zamiast liter. Jest to jedynie przykład szyfru (monoalfabetycznego) z grupy bardzo wielu szyfrów kodujących tekst do postaci cyfrowej. Zarazem klasyczny przykład idei wykorzystywanej w wielu innych metodach szyfrowania. Idea opiera się na rozpisaniu 26 liter alfabetu łacińskiego (przy wpisaniu I oraz J w to samo pole) na pola tablicy 5x5:

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

Ta idea pozwala przedstawić każdą literę alfabetu w postaci „współrzędnych", np. G to 22. Wówczas tekst zakodowany (niejawny) ma dwie cechy: ma zawsze parzystą długość oraz składa się z par cyfr od 1 do 5.

Zatem wyraz ISKRA byłby tutaj zaszyfrowany do postaci: 2443254211

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

Po wprowadzeniu dodatkowych utrudnień kryptoanalitycznych tablicę Polibiusza wykorzystała podczas I wojny światowej m.in. niemiecka armia przy konstruowaniu systemów ADFGX oraz ADFGVX. Istnieje wiele wariantów tego szyfru opartych na takiej lub podobnej tablicy. Jeden z nich („z rozwidleniem") był częścią kilku najsłynniejszych radzieckich szyfrów z połowy XX w., m.in. szyfru używanego przez Rote Kapelle, szyfru Ramsaya i szyfru VIC – najdoskonalszego szyfru ręcznego w historii kryptologii.

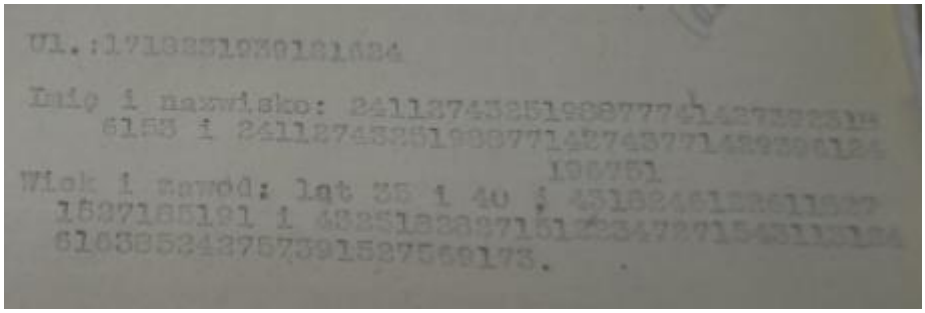
Odkrywanie metody i klucza szyfrowania w protokołach akcji „Iskra-Dog"

Wstępne analizy

Współczesny czytelnik materiałów akcji „Iskra-Dog" zamiast danych osobowych czy adresowych widzi jedynie szereg cyfr, jak na przykład:

21726145771571227734266174196791 (32 cyfry)

Przykładowy nagłówek dokumentu wygląda więc następująco:



Jak wspomniano na wstępie, odnalezienie znaczenia poszczególnych tekstów niejawnych w treści protokołów nie przedstawia – jak się okazuje – większego problemu.

Istnieje bowiem całkiem duża część takich tekstów, które zostały rozkodowane przez inicjatora i uczestników akcji „Iskra-Dog" podczas opracowania protokołów dla celów publikacji po wojnie. Dysponując licznym zbiorem par „tekst niejawny – tekst jawny" łatwo zauważyć, że długość tekstu niejawnego jest zawsze dwukrotnością długości tekstu jawnego.

Zatem można postawić hipotezę, że każda para cyfr odpowiada jakiejś literze alfabetu. Mając w dyspozycji odpowiednio liczny zestaw tekstów niejawnych i odpowiadających im tekstów rozkodowanych można odtworzyć hipotetyczny alfabet i następnie zweryfikować hipotezę, stosując ten alfabet do innych tekstów (jawnych i niejawnych). Jeśli weryfikacja przebiegnie pozytywnie, to można użyć „alfabetu" do wszystkich tekstów (również tych dotąd nierozkodowanych).

Istotnie, po analizie danych o imieniu i nazwisku z nagłówków zaledwie ośmiu (sic!) przykładowych protokołów (w tych przypadkach dzięki zapiskom na dokumentach są dostępne dane w formie jawnej) można sporządzić następującą tabelę mapującą pary cyfr na litery alfabetu:

Nr teczki	Nr protokołu	imie i nazwisko niejawnie	imie i nazwisko jawnie	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
I.Z.Dok.V-223/5	215	217261457715712277342661741967 91	STEFANSTASZEWSKI	21	72	61	45	77	15	71	22	77	34	26	61	74	19	67	91		
				S	T	E	F	A	N	S	T	A	S	Z	E	W	S	K	I		
I.Z.Dok.V-223/5	229	682788675737886727	LASKOWSKA	68	27	88	67	57	37	88	67	27									
				L	A	S	K	O	W	S	K	A									
I.Z.Dok.V-223/1	503	67361816747181772451885427247 7	KUROWSKAWISLAWA	67	36	18	16	74	71	81	77	24	51	88	54	27	24	77			
				K	U	R	O	W	S	K	A	W	I	S	L	A	W	A			
I.Z.Dok.V-223/2	172	145118161913272477294727494344421277	MIROSLAWACHAJDECKA	14	51	18	16	19	13	27	24	77	29	47	27	49	43	44	42	12	77
				M	I	R	O	S	L	A	W	A	C	H	A	J	D	E	C	K	A

Z powyższego można zestawić litery alfabetu i odpowiadające im pary cyfr. Już na podstawie zaledwie tych 8 tekstów można wskazać 35 par cyfr wraz z odpowiadającymi im literami. Warto zauważyć, że dana litera może być kodowana przez kilka par cyfr, bowiem liter w alfabecie łacińskim jest 26, zaś liczb dwucyfrowych jest 90. Osobna kwestia to pytanie o faktycznie używany tutaj alfabet – polskie litery, litery Q, X, Y etc.

Dodatkowo pobieżna analiza kilkunastu protokołów wykazała, że nie występuje w tych kodach liczba 0, a to zmniejsza liczbę możliwych par cyfr do 81. Z tego wynika, że posiadanie zaledwie 8 rozkodowanych szyfrów pozwalałoby poznać znaczenie niemal połowy (35) możliwych par cyfr (oczywiście zakładając, że ten szyfr jest prosty i że pozwala przyjąć stałe przypisanie par cyfr do poszczególnych liter alfabetu).

A	B	C	D	E	F	G	H	I	J	J	K	L	M	N	O	P	R	S	T	U	W	Y	Z
77		29	43	61	45		47	91		49	67	68	14	15	57		18	21	72	36	74		26
27		42		44				51			81	54			16			71	22		37		
											12	13						34			24		
																		19					
																		88					

Zatem z takim hipotetycznym „alfabetem" można próbować deszyfrować pozostałe teksty i zweryfikować tę hipotezę.

Jednak nawet jeśli takie przyporządkowanie okaże się skuteczne i umożliwi odkodowanie szyfrów, to niestety takie podejście nie pozwala odtworzyć metody ani klucza użytych do zaszyfrowania tekstów.

Dalsza analiza dostępnych w protokołach niejawnych tekstów pokazała, że wszystkie teksty niejawne (z wyjątkiem pojedynczych przypadków, które być może są błędami w zapisie) mają parzystą długość i składają się wyłącznie z cyfr od 1 do 9. Te cechy przypominają charakterystyczne elementy szachownicy Polibiusza.

SANATORIUM, czyli jak szyfrowano w AK

Jak wspomniano, bardzo wiele metod szyfrowania daje w wyniku ciąg cyfr. I często nie są to szyfry tak proste do złamania, jak zwykła szachownica Polibiusza. Wobec dużego wyboru różnych metod warto zatem uwzględnić okoliczności inne niż tylko struktura samego szyfru.

W ramach akcji „Iskra-Dog" szyfr był używany w bardzo trudnych warunkach z ograniczonym zasobem materiałowym. Dlatego musiał być stosunkowo prosty w użyciu. Był również używany w środowisku zaangażowanym w konspirację. Chociaż bowiem akcja „Iskra-Dog" nie była typową akcją AK, była jednak cywilną inicjatywą dokumentacyjną prowadzoną przez członków podziemnej organizacji „Ojczyzna".

Dlatego wyjaśniając szyfry akcji „Iskra-Dog", warto szukać analogii wśród metod szyfrowania używanych przez AK. Niestety na ten temat istnieje stosunkowo niewiele źródeł. Ten fakt nie zaskakuje, jeśli wziąć pod uwagę, że podstawowe zasady postępowania w przypadku ewakuacji komórki AK przewidywały zniszczenie w pierwszej kolejności instrukcji kancelaryjnych (w tym instrukcji szyfrowania informacji). Dostępna literatura[4] wskazuje nawet, że istniały regulaminy AK zakazujące pisemnych instrukcji: „*według zasad przyjętych w kryptografii nie powinno się wydawać na piśmie instrukcji, dotyczących systemu szyfru. Instruowanie powinno się odbywać* ***wyłącznie w drodze osobistego kontaktu***"[5].

Oczywiście na różnych odcinkach i na różnych szczeblach działalności AK korzystano z metod szyfrowania o różnym stopniu trudności i złożoności. Akcja „Iskra-Dog" nie dotyczyła kierowniczych szczebli konspiracji ani nie była misją wywiadu cywilnego

[4] M. Jedynak, *Zasady stosowania kryptonimów i szyfrów w korespondencji służbowej Okręgu Radomsko-Kieleckiego AK (1943/1944 r.)*, „Przegląd Historyczno-Wojskowy" 2016, R. XVIII (LXVIII), nr 4 (258), s. 73-98

[5] Za: M. Jedynak, *op. cit.*, s. 79; Centralne Archiwum Wojskowe, WBBH, IX.3.22.40, Instrukcja do szyfru „Lombard" [odpis], b.m., b.d., k. 1.

itp. – była inicjatywą, w której nie było potrzeby (ani możliwości!) wykorzystywania wyrafinowanych metod szyfrowania.

W literaturze opisano szyfr używany w takich przypadkach przez AK. Mimo, iż *„każdy obszar i okręg AK korzystał z własnych kluczy szyfrujących i tabel kryptonimów, co dodatkowo utrudniało rozpracowanie poszczególnych struktur konspiracyjnych”*[6], to jednak poznanie tego konkretnie szyfru jest inspirujące i pozwala sprawdzać kolejne hipotezy na temat szyfrowania w akcji „Iskra-Dog”.

Używany w Okręgu Radomsko-Kieleckim AK szyfr „SANATORIUM” był *„stosunkowo prosty, ale uniemożliwiał w warunkach polowych deszyfrację wiadomości. W zupełności wystarczał do szybkiego przekazywania wiadomości, stąd też zazwyczaj wykorzystywany był od struktury okręgu w dół”*[7]. Marek Jedynak w swym artykule tak opisał działanie tego szyfru: *„Nazwa własna kodu stanowiła jednocześnie klucz do niego. Słowo „Sanatorium” wpisywane było po przekątnej (z górnego lewego do dolnego prawego rogu) w tabelę o długości i szerokości liter. Następnie uzupełniano ją danymi w rzędach tak, aby kolejne litery alfabetu zgrywały się z wpisanym hasłem. Poszczególne litery mogły więc w tabeli być zapisane kilkakrotnie, co pozwalało na zwiększenie kombinacji dla powtarzających się znaków. Szyfrowanie polegało na wybraniu litery (jak w popularnej grze „w statki”), a następnie zapisaniu jej w postaci dwóch cyfr (rzędnej i odciętej). Odczytywanie następowało w sposób odwrotny, poprzez odnalezienie w kolumnach i wierszach zastosowanych liczb i wskazanie odpowiedniej litery”* [8].

[6] M. Jedynak, *op.cit.*, s.74.
[7] M. Jedynak, *op.cit.*, s.79.
[8] M. Jedynak, *op.cit.*, s.79.

Nr 3
1943 sierpień, [b.m.] – Klucz do szyfru „Sanatorium"

	1	2	3	4	5	6	7	8	9	0
1	S	t	u	w	y	z	ż	.	a	b
2	.	A	b	c	d	e	f	g	h	i
3	ł	m	N	o	p	r	s	t	u	w
4	z	ż	.	A	b	c	d	e	f	g
5	o	p	r	s	T	u	w	y	z	ż
6	k	l	ł	m	n	O	p	r	s	t
7	l	ł	m	n	o	p	R	s	t	u
8	b	c	d	e	f	g	h	I	j	k
9	ł	m	n	o	p	r	s	t	U	w
0	d	e	f	g	h	i	j	k	l	M
	1	2	3	4	5	6	7	8	9	0

Źródło: AIPN Ki, WUSW Kielce, 015/170, t. 2, k. 104/3, [oryginał], rkps.

3. Klucz do szyfru Sanatorium[9]

Opisana zasada wskazuje, że szyfr ma cechy szyfrów polialfabetycznych – kolejne wiersze są przesuniętym alfabetem, jak w metodzie Trithemius'a czy Vigenère'a. Przesunięcie kolejnych wierszy wyznacza słowo kluczowe wpisane na przekątnej. Jak widać, używano skróconego (bez ą, ę, ć, ń, ó, ś, x, ź, ale z ł, ż) alfabetu polskiego (a nie łacińskiego) z dodanym znakiem „.". Natomiast metoda zapisywania „współrzędnych" przypomina szachownicę Polibiusza.

Co więcej, przeznaczenie tego szyfru przypomina cele w akcji „Iskra-Dog": „*Korzystając z szyfru „Sanatorium", m.in. zostały utajnione informacje dla oddziału dywersyjnego Obwodu AK Końskie. Ciąg liczb skrywał dane osoby przewodnika, a także hasło, odzew i kontrodzew, które miały zostać użyte w chwili nawiązania kontaktu w celu wykonania powierzonego oddziałowi zadania*" (s.79).

[9] M. Jedynak, *op.cit.*, s. 94.

Nr 4

1943 sierpień 5, [b.m.] – Wiadomość zakodowana z wykorzystaniem szyfru „Sanatorium".

Ad. Nr 165 Niemen[45] 5 VIII [19]43 [r.]

Kontakt dla dyw[ersji] obwodu – przewodnik.

75, 96, 28, 44, 65, 20, 37, 79, 19, 21, 93, 06, 84, 61, 91, 22, 74, 25, 56, 17, 58.[46]
hasło: 95, 36, 66, 54, 16, 48, 92, 84, 98, 68, 15, 61, 26, 39, 77, 66, 25, 59, 84, 33, 06, 19.[47]
odzew: 82, 16, 58, 43, 12, 34, 21, 76, 20, 71, 33, 26.[48]
kontrodzew: 66, 47, 20, 84, 17, 83, 50, 22, 00, 41, 19, 68, 44, 59, 21.[49]

4. Przykład szyfrogramu[10]

Powyższy przykład pokazuje, że zakodowane w Kielcach wiadomości bardzo przypominają teksty z protokołów zebranych pod Warszawą.

Metoda i klucz szyfrowania w protokołach akcji „Iskra-Dog"

Niestety słowo SANATORIUM ma 10 znaków – zatem „nie pasuje" do szyfrów zebranych w akcji „Iskra-Dog" (które nie zawierają liczby 0). Jednak informacja o stosowaniu w AK tego typu szyfrowania i to w celu kodowania nazwisk etc. pozwala postawić hipotezę, że podczas akcji „Iskra-Dog" także używano jakiegoś polialfabetycznego szyfru typu tablicowego (z tym, że tablica musi mieć wymiary 9x9).

Pozostaje zatem odszukać słowo kluczowe oraz ustalić używany alfabet.

W tym celu dostępne (patrz powyżej) z 8 protokołów dane o mapowaniu 35 dwucyfrowych liczb na litery alfabetu warto wpisać w tablicę o wymiarach 9x9:

	1	2	3	4	5	6	7	8	9
1		K	L	M	N	O		R	S
2	S	T		W		Z	A		C
3				S		U	W		
4		C	D	E	F		H		J
5	I			L			O		
6	E						K	L	
7	S	T		W			A		
8	K							S	
9	I								

[10] M. Jedynak, *op.cit.*, s. 95.

Przyjmując, że tablica zawiera przesunięty w wierszach alfabet, łatwo uzupełnić brakujące pola, zaczynając od pierwszego wiersza (dzięki dość gęstemu wypełnieniu wierszy 1 oraz 4):

	1	2	3	4	5	6	7	8	9
1	J	K	L	M	N	O	P	R	S
2	S	T	U	W		Z	A	B	C
3	O	P	R	S	T	U	W		Z
4	B	C	D	E	F	G	H	I	J
5	I	J	K	L	M	N	O	P	R
6	E	F	G	H	I	J	K	L	M
7	S	T	U	W		Z	A	B	C
8	K	L	M	N	O	P	R	S	T
9	I	J	K	L	M	N	O	P	R

Niepewne jest tylko znaczenie pola między W a Z – można tu bowiem wpisać X lub Y. Lecz to jest już bardzo proste do weryfikacji podczas deszyfracji (z przeprowadzonych dotąd prac wynika, że należy tu wpisać literę Y).

Wypełniona w ten sposób tablica odsłania też użyty **klucz**, który – jak się okazuje – nie został umieszczony na przekątnej (jak w przypadku szyfru „SANATORIUM"), lecz w pierwszej kolumnie i brzmi:

JSOBIESKI

	1	2	3	4	5	6	7	8	9
1	**J**	K	L	M	N	O	P	R	S
2	**S**	T	U	W		Z	A	B	C
3	**O**	P	R	S	T	U	W		Z
4	**B**	C	D	E	F	G	H	I	J
5	**I**	J	K	L	M	N	O	P	R
6	**E**	F	G	H	I	J	K	L	M
7	**S**	T	U	W		Z	A	B	C
8	**K**	L	M	N	O	P	R	S	T
9	**I**	J	K	L	M	N	O	P	R

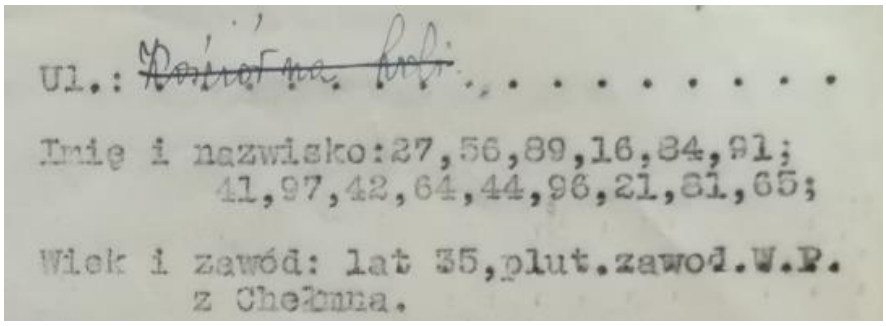
Nowe informacje odkryte w protokołach akcji „Iskra-Dog" – przykłady

Spośród ponad 300 ankiet wiele zostało odszyfrowanych i opublikowanych. Niemniej niektóre protokoły nie zostały opublikowane w całości (pozostawiono niejawne fragmenty). Organizację procesu zbierania i opracowania protokołów opisał Edward Serwański we wstępach do swych trzech książek, a także w artykule z okazji 40. rocznicy Powstania Warszawskiego[11]. Niestety w żadnej z tych publikacji nie opisał dokładniej sposobu szyfrowania.

Autor niniejszego opracowania przeanalizował 284 protokoły przechowywane w teczkach Archiwum IZ. Analiza miała przede wszystkim doprowadzić do odkrycia metody i klucza szyfrowania. Gdy to zadanie osiągnięto, przystąpiono do odszyfrowania wszystkich fragmentów utajnionych (także tych, które uprzednio były ujawnione przez prof. Serwańskiego – aby potwierdzić poprawność odtworzonej metody).

Przedstawione poniżej wybrane przykłady służą jedynie ukazaniu użyteczności poznania mechanizmu szyfrowania. Poza tym jednak poniższe protokoły uzupełnione o dane osobowe pozwalają zidentyfikować konkretnych ludzi i przypominają, że są świadectwem życia konkretnych osób, o konkretnej historii… Przy każdym z tych protokołów niejako pojawia się i odkrywa po latach twarz człowieka – podmiotu danej relacji.

Protokół nr 8 – nie został opublikowany w żadnym ze zbiorów. Jest to relacja o wydarzeniach w kościele na Woli, gdy to 8 sierpnia Niemcy nakazali 3 osobom znającym język niemiecki przedarcie się przez linie walk i powrót z relacją. W razie ich ucieczki Niemcy zagrozili rozstrzelaniem 100 osób z zatrzymanych w kościele cywilów. Na protokole brak jawnego tekstu z danymi osoby zeznającej:


Ul.: [illegible]

Imię i nazwisko: 27,56,89,16,84,91;
41,97,42,64,44,96,21,81,65;

Wiek i zawód: lat 35, plut. zawod. W.P.
z Chełmna.

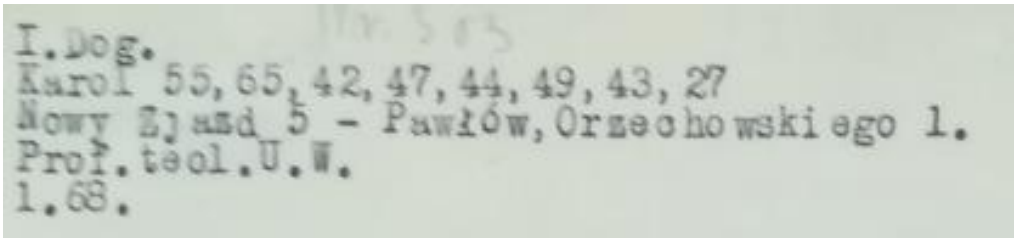
Odkryty mechanizm szyfru pozwala odczytać imię i nazwisko:

27568916849141974264449621816 5 to ANTONIBOCHENSKI

[11] E. Serwański, *Akcja „Iskra-Dog". Z badań nad dziejami Powstania Warszawskiego – 1944*, „Życie i Myśl" nr 7/8, 1985.

Chodzi oczywiście o znanego księgarza Antoniego Bocheńskiego „Mariana" (1910-1994), pracownika Księgarni św. Wojciecha, którego inne zeznanie zostało opublikowane w „Życiu w powstańczej Warszawie" (protokół nr 9).

Protokół nr 303 – to przykład ujawnienia danych osoby, która nie pojawia się w innych protokołach, a jej nazwisko nie było ujawnione nawet w formie odręcznej notatki na protokołach. Karol Michejda (1880-1945), którego nazwisko kryje się za szyfrogramem 5565424744494327, to zasłużony dla zachowania polskości na Ziemi Cieszyńskiej duchowny luterański i profesor teologii ewangelickiej. Wykładał na Uniwersytecie Warszawskim, gdzie pełnił między innymi funkcję kierownika Katedry Teologii Praktycznej i dziekana Wydziału Teologii Ewangelickiej UW. Wkrótce po wojnie zmarł w Wiśle.


I.Dog.
Karol 55,65,42,47,44,49,43,27
Nowy Zjazd 5 - Pawłów, Orzechowskiego 1.
Prof.teol.U.W.
1.68.

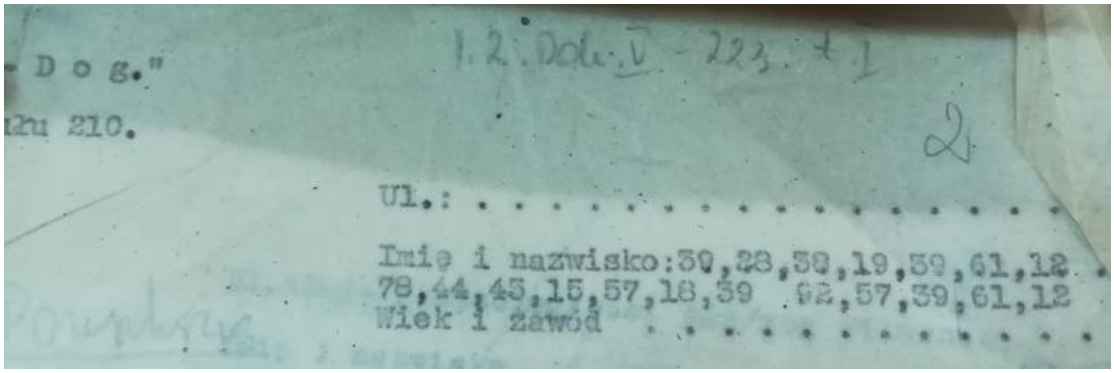
Protokół nr 266 – to także przykład ujawnienia danych wcześniej niepublikowanych i nierozkodowanych. W publikacji jest jedynie opis: „świadek kobieta lat 60, żona emer. urzędnika Miejsk. Tow. Kredytowego". Tymczasem po rozkodowaniu szyfrogramu 1427189177161827565737195327 ujawnia się nazwisko MARIAORANOWSKA. W treści protokołu pojawia się wzruszająca apostrofa: „Kochanemu mężowi Józefowi Oranowskiemu", przy czym imię i nazwisko męża jest w zeznaniu podane szyfrem.

Ponad rok później, w 1946 r. M. Oranowska opisała swoje przeżycia także w liście do Komisji Badania Zbrodni Niemieckich[12], rozpaczliwie błagając Komisję „*o pomoc w dowiedzeniu się o losie mego męża Seweryna Józefa Oranowskiego (lat 70) byłego urzędnika Towarzystwa Kredytowego Miejskiego Działu Kontroli, ostatnio emeryta, odznaczonego Złotym Krzyżem Zasługi za sprawy społeczne, a którego razem ze mną i szwagrem Adamem Chamskim wypędzili 4 sierpnia 1944 roku z ul. 6 Sierpnia 18 m. 3, jak również i wszystkich lokatorów całego domu, a w alei Szucha na gestapo oddzielili mężczyzn*". Niestety mąż – jak się zdaje – zginął jeszcze podczas Powstania.

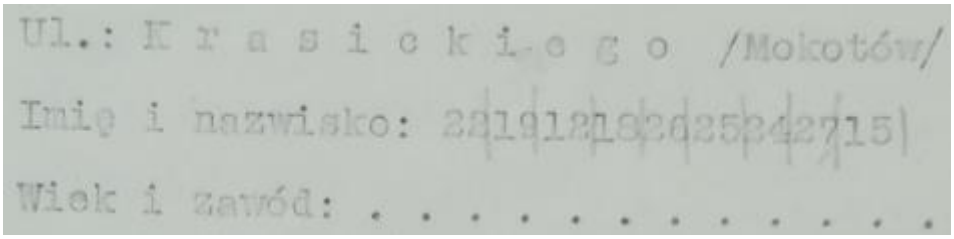
Protokół nr 210 – nie został opublikowany w żadnym ze zbiorów. Nie zachowała się choćby odręczna notatka z jawnym imieniem i nazwiskiem. Po odszyfrowaniu zidentyfikowano osobę zeznającą: Zbyszko Bednorz (1913-2010) pseud. „Józek", pisarz i

[12] Maria Oranowska, Miasto skazana na śmierć, relacja dostępna na stronie: www.zapisyterroru.pl.

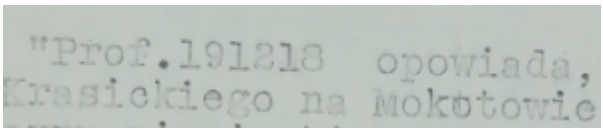
publicysta, pracownik Delegatury Rządu na Kraj i współpracownik Zygmunta Wojciechowskiego, honorowy profesor Uniwersytetu Opolskiego. Opisał po latach swe wspomnienia w książce *Lata krecie i orłowe*.



Protokół nr 127 – relacja osoby o zaszyfrowanym nazwisku o bezczelnych i bezdusznych rabunkach dokonanych na jego rodzinie przez niemieckich żołnierzy. Po rozszyfrowaniu imię i nazwisko brzmi: TSKRZYWAN.



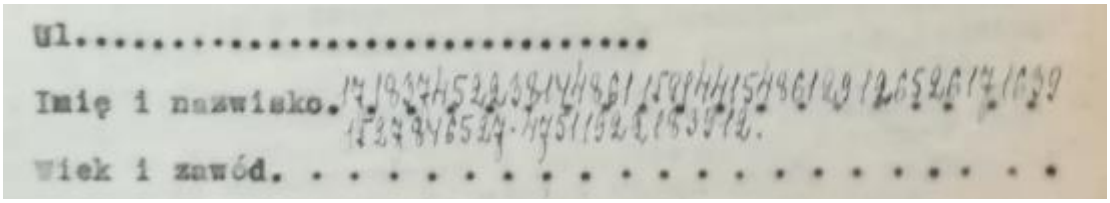
W tekście występuje jedynie forma „prof.” przed zaszyfrowanymi kilkoma literami nazwiska ([SKR]).



Identyfikacja tej osoby była trudna z uwagi na literę T w odszyfrowanych danych osobowych. W tekście jest mowa o tym, że rodzina została wygnana z domu przy ul. Krasickiego. Z innych relacji powstańczych[13] wiemy, że przy tej ulicy mieszkał prof. SGH Stanisław Skrzywan (1902-1971). Zatem litera T jest zapewne pomyłką lub podczas szyfrowania pominięto poprzedzające ją S (wówczas byłby to skrót „ST” od „Stanisław”). Prof. Skrzywan był wybitnym ekspertem z dziedziny ekonomii i rachunkowości – tym bardziej ponuro i niemal ironicznie brzmi jego relacja w protokole o „odkupieniu” od niego przez niemieckich żołnierzy kilku złotych monet o wartości 100 tys. zł za niecałe 20 tys. zł.

[13] „Kwaterowaliśmy na ulicy Krasickiego 25 u profesora Skrzywana. To był profesor SGH.” Zob. https://www.1944.pl/archiwum-historii-mowionej/tadeusz-jaroszewski,610.html (dostęp: 30.12.2020).

Protokół nr 45 – nie został opublikowany w żadnym ze zbiorów. Zawiera opis szkód, jakie barbarzyńskie działania okupanta wyrządziły dla polskiej kultury narodowej. Dane osobowe nie były nigdy rozszyfrowane (nie zapisano nigdzie w jawnej postaci nazwisk występujących w tym protokole). Ich odszyfrowanie stało się możliwe po odkryciu metody i klucza szyfrowania (choć wiele z osób, które tu wymieniono, występuje w innych protokołach). W nagłówku zaszyfrowano nazwisko profesora Tymienieckiego:


Ul.....
Imię i nazwisko.
Wiek i zawód. . . . . .

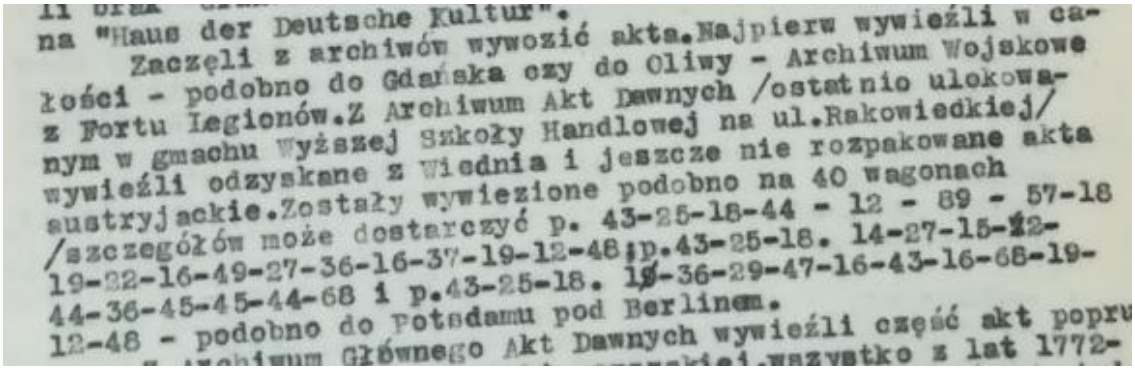
Jest to zarazem dobry przykład błędów w szyfrowaniu, jakie musiały się zdarzyć w tak trudnych warunkach konspiracji. Bowiem powyższy szyfr po odkodowaniu przedstawia się następująco (kolorem czerwonym oznaczono literówki, poszczególne wyrazy oddzielono spacjami, których nie ma w oryginale):

PRWF TYMIENIENIECKI Z POZNANIA HISTRZK

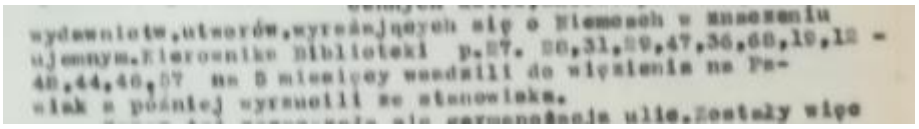
Ten protokół zawiera także sporo danych w treści dokumentu (nie tylko w nagłówku).

Poniżej zacytowano te fragmenty, w których w nawiasach kwadratowych podano odkodowaną formę nazwisk zaszyfrowanych w protokole:

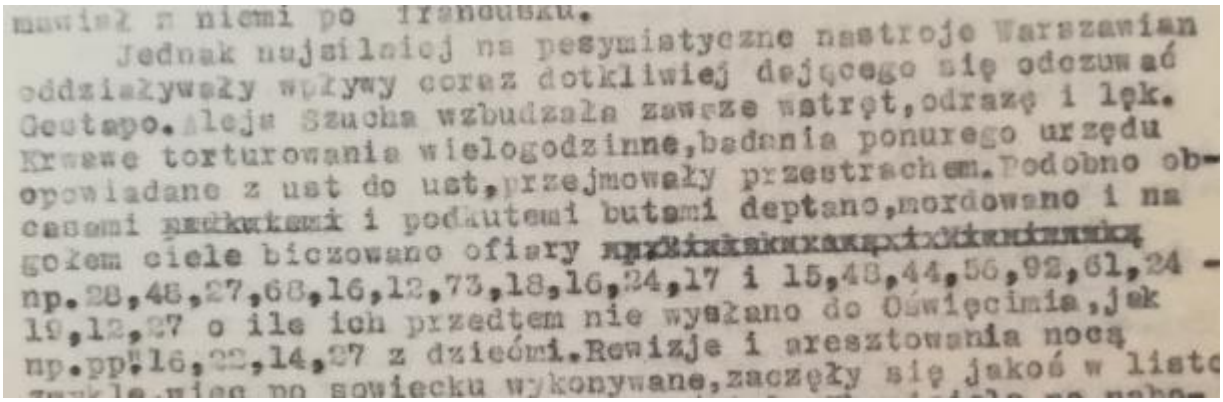
- „szczegółów może dostarczyć p.[DYREKTORSTOJAUOWSKI] , p.[DYRMANTEUFFEL] i p.[DYRSUCHODOLSKI]– podobno do Potsdamu pod Berlinem”.


na "Haus der Deutsche Kultur".
Zaczęli z archiwów wywozić akta.Najpierw wywieźli w ca-
łości - podobno do Gdańska czy do Oliwy - Archiwum Wojskowe
z Fortu Legionów.Z Archiwum Akt Dawnych /ostatnio ulokowa-
nym w gmachu Wyższej Szkoły Handlowej na ul.Rakowiedkiej/
wywieźli odzyskane z Wiednia i jeszcze nie rozpakowane akta
austryjackie.Zostały wywiezione podobno na 40 wagonach
/szczegółów może dostarczyć p. 43-25-18-44 - 12 - 89 - 57-18
19-22-16-49-27-36-16-37-19-12-48 ;p.43-25-18. 14-27-15-12-
44-36-45-45-44-68 i p.43-25-18. 19-36-29-47-16-43-16-68-19-
12-48 - podobno do Potsdamu pod Berlinem.
Głównego Akt Dawnych wywieźli część akt popru
Warto zauważyć, że nazwisko dyrektora Stojanowskiego jest zapisane błędnie jako STOJAUOWSKI (bowiem chodzi najprawdopodobniej o Józefa Stojanowskiego (1884-1964), dyrektora Archiwum Wojskowego). Wymienia też Tadeusza Manteuffla (1902-1970), późniejszego dyrektora Instytutu Historii PAN oraz Witolda Suchodolskiego (1887-1967), dyrektora Archiwów Państwowych.
- „Kierownika Biblioteki p.[ABOCHULSKIEGO] na 5 miesięcy wsadzili do więzienia”. W tym zdaniu mowa o zasłużonym archiwiście Aleksym Bochulskim

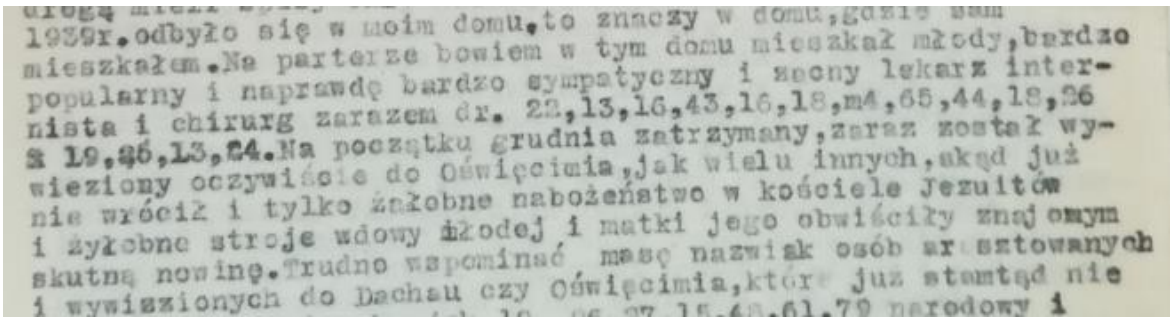
(1893-1951), dyrektorze Biblioteki Publicznej m.st. Warszawy przy ul. Koszykowej.



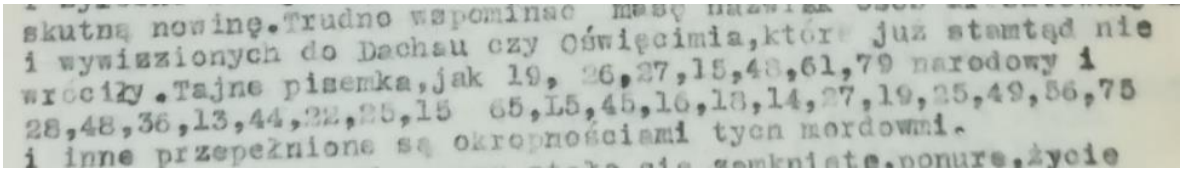
- „biczowano ofiary, np.[BIALOKUROWP] i [NIENJEWSKA], o ile ich przedtem nie wysłano do Oświęcimia, jak np. pp.[OTMA] z dziećmi". Nazwisko Anny Białokurowej (1897-1942), polonistki zamęczonej na Pawiaku, zapisano z błędem jako BIALOKUROW**P**. Obok niej wymienia się Halinę Nieniewską (1890-1942), także nauczycielkę zaangażowaną w KG ZWZ-AK, zamordowaną podczas przesłuchań na Pawiaku i w al. Szucha. Nie udało się zidentyfikować nazwiska (?) OTMA.



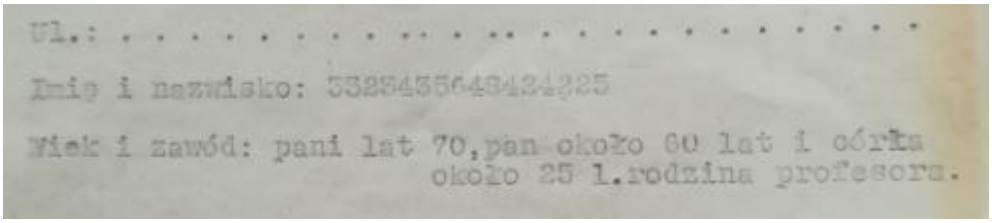
- „zacny lekarz internista i chirurg zarazem dr.[TLODORIERZSYLW]".
Ta część zawiera zapewne błąd w szyfrowaniu – możliwe warianty to np. TEODOR? WIERZ...?



- „Tajne pisemka, jak [SZANIEC] narodowy i [BIULETYN INFORMACYJNY] i inne przepełnione są okropnościami tych mordowni".



Protokół nr 134 – nie został opublikowany w żadnym ze zbiorów. Zawiera zeznania rodziny profesora Rudnickiego. Nazwisko „RUDNICCY" nie pojawia się tam w formie jawnej – jest zaszyfrowane, jak widać poniżej:

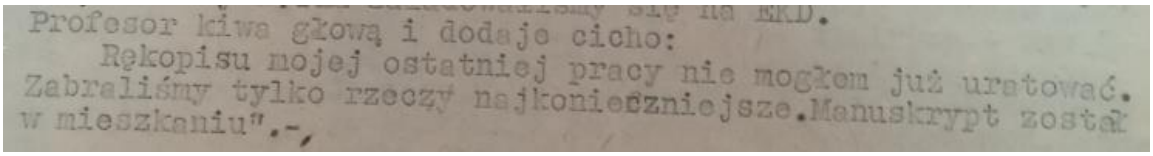

Ul.: . . . . . .
Imię i nazwisko: 33284356484242
Wiek i zawód: pani lat 70, pan około 60 lat i córka około 25 l. rodzina profesora.

Najpewniej chodzi tutaj o profesora Mikołaja Rudnickiego (1881-1978), wybitnego językoznawcę i współzałożyciela Uniwersytetu Poznańskiego, który podczas okupacji był m.in. wykładowcą Tajnego Uniwersytetu Ziem Zachodnich oraz członkiem Instytutu Zachodniego.

Dokument opisuje bardzo trudne warunki życia tej rodziny i okoliczności ich ewakuacji po upadku Powstania. Sytuacja mocno odbiła się na kondycji zdrowotnej państwa Rudnickich, o czym świadczy m.in. fragment: „*Profesor przeraźliwie chudy, tak jak gdyby skóra obciągnięta była wprost na kościach, przysiadł osłabiony na jakimś tłomoku, na nogach ma tylko kalosze przewiązane sznurkiem*” (pisownia oryginalna).

Ten opis nie był zaszyfrowany – można go było odczytać bez przeszkód. Lecz dotąd był to opis anonimowej rodziny „jakiegoś” profesora. Zupełnie inaczej się go odbiera, gdy wiadomo kogo dokładnie dotyczy ten tekst. Dość wymownie brzmi ostanie zdanie protokołu, gdzie profesor, wybitny uczony i gorący patriota, kończy swą wypowiedź:

„*Profesor kiwa głową i dodaje cicho: Rękopisu mojej ostatniej pracy nie mogłem już uratować. Zabraliśmy tylko rzeczy najkonieczniejsze. Manuskrypt został w mieszkaniu*”.


Profesor kiwa głową i dodaje cicho:
Rękopisu mojej ostatniej pracy nie mogłem już uratować.
Zabraliśmy tylko rzeczy najkonieczniejsze. Manuskrypt został
w mieszkaniu".-

Podsumowanie

Oczywiście niniejsze opracowanie ma charakter przyczynkarski i nie ma aspiracji do pełnej analizy zagadnienia. Przynosi jednak nową wiedzę, którą udało się pozyskać o akcji „Iskra-Dog”. Jest to wiedza o sposobie szyfrowania oraz o kluczu szyfrującym. Dzięki temu udało się potwierdzić lub zweryfikować, a czasem ujawnić ukryte dotąd informacje zakodowane w nagłówkach i treści protokołów tworzonych podczas akcji „Iskra-Dog”.

Uzyskanie tej wiedzy było możliwe jedynie dzięki temu, że warunki akcji „Iskra-Dog” nie pozwalały użyć bardziej złożonych szyfrów i że nawet w tym prostym szyfrowaniu klucz okazał się stały i (co ważne) niezmienny w czasie i w różnych lokalizacjach.

Gdyby nie te okoliczności – zadanie, którego wyniki tutaj opisano, nie byłoby tak proste.

Z literatury przedmiotu w zasadzie uwzględniono jedynie artykuł Marka Jedynaka z kieleckiej delegatury IPN. Jego fragmenty były bowiem przykładem metod szyfrowania używanych w tym okresie przez AK oraz potwierdzeniem własnych hipotez autora niniejszego artykułu (oraz źródłem informacji bibliograficznych). Autor ma jednak świadomość istnienia innych (choć jak wspomniano – nielicznych) źródeł z tej tematyki[14]. Zdaniem M. Jedynaka: „W historiografii dotyczącej AK niemal nie występują prace na temat stosowania szyfrów” [15].

Być może analiza innych prac dostarczyłaby szerszego kontekstu i pomogła wyjaśnić pytania, na które ten artykuł nie odpowiada. Na przykład co do genezy klucza – dlaczego wybrano akurat taki klucz szyfrujący (JSOBIESKI)? Autor ma na ten temat hipotezy, jednak nie posiada aktualnie żadnych argumentów, które by je uzasadniały i pozwalały tutaj przytoczyć te domysły. Innym ciekawym tematem z zakresu utajniania informacji, choć już nieco wykraczającym poza dziedzinę szyfrów, jest sprawa genezy kryptonimów, np. kryptonimu akcji: „Iskra-Dog”. Tej sprawie być może zostanie poświęcony kolejny artykuł.

Krystian Sobański – mgr matematyki i teologii, przewodnik miejski po Poznaniu. Interesuje się także historią – głównie historią nauki, a zwłaszcza historią matematyki. Pracuje jako analityk danych w dużej firmie e-commerce. Podstawy szyfrowania poznał m.in. przez udział w internetowej grze lamaczeszyfrow.pl . O akcji „Iskra-Dog” dowiedział się, szukając materiałów do biografii inż. Szczepana Jeleńskiego, autora m.in. „Lilavati”, pierwszego polskiego zbioru łamigłówek i anegdot matematycznych.

[14] Por. m.in. (za M. Jedynak, *op.cit.): Krakowski Okręg Armii Krajowej w dokumentach*, t. II: *Dział Łączności Operacyjnej. Łączność radiowa (1943–1945)*, cz. 1, oprac. A. Zagórski, Kraków 1999, s. 15–144; *Kedyw Okręgu Warszawa Armii Krajowej. Dokumenty – rok 1944*, wybór i oprac. H. Rybicka, Warszawa 2009, s. 121–123, 155–156, 278–280; *Oddziały i akcje Kedywu Okręgu Warszawskiego poza Warszawą. Dokumenty z lat 1943–1944*, wybór i oprac. H. Rybicka, Warszawa 2011, s. 157–159.
[15] Za: M. Jedynak, *op.cit.*: „Autorowi udało się odnaleźć jedynie artykuł Izabeli Nowickiej-Kuczyńskiej, Szyfry i szyfrantki w SZP–ZWZ–AK [w:] Służba Polek na frontach II wojny światowej, cz. 2: Referaty i komunikaty. Materiały sesji popularnonaukowej w Toruniu w dniach 16–17 listopada 1996 roku, red. E. Zawacka, Toruń 1998, s. 169–178”.