

Maciej Jasiński

<https://orcid.org/0000-0002-3484-4039>

Instytut Historii Nauki im. Ludwika i Aleksandra Birkenmajerów
Polskiej Akademii Nauk

Szyfr Stanisława Lubienieckiego

Artykuł zawiera omówienie klucza szyfrowego, który znajduje się w materiałach po Stanisławie Lubienieckim młodszym (1623–1675), przechowywanych w Zbiorach Specjalnych Uniwersytetu w Amsterdamie. Szyfr zachował się jedynie w brudnopisie i nie jest pewne, czy był wykorzystywany. Artykuł podejmuje także próbę wskazania, do czego Lubienieckiemu mógł ten szyfr posłużyć.

The article discusses the cipher key which is kept in Stanisław Lubieniecki the Younger's (1623–1675) materials in the Special Collections of the University of Amsterdam. Only a draft of the code is preserved and it is uncertain whether it was used or not. The paper also aims to determine the purpose of creating such a code.

Słowa kluczowe: Stanisław Lubieniecki młodszy (1623–1675), kryptografia, bracia polscy

Key words: Stanisław Lubieniecki the Younger (1623–1675), cryptography, Polish Brethren

Biblioteka Uniwersytetu w Amsterdamie posiada bogaty zbiór materiałów po Stanisławie Lubienieckim młodszym (1623–1675), aktywnym członku ruchu braci polskich, który po Potopie opuścił Rzeczpospolitą i osiadł w Hamburgu. Zostały one obficie wykorzystane w poświęconych Lubienieckiemu pracach – przede wszystkim w podstawowej

jego biografii pióra prof. Janusza Tazbira¹ – jednak można wśród nich znaleźć kilka interesujących drobiazgów, które nie zostały do tej pory szerzej omówione. Nie zmieniają one wprawdzie obrazu postaci Lubienieckiego, ale rzucają nowe światło na pewne aspekty jego życia i działalności. Jednym z takich interesujących materiałów jest klucz do szyfru.

Rękopis Lubienieckiego zawierający ów klucz znajduje się w Zbiorach Specjalnych Uniwersytetu w Amsterdamie (Bijzondere Collecties van de Universiteit van Amsterdam), w zbiorze o sygnaturze OTM: hs. Ar 53, nazwanym Aanteekeningen van versehiden aard (Szkice różnej natury)², i jest oznaczony Ar 53:6. Jak sugeruje nazwa zbioru, zawiera on różnego rodzaju luźne i w większości niepowiązane ze sobą zapiski i notatki, m.in. inwentarz księgozbioru Lubienieckiego³, wiersz poświęcony narodzinom jego córki Katarzyny Salomei⁴, notatki odnoszące się do dziejów Kościoła⁵ i zagadnień teologicznych⁶ oraz różne pokwitowania, w tym dotyczące pożyczanych książek⁷. Klucz do szyfru jest niedatowany, podobnie jak większość pozostałych materiałów w tym zbiorze. Te z nich, które noszą daty, powstały między rokiem 1651⁸ a 1671⁹.

Napisany ręką Lubienieckiego klucz jest nieukończony i sprawia wrażenie, jakby był brudnopisem albo niezrealizowanym pomysłem. Jest on rodzajem prostego nomenklatora – połączenia szyfru

¹ J. Tazbir, *Stanisław Lubieniecki. Przywódca arińskiej emigracji*, Warszawa 1961; idem, *Stando lubentius moriar. Biografia Stanisława Lubienieckiego*, Warszawa 2004.

² M. B. Mendes da Costa, J. Berg, *Bibliotheek der universiteit van Amsterdam. Catalogus der handschriften. VII, De handschriften, krachtens bruikleencontract in de universiteitsbibliotheek berustende*, Amsterdam 1923, s. 93.

³ Zbiory Specjalne Uniwersytetu w Amsterdamie (dalej: ZSUA), sygn. OTM: hs. Ar 53:3, Ar 53:4, Ar 53:7; inwentarz ten został wydany przez J. Tazbira, *Księgozbiór Stanisława Lubienieckiego*, „Rocznik Biblioteki Narodowej”, 4, 1968, s. 197–223.

⁴ ZSUA, sygn. OTM: hs. Ar 53:5; zob. też J. Tazbir, *Wiersze Stanisława Lubienieckiego*, „Przegląd Humanistyczny”, 9, 1965, 2, s. 118.

⁵ ZSUA, sygn. OTM: hs. Ar 53:8.

⁶ ZSUA, sygn. OTM: hs. Ar 53:18.

⁷ ZSUA, sygn. OTM: hs. Ar 53:10, Ar 53:14, Ar 53:15.

⁸ ZSUA, sygn. OTM: hs. Ar 53:18, k. 1ver. – taką datę nosi list, którego niezapisaną stroną Lubieniecki wykorzystał na notatki.

⁹ ZSUA, sygn. OTM: hs. Ar 53:1 – wiadomość Lubienieckiego dla Adamusa Francusa w sprawie sprzedaży książki Lubienieckiego *Theatrum cometicum* (Amsterdamami 1666–1668) w Holandii, nosząca datę 22 XII 1670 r. starego stylu (1 I 1671 r. nowego stylu).

(utajniania poszczególnych znaków) i kodu (utajniania sylab, całych słów lub zdań)¹⁰. Zawiera alfabet szyfrowy oraz kilka najważniejszych słów, przede wszystkim czasowników. Większości elementów odpowiadają dwie wartości homofoniczne.

Jednostronnie zapisana karta o wymiarach 20 na 5,8 cm¹¹ podzielona jest na trzy kolumny, z których wypełnione są tylko pierwsze dwie. Kolumna „Valor” przedstawia litery, zbitkę „sc” oraz dwuznak „sz” tekstu jawnego, a także słowa: „aby”, „był”, „posłał”, „poszedł”, „przeszedł”, „przez”, „obieczał”, „dał” i „wziął” oraz „do”, które zostało jednak skreślone. Przy niektórych czasownikach dopisane są także formy w innych rodzajach i liczbach – należy przypuszczać, że oznacza to, iż czasowniki należy kodować w podany sposób niezależnie od formy gramatycznej, przynajmniej w czasie przeszłym. Kolumna „Figura” zawiera dwie homofoniczne liczby, które odpowiadają danej literze lub słowu, zapisane w dwóch kolumnach. Pierwsza zawiera liczby od 1 do 37 (bez wykorzystania liczby 35), druga – od 41 do 79 (niewykorzystane pozostają 58, 59 i 68). Trzecia kolumna jest opisana „Accessoria ktorzych pro lubitu zazywac dla zatrudnienia, ale te nic nie znaczą” i nagłówek ten sugeruje, że miała zawierać symbole puste – nic nieznaczące wartości, których stosowanie miało utrudnić złamanie szyfru. Kolumna ta nie zawiera jednak symboli pustych, lecz uzupełnienie do wcześniejszej części alfabetu szyfrowego – litery „ą”, „q” i „v” oraz zbitki „ff”, „ll”, „ss” i „st”, a także odpowiadające im znaki szyfru, będące jednak nie liczbami, lecz prostymi kształtami i figurami¹². Tym razem wartościom tekstu jawnego odpowiada tylko jeden znak szyfru bez wartości homofonicznych.

Obecność symboli pustych nie była konieczna w prostym alfabecie szyfrowym, ale niezrealizowany zamiar ich wprowadzenia pokazuje, że mamy do czynienia ze wstępną wersją projektu, który być może nie został nigdy ukończony. To zaś, że jest to brudnopis, sugeruje naniesiona przez Lubienieckiego poprawka – skreślone słowo „do”

¹⁰ D. Kahn, *Łamacze kodów. Historia kryptologii*, tł. B. Kołodziejczyk, Warszawa 2004, s. XIX. Dla uproszczenia pozwałam sobie tutaj używać nazwy „szyfr” dla metody utajniania tekstu znalezionej w archiwum po Lubienieckim, ponieważ jej większą część stanowi alfabet szyfrowy.

¹¹ Dziękuję p. Jesperowi Poulssenowi ze Zbiorów Specjalnych Uniwersytetu w Amsterdamie za przekazanie tej informacji.

¹² Pamiętając o amatorskich zainteresowaniach Lubienieckiego astronomią, warto wspomnieć, że jeden z tych symboli, przypisany zbitce „ss”, jest astronomicznym i astrologicznym symbolem Słońca.

i odpowiadające mu wartości, które zostały przypisane dodanej między wierszami literze „ę”.

Językiem, który miał być szyfrowany za pomocą klucza, był polski – świadczy o tym obecność litery „ł” oraz dwuznaku „sz”. O literach „ę” i „ą” Lubieniecki początkowo zapomniał, ale uzupełnił ten brak. Typowe dla łaciny litery „q” i „v” znajdują się na ostatnim miejscu wśród znaków, które zostały dopisane w bocznej kolumnie. Ponadto czasowniki i przyimki są zapisane po polsku, chociaż łatwo sobie wyobrazić, że w razie potrzeby można było tymi samymi wartościami szyfru kodować ich odpowiedniki w innych językach.

Można przypuszczać, że przygotowanie przez Lubienieckiego klucza do szyfru – czego celem naturalnie było utajnianie notatek i wiadomości – w zamierzeniach wiązało się z jednym z jego głównych zajęć na wygnaniu w Hamburgu i Altonie, mianowicie z działalnością informacyjną i wywiadowczą. Lubieniecki był dostawcą wiadomości na bieżące tematy, przede wszystkim, choć nie wyłącznie, z Polski i Litwy, dla kilku europejskich dworów – m.in. szwedzkiego i duńskiego, a w ostatnich latach swojego życia także francuskiego – oraz różnych dygnitarzy i możnowładców. Jego wysiłki na tym polu nie zawsze były jednak owocne. Przesyłane przezeń raporty częstokroć nie znajdowały uznania w oczach adresatów, a niektórzy potencjalni odbiorcy – jak dwór angielski – szybko rezygnowali z jego usług¹³. Mimo to miał dostatecznie wielu chętnych, by prowadzić tę działalność.

Niewykluczone, że klucz do szyfru miał służyć utajnieniu części korespondencji politycznej Lubienieckiego, chociaż wśród przebadanych przeze mnie materiałów archiwalnych po nim w bibliotekach uniwersyteckich w Amsterdamie, Lejdzie i Uppsali nie znalazłem żadnego przykładu stosowania go¹⁴. Także dotychczasowa literatura poświęcona Lubienieckiemu nie wspomina o jego stosowaniu. Nie można w związku z tym stwierdzić, czy projekt został ukończony i był stosowany, czy też pozostał jedynie niezrealizowanym szkicem, po którym wśród notatek autora zachował się tylko brudnopis.

¹³ J. Tazbir, *Stando lubentius moriar*, s. 144–153; J. Kowalik, *Szwedzka korespondencja Stanisława Lubienieckiego*, OiRwP, 47, 2003, s. 177–190.

¹⁴ Badania prowadziłem m.in. w ramach projektu badawczego „Analiza astro-nomicznych poglądów Stanisława Lubienieckiego (1623–1675), ich źródeł i uwarunkowań oraz przedstawienie ich na tle twierdzeń nauki XVII wieku”, finansowanego przez Narodowe Centrum Nauki w ramach programu PRELUDIUM 8 (nr decyzji DEC-2014/15/N/HS3/01305).

Mimo braku świadectw wykorzystywania amsterdamskiego szyfru wiadomo, że Lubieniecki stosował – a przynajmniej deklarował, że stosował – szyfrogramy w swojej korespondencji politycznej. Wspomina o tym Janina Kowalik, opisując raporty z informacjami politycznymi przesyłane przez Lubienieckiego szwedzkiemu kanclerzowi Magnusowi Gabrielowi De La Gardie (1622–1686). Otóż Lubieniecki miał mu zaoferować przesyłanie poufnych informacji, które otrzymywał w formie szyfrogramów od zaufanego korespondenta w Warszawie (tej postaci nie udało się zidentyfikować). Otrzymane materiały miały być rozszyfrowywane w Hamburgu, a następnie przesyłane z zachowaniem anonimowości nadawcy i pośrednika do Sztokholmu¹⁵. Nie udało mi się niestety odnaleźć tych szyfrogramów. Także J. Kowalik nie opisuje ani nie identyfikuje tych rękopisów. Nie można zatem stwierdzić, czy był w nich wykorzystywany alfabet szyfrowy zachowany w Amsterdamie.

Ponieważ klucz jest nieukończony i napisany ręką Lubienieckiego, należy przypuszczać, że to on był autorem tego szyfru, w przeciwnym bowiem razie należałoby się spodziewać odpisu gotowego klucza. Na tej podstawie można wysnuć pewne wnioski na temat wiedzy Lubienieckiego o współczesnej mu kryptografii. Nie wypadają one dla niego korzystnie. Szyfr Lubienieckiego – jeżeli można stwierdzić coś pewnego na podstawie jedynie brudnopisu – zapewne był szyfrem monoalfabetycznym, czyli wykorzystującym dla całej szyfrowanej wiadomości jeden alfabet szyfrowy, ponieważ klucz nie zawiera sugestii, by należało go rozpatrywać w połączeniu z innymi. W epoce, gdy Lubieniecki prowadził swoją korespondencję, znane były już szyfry polialfabetyczne, które używały równocześnie kilku alfabetów szyfrowych dla zakodowania wiadomości (np. nieparzyste znaki tekstu jawnego były szyfrowane za pomocą pierwszego alfabetu, parzyste – drugiego). Pionierem ich stosowania był Leon Battista Alberti (1404–1472), a rozwijali je Johannes Trithemius (1462–1516), Giovan Battista Bellaso (połowa XVI w.), Giovanni Battista Porta (1536–1615), Girolamo Cardano (1501–1576) i Blaise de Vigenère (1523–1596). Szyfr nazywany nazwiskiem Vigenère'a (w rzeczywistości przedstawiony już przez Bellasa), w którym każda litera tekstu jawnego była szyfrowana innym alfabetem szyfrowym według określonego słowa kluczowego, bywał nawet przesadnie określany jako niemożliwy do złamania. Mimo to kancelarie dworskie przez cały okres wczesnej

¹⁵ J. Kowalik, op. cit., s. 188–189.

nowożytności stosowały łatwiejsze i szybsze nomenklatory¹⁶. Choć szyfr Lubienieckiego należy do tej grupy kodów, nie można stwierdzić, czy miał tego rodzaju pochodzenie urzędowe. Jest on jednak ciekawym dodatkiem do obrazu działalności ariańskiego uchodźcy i być może kiedyś odnalezione zostaną rękopisy, które były zaszyfrowane za jego pomocą¹⁷.

Bibliografia

Źródła archiwalne

Zbiory Specjalne Uniwersytetu w Amsterdamie, sygn. OTM: hs. Ar 53

Opracowania

Kahn D., *Łamacze kodów. Historia kryptologii*, tł. B. Kołodziejczyk, Warszawa 2004

Kowalik J., *Szwedzka korespondencja Stanisława Lubienieckiego*, OiRwP, 47, 2003, s. 177–190

Mendes da Costa M. B., Berg J., *Bibliotheek der universiteit van Amsterdam. Catalogus der handschriften. VII, De handschriften, krachtens bruikleencontract in de universiteitsbibliotheek berustende*, Amsterdam 1923

Tazbir J., *Księgozbiór Stanisława Lubienieckiego*, „Rocznik Biblioteki Narodowej”, 4, 1968, s. 197–223

Tazbir J., *Stando lubentius moriar. Biografia Stanisława Lubienieckiego*, Warszawa 2004

Tazbir J., *Stanisław Lubieniecki. Przywódca ariańskiej emigracji*, Warszawa 1961

Tazbir J., *Wiersze Stanisława Lubienieckiego*, „Przegląd Humanistyczny”, 9, 1965, 2, s. 113–122

¹⁶ D. Kahn, op. cit., s. 141–185.

¹⁷ Za uwagi do wstępnej wersji artykułu dziękuję dr Barbarze Bienias (IHN PAN).

II. 1. Klucz do szyfru Stanisława Lubienieckiego młodszego i jego transkrypcja

Valor.	Figura.	Accessoria których pro lubitu zazywac dla zatrudnienia, ale te nic nie znaczą
a.	30. 46.	
b.	23. 42.	
c.	15. 44.	
d.	32. 41.	
e.	29. 43.	ą. +.
ę.	-- 1 -- 73. ¹⁸	ff. △.
f.	13. 45.	ll. ▽. ss. ○.
g.	6. 47.	st. ⊕.
h.	9. 48.	q. ▬.
i.	14. 49.	v. ∩.
k.	5. 52.	
l.	16. 54.	
ł.	4. 51.	
m.	7. 56.	
n.	3. 50.	
o.	17. 53.	
p.	21. ¹⁹ 55.	
r.	2. 57.	
s.	8. 60.	
sc.	24. 62.	
sz.	10. 65.	
t.	11. 61.	
u.	19. 63.	
w.	22. 67.	
x.	25. 64.	
y.	18. 66.	
z.	20. 69.	
aby.	26. 70.	
był.	27. 72.	była, byli, było.
posłał.	28. 75.	posłali
poszedł.	12. 77.	poszli
przeszedł.	31. 76.	przeszli
do.	4. 73.	
przez.	33. 71.	
obiegał.	34. 74.	
dał.	36. 78.	
wziął.	37. 79.	

Zbiory Specjalne Uniwersytetu w Amsterdamie, sygn. OTM: hs. Ar 53:6

¹⁸ Litera „ę” i odpowiadające jej liczby są dopisane między wierszami.

¹⁹ Pierwsza liczba odpowiadająca literze „p” jest częściowo uszkodzona. Tu została odtworzona na podstawie zestawienia użytych liczb.

Stanisław Lubieniecki's Code

The Special Collections of the University of Amsterdam hold a number of papers formerly belonging to Stanisław Lubieniecki the Younger (1623–1675), an Arian refugee settled in Hamburg. Among these items one can find a cipher key. It is a draft of a simple nomenclator, a code using numbers to conceal letters, some verbs, and prepositions. The key is unfinished: it lacks nulls, even though there was a separate column for them; moreover, there are some erasures and annotations in the manuscript. The cipher was devised to code Polish, however it was supplemented with letters typical for Latin.

I have not found any testimonies proving that Lubieniecki had ever used this cipher key. It is known, however, that in his intelligence and political correspondence he mentioned an informer who used to send him encrypted reports from Warsaw.

Maciej Jasiński – adiunkt w Instytucie Historii Nauki im. Ludwika i Aleksandra Birkenmajerów Polskiej Akademii Nauk. Jego zainteresowania badawcze obejmują historię astronomii i korespondencję astronomiczną wczesnej epoki nowożytnej.

Maciej Jasiński – PhD, assistant professor at the Ludwik and Aleksander Birkenmajer Institute for the History of Science, Polish Academy of Sciences. His research interests include history of astronomy and astronomic correspondence of the early modern era.

E-mail: mjasinski@ihnpan.waw.pl