Ihnatowicz, Ireneusz

Próba dekryptowania szyfrowanych depesz namiestnika do Aleksandra II z 1863 roku

Przegląd Historyczny 65/3, 537-544

1974

IRENEUSZ IHNATOWICZ

Próba dekryptowania szyfrowanych depesz namiestnika do Aleksandra II z 1863 roku

Wśród źródeł do dziejów powstania styczniowego przygotowywanych do druku przez zespół pod kierunkiem prof. Stefana Kieniewicza znalazło się czterdzieści kilka przeważnie krótkich szyfrowanych depesz wysłanych z Warszawy między lutym i lipcem 1863 r. do Petersburga. Mają one być ogłoszone w tomie pt. „Korespondencja namiestników Królestwa Polskiego, styczeń—sierpień 1863 r.". Teksty te uprzejmie udostępniono podpisanemu, który spróbował je dekryptować, jako że *clair* tych depesz z pewnymi wyjątkami, o których niżej, nie był znany. Wydawało się, że w przypadku udania się próby można byłoby dążyć także do odtworzenia klucza lub kodu szyfru, gdyż mógłby okazać się on przydatny w przyszłości. Jest to tym bardziej uzasadnione, że wiadomo iż istnieją dalsze podobne szyfrowane teksty, m.in. także mikrofilmowane w zbiorach IH PAN. Ponieważ jednak chwilowo zbadanie ich trzeba odłożyć, wydaje się celowe opublikowanie niniejszych wyników częściowych. Interesujące ponadto mogły okazać się niektóre cechy szyfru i sposób posługiwania się nim.

Teksty dotychczas znalezione pochodzą z Centralnego Państwowego Archiwum Wojskowo-Historycznego w Moskwie z zespołu nr 484, inwentarz nr 1, vol. 64 i dadzą się podzielić na trzy grupy. Pierwszą stanowią takie, które zawierają jedynie tekst szyfrowany bez żadnych elementów treści pisanych w sposób zwykły, clairem. Depesz takich jest 20. Do drugiej grupy należą takie, które prócz tekstu szyfrowanego zawierają także tekst pisany clairem. W kilku przypadkach są to zdania wstępne o jednakowym brzmieniu „Дома все благополучно" lub „В городе и дома все благополучно". W kilku przypadkach *clair* jest dłuższy. Dalszy ciąg depeszy stanowi tekst szyfrowany i jak się później okazało, dotyczący spraw innych niż te, o których mówi tekst pisany sposobem zwykłym. Takich depesz w części tylko szyfrowanych jest 17. Wreszcie do trzeciej grupy należy 7 depesz, które odcyfrował ich odbiorca, nie pozostawił jednakże wskazówek co do sposobu odcyfrowania, co do związku znaków clairu i kryptogramu. W tym przypadku wiadomo więc było, że treść depeszy brzmi np. „Сегодня послан адьютант мой, Ухтомский с письмом и военным журналом", i że odpowiadają temu znaki „4078, 5856, 3611, 2725, 1334, 1572, 4025, 1500, 1524, 3970, 1543, 1395, 2725, 4023, 1582, 5869, 2735, 5825, 5104, 5834, 1563, 3905". Nie było jednak wiadomo, czy 4078 odpowiada literze „C" czy sylabie „cer", czy słowu „сегодня", czy może jakiemuś innemu słowu clairu. Podobna wątpliwość dotyczyła wszystkich znaków kryptogramu; nie wiadomo też było w ogóle, czy porządek znaków clairu i kryptogramu jest ten sam.

Zbadanie tekstów szyfrowanych doprowadziło do następujących wniosków wstępnych:

1. Wszystkie znaki kryptogramu zamknąć można między liczbami 1300 i 5900. Znaczy to, że kod szyfru zawiera nie więcej niż 4600 znaków.

2. Czterocyfrowe znaki zawarte w tych granicach zaczynają się od następujących cyfr: 13, 15, 24, 27, 36, 39, 40, 42, 51, 58. Oznaczało to, że z każdego tysiąca wzięto do kodu nie więcej niż dwie setki i że wobec tego rzeczywista liczba znaków wynosi zapewne 1000.

3. Tekst został zaszyfrowany metodą podstawienia, to znaczy, że znaki kryptogramu zastępują znaki clairu nie zaś wskazują porządek ich czytania itp.

4. Liczba znaków w odcyfrowanych kryptogramach zestawiona z clairem wskazuje, że szyfr oparty jest na kodzie poligramatycznym, zawierającym zarówno pojedyncze litery, jak i sylaby, a nawet całe słowa.

5. Brak powtórzeń w kryptogramie w niektórych przypadkach, gdy w clairze występują sylaby dwukrotnie powtórzone, może oznaczać, że ta sama litera, sylaba lub słowo bywa oznaczane przy pomocy kilku różnych znaków, za każdym razem inaczej.

6. Porządek znaków kryptogramu i clairu jest ten sam.

Zestawienie rozmaitych kombinacji clairu i kryptogramu depesz odcyfrowanych przez odbiorcę (grupa trzecia) doprowadziło do ustalenia znaczenia około 80 znaków użytych w tych depeszach. Nie wszystkie znaki użyte dały się jednakże w ten sposób zidentyfikować, a działo się tak przede wszystkim w przypadku dłuższych sekwencji znaków występujących w całym zasobie kryptogramów tylko raz. Okazało się też, że kryptogramy zawierają także znaki nic nie znaczące lub zamierzone zapewne błędy szyfranta, które miały utrudnić dekryptowanie przez niepowołanego.

Dalsze postępowanie, którego omawianie ze względu na istniejące opisy metod w opracowaniach dotyczących kryptografii i ze względu na brak miejsca tutaj należałoby pominąć, doprowadziło do rezultatów przedstawionych w poniższej tabeli:

Liczba depesz szyfrowanych

Grupy pierwszej	Grupy drugiej i trzeciej (tj. takich, w których *clair* kryptogramu nie był znany)			
Całkowicie zweryfikowanych	Odczytanych całkowicie pewnie lub z małymi wątpliwościami	Odczytanych z niewielkimi lukami, nie przeszkadzającymi w rozumieniu	Odczytanych z większymi lukami pozwalającymi jednak domyśleć się treści	Odczytanych tylko w niewielkich fragmentach
7	22	6	3	6

Co zaś do odtworzenia kodu — stwierdzono, że we wszystkich depeszach użytych było 365 rodzajów znaków. Niektóre z nich powtarzały się wielokrotnie, niektóre występowały tylko raz lub dwa. W sumie licząc wraz z powtórzeniami depesze zawierają 1320 znaków. Powstało naturalnie pytanie o to, jak się to ma do całego zasobu znaków kodu, to znaczy, czy aby wśród 1000 miejsc, jakie według wstępnego wyliczenia powinien zawierać kod nie ma miejsc pustych. Inaczej mówiąc nie było pewności co do tego, czy wszystkim znakom mieszczącym się w wyliczonej na wstępie objętości kodu odpowiada zawsze jakiekolwiek znaczenie. Już

wstępne przejrzenie zidentyfikowanego zasobu znaków doprowadziło do wniosku, że istnieją w kodzie znaki w depeszach nie użyte. W dekryptowanych tekstach występują np. litera Ф, ale wyrażano ją zawsze w związku z innymi literami, np. w sylabie „Факм" lub w innych podobnych. Ponieważ przypuszczać można, że kod zawiera prócz słów i sylab także pełny alfabet i to zapewne powtórzony (co do niektórych liter stwierdzono to na podstawie kryptogramów) wskazywało to już na istnienie niezidentyfikowanej grupy znaczącej. Można było przypuszczać, a tekst depesz to potwierdził, że w kodzie są uwzględniane połączenia liter typowe dla języka rosyjskiego. Nie wszystkie jednak częste połączenia występujące w rosyjskim zostały użyte w depeszach, gdyż nie wymagał tego tekst. Można więc było spodziewać się w kodzie pewnej możliwej do przybliżonego określenia liczby znaków reprezentujących typowe połączenia liter nie użyte w kryptogramach. Kontynuując tę drogę można było upewnić się, że kod faktycznie liczy 1000 znaków i że zapewne około 50 z nich oznacza znaki przestankowe, służy do zmącenia kryptogramu, aby utrudnić jego dekryptowanie, służy jako znak rozpoznawczy szyfranta (np. 1563, 1360) itp. Znaki użyte w depeszach stanowią więc około 37% całego zasobu zawartego w kodzie. Ustalić znaczenie udało się w stosunku do 250 znaków, tj. około 1/4 całego kodu.

Nie wszystkie znaki udało się zidentyfikować z jednakową pewnością. Te z nich, które występują w depeszach tylko jeden raz i to obok innych jednorazowych (np. dwa nie powtórzone znaki oznaczające „руки" (mogły być czytane rozmaicie) w tym przykładzie ру-ки, albo р-уки albo рук-и). Wątpliwość tego typu w odtworzonym kodzie oznaczano nawiasem zwykłym: ру(к), р(ук). Nawiasem prostokątnym oznaczano wątpliwość co do tego, czy cały znak został dobrze dekryptowany np. [рук]. Szczególnie wątpliwe przypadki oznaczono ponadto znakiem zapytania. Znaki, które w kryptogramach występowały, lecz nie zostały dekryptowane zapisano w odtworzonym kodzie mimo, że nie można było podać ich znaczenia, pominięto natomiast znaki, których w depeszach brak.

Odtworzony w ten sposób kod przedstawia się następująco (kropka oznacza jeden lub kilka znaków szyfru, które aczkolwiek występowały w kodzie nie zostały użyte w badanych tekstach):

.	.	.
1303	1332 ни	1358 [котор]
1304	.	.
.	1334 й	1360 [kropka, ъ, lub sygla]
1308 во	1335	1361 [kropka]
.	.	.
1311 отправ	1340 он	1365 [житель]
.	.	.
1315 д	1343 [управ]	1368 ны
.	1344 за	.
1319 ие	.	1370 мо
.	1346 [ка]	.
1321	.	1372 [се]
.	1348	.
1327 л	.	1376 л
1328	1350 [а]	1377
.	.	.
1330 а	1353 ша	1379 для

.
1382 [русск]
.
1385
.
1392 ав
.
1395 пис(ь)
1396 ф(акт)
.
1398
.
1500 м
.
1503
.
1505 [евы]
1506 [сношен]
1507
.
1510 в
1511 [инт]
.
1516 у(бе)
.
1519
.
1521 у
.
1523 [им]
1524 ск
.
1526
1527
1528 ут
.
1530
.
1534
.
1537
1538
.
1541
1542 ен
1543 с
1544 [за]
.
1550 ан
.
1555 п(и)
.
1558

.
1560 я(ю)
1561
1562
1563 [zapewne sygla lub ъ]
1564 [об]
.
1566 [kropka, бы lub и]
.
1569 Фелинск(ий)
.
1571 (и)с
1572 у(хт)
.
1574 ыл
1575 что
1576
.
1579 [ую]
.
1582 и
.
1586 ст
.
1590 (е)ю(щ)
1591 л(яю)
1592
.
1595 [зя]
.
1597 т
.

2401
.
2403 вт
2404 б
.
2408 ес
2409 [przecinek]
.
2412 [жи]
.
2414 цу
2415 бе
.
2428
.
2431
.
2433
.
2435 ого

2438 военн(ый)
2439 ко
2440 л
.
2442 у
.
2445
.
2447 ь
.
2449 дост
.
2452 е
.
2463
.
2467
.
2471 з
.
2476 сп
.
2480 ов
.
2483
.
2494
.
.
2701
2702 я
.
2705
.
2709 ер
.
2711 г
.
2714 са
2715 [а(ци)]
.
2720 шл
2721 ря
.
2723 е
2724
2725 мо
.
2730 ием
.
2735 р
.
2742 и

.
2744 со
.
2749 (и)л
2750
.
2752 ех
.
2757 [з]
.
2759
.
2765 но
.
2768 [ей]
.
2774 ым
.
2780 ла
.
2783 (и)ч
.
2785 но
2786 шу
.
2788
.
2791
.
2795 ств
.
.
2797 ро
.
3600 [сего]
3601 га
.
3606 в
.
3611 адъютант
3612
.
3617
.
3622 [д]?
.
3624 перед
3625 [ва]
.
3627
3628 [(у)р]
3629 [пк]
.
3633 х
.
3636 след
.
3639 [ж(у)]
.
3646 ен
3647
.
3649
3650 Петербург
.
3653
.
3656 [е]
.
3659 гот
3660 ре [ale także рен, рье]
.
3665 фи
.
3669
.
3671 [л]?, [ит]?
.
3673 [кор]
.
3675 л
3676 ра
.
3679 хо
3680
.
3682
.
3684 ы
.
3688 аж
3689
3690 ден
3691 [пис]
.
3695 благо
.
3697
3698 [ем]
3699 ру
.
3900
3901
.
3905 ве
3905 [kropka lub sygla]
3906 бо
.
3910 ат
.
3915 н
3916 от
3917 ду
.
3919
.
3923 ле
3924 на
3925 [иб]
3926 од
3927
3928 о
.
3930 че
3931 же
.
3934
.
3938 ча
.
3949 см
3950 да
.
3952 ю
3952 по
.
3958 [чего]
3959 воз [albo всс]
.
3962 г
.
3965 у
.
3970 ии (albo ий
3971 опр
.
3973 цитадель
.
3977
3978
.
3981 выс
3982 курьер
3983
3984 е
.
3986 оч
.
3992 [zapewne sygla szyfranta]

.
3997 ки
.
3999 ру
4000 Росси
4001 [(кт)о]
.
4003
4004 при
4005 а
.
4011 [kropka lub sygla]
.
4013
4014
4015
4016
.
4018 т
.
4020
4021 [(ци)ю]
.
4923 кого
.
4025 то
.
4028 м
.
4045 [щи]
4046 и
.
4048 приказ
4049
.
4051 и
4052 го
.
4056
.
4058 ми
.
4061 [назнач]
.
4063 [кро]
.
4069 ло
.
4071
4072
4073 [пря]
.
4077 о
4078 сегодня
4079
.
4084 име
.
4086
.
4088 ок
.
4091
.
4093 гр
.
4095 сы
.
.
4202 аз
.
4210 [е]
.
4212
4213 ц
.
4220 чи
.
4223 ас
.
4230 к(у)
4231
.
4246 [kropka lub sygla]
.
4248 ых
.
4251
.
4262
4263 ре
.
4272
.
4275
.
4278 ши
4279 офицер
.
4281
.
4290
.
4292 [его]
.
4296 не
.
4299 [на]
.
5103
5104 ал
5105 [два, двух, 2]
5106 [отправля]
5107 жа
.
5112 ме
.
5115
.
5118
.
5122 ной
.
5129 пе
5130 ви
5131 дер
.
5138 про
5139
.
5147 л
.
5151 [ш]
.
5156 посла(н)
.
5158 ю
.
5161
.
5163 вче
.
5167 х
.
5170 те
5171 (бе)ж
5172 ия
.
5174 ос
5175
5176 сл
.
5182
5183
.
5186
.
5188 ю
.

5190
.
5192 вс
.
5196 [ме]
.
5199
.
.
5802 [с]
.
5804
.
5808 [пр]
.
5812 [тр]
5813 [ется]
.
5819
5820 [ш]
5821 ня
.
5825 н
.
5829
.
5834 ом
5835
.
5838
.
5851
.
5856 послан
5857 ол
5858 [ят]
5859 п
.
5861 ку
5862 [в]
.
5867
.
5869 жу
.
5871 зе
.
5876
.
5881 пи
5882 с
5883 [нр]
.
5886 [под]
.
5888 [kropka lub sygla]
.
5891 [был]
.
5893 [мисси]
.
5895 су
.

Statystycznie rozrzut użytych znaków przedstawia się następująco (bez powtórnie użytych):

Setka	Użytych w depeszach	W tym zidentyfikowanych bez wątpliwości	Zidentyfikowanych niedokładnie	Zidentyfikowanych niepewnie	Nie zidentyfikowanych
1300—1400	36	18	2	7	9
1500—1600	48	15	9	8	16
2400—2500	27	16	1	1	9
2700—2800	33	20	4	2	7
3600—3700	43	20	2	7	14
3900—4000	45	32	2	2	9
4000—4100	41	21	2	5	13
4200—4300	23	11	1	3	8
5100—5200	36	21	2	2	11
5800—5900	33	13	—	10	10
	365	187	25	47	106

Ogółem znaków użytych w depeszach wraz z wielokrotnie powtórzonymi („długość tekstu depesz") jest 1320.

Jak z zestawienia wynika nie wszystkie części kodu były jednakowo często używane. Oznaczać to mogłoby wadę budowy kodu polegającą na skupieniu obok siebie znaków częściej używanych, w innym zaś miejscu znaków mniej potrzebnych. Mogłoby to jednak oznaczać także lenistwo lub niefachowość szyfranta, który przyzwyczaił się do posługiwania się pewną częścią kodu i stale z niej korzystał.

Odtworzenie części kodu i dekryptowanie depesz pozwoliło także na pewne spostrzeżenia dalsze. Dotyczą one spraw następujących:

1. Kod zawiera litery, sylaby i słowa. Można sądzić, że tworząc kod wybrano wśród słów przede wszystkim takie, których zamierzano często

używać. Kod zawiera więc znaki wskazujące na jego przeznaczenie. Znak 1506 — „сношен(ия)" wskazuje na to, że przewidywano użycie kodu dla informowania o nielegalnych zapewne kontaktach, podobny charakter użycia kodu zapowiada znak 3973 — „цитадель", 3636 — „след(ствие)" i kilka innych jeszcze znaków. Umieszczenie w kodzie takich słów jak „офицер", „адьютант", „приказ", „военн(ый)", a równocześnie słów takich „житель", „управ(ление)", „пись(мо)", odzwierciedla swoiste łączenie elementów wojskowych i cywilnych w rosyjskiej administracji.

Występujący w kodzie znak 1569 — „Фелинск(ий)" wskazywać mógłby na to, że kod opracowano specjalnie dla korespondencji namiestnika Królestwa Polskiego i to krótko przed powstaniem styczniowym, gdyż wtedy nazwisko to weszło w szerszy obieg, bądź też na to, że przewidziano w kodzie wolne miejsca dla późniejszych uzupełnień. Za pierwszym wariantem przemawiałoby to, że znany jest kryptogram depeszy z Warszawy do Petersbugrga z roku 1861 szyfrowany przy pomocy innego kodu, a ponadto również i brak jakichkolwiek innych dowodów świadczących o wolnych, rezerwowych miejscach w kodzie.

3. Sposób grupowania liter w znakach oznaczających sylaby lub większe części słowa wskazuje na znaczną wprawę twórcy kodu, a także na pewne wiadomości filologiczne. Przewidziano więc w kodzie zamienne stosowanie sylab - oro, - aro, zamienne stosowanie liter oznaczających ten sam dźwięk, np. e (jat') i e, rozbijając wyraz między dwa znaki dzielono go zwykle na rdzeń i końcówkę, co znacznie zwiększało pojemność kodu, dla liter lub sylab często w rosyjskim występujących przewidziano po kilka znaków, dla rzadszych zapewne po dwa itp.

Występuje jednak w kodzie i pewna nieporadność, choćby w sekwencji znaków. Błąd popełniony w tej dziedzinie przy budowie kodu pozwala przewidywać z pewnym prawdopodobieństwem charakter znaku mimo, że nie został on w badanych kryptogramach użyty.

4. Sposób posługiwania się kodem przez szyfrantów nie był jednakowy. Szyfrantów było chyba trzech, a wskazują na to ich sygle używane w kryptogramie i zasób używanych przez nich znaków. Jeden z szyfrantów, gdy w paru kolejnych depeszach przyszło użyć tych samych słów lub zwrotów, powtarzał poprzednio użyte znaki, drugi zestawiał te same słowa z każdym razem z innych znaków. Jeden często popełniał błędy jak się zdaje niezamierzone, drugi swą syglę umieszczał zawsze w środku tekstu, często w środku słowa i częściej stosował inne utrudnienia i środki ostrożności. Wreszcie i odbiorca tekstu postępował niejednakowo. Tak się składa, że znane dziś teksty odcyfrowane przez odbiorcę pochodzą z tego samego czasu (koniec maja i pierwsza połowa czerwca 1863 r.), co i łatwiej szyfrowane kryptogramy; dla pozostałego okresu odcyfrowanych depesz chyba nie ma. Czyżby oznaczać to miało zmiany stopnia ostrożności przez cały aparat zaangażowany w tłumieniu powstania?

Ku podobnym przypuszczeniom prowadzić mogłoby traktowanie, jako rzeczy szczególnie tajnej, informacji o tym, że obszerniejszy list i dziennik działań wojennych zostają przesłane przez umyślnego kuriera. Ta właśnie informacja bywała szyfrowana, podczas gdy zdarzało się, że pozostałe zawarte w tej samej depeszy pisano zwykłym sposobem. Czyżby oznaczać to miało, że obawiano się, iż powstańcy mają dostęp do przesyłanych depesz i że mogliby, dowiedziawszy się o przesyłce, o której mowa, przechwycić ją w jakiś sposób?