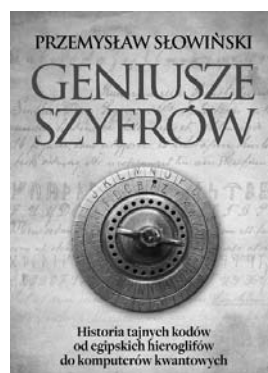


Paweł Perekietka

Fundacja Zakłady Kórnickie

Kórnik



Przemysław Słowiński, *Geniusze szyfrów. Historia tajnych kodów od egipskich hieroglifów do komputerów kwantowych*, Zona Zero, Warszawa 2024, 395 s.

Przedmiotem niniejszej recenzji jest książka popularnonaukowa przygotowana przez Przemysława Słowińskiego, z wykształcenia prawnika, parającego się różnymi zajęciami — pracował m.in. jako górnik, malarz i agent ubezpieczeniowy. Z katalogu Biblioteki Narodowej wynika, że Słowiński jest autorem 50 książek i współautorem ponad 20, które można sklasyfikować jako książki popularnonaukowe, biograficzne, powieści historyczne, kryminały i in. Aby zobrazować rozrzut tematyczny tych publikacji, podamy tu wybrane tytuły, które wyszły spod jego pióra w latach 2010–2011 r.: *Saleta. Łowca adrenaliny*, *Największe skandale w świecie filmu*, *Lech Kaczyński. Wspomnienie*, *Niepokorny bard. Opowieść o Włodzimierzu Wysockim*, *Falszerz. Han van Meegeren — człowiek, który oszukał Göringa* (jest to biografia holenderskiego malarza, który zasłynął jako fałszerz obrazów), *Brzemię. Opowieść o księdzu Władysławie Bukowskim, duszpasterzu sowieckiej Rosji*. W 2022 r. wydanie dwóch jego pozycji zostało dofinansowane ze środków Ministerstwa Kultury i Dziedzictwa Narodowego: *Ten drugi Piłsudski. Biografia Bronisława Piłsudskiego — zesłańca, podróżnika i etnografa* oraz *Księżę przygody. Biografia Ferdynanda Antoniego Ossendowskiego*, obie zostały wydane przez wydawnictwo Zona Zero.

Część sloganu reklamowego wydawnictwa Zona Zero brzmi „Sprawdzone źródło wiedzy”, a na stronie internetowej widnieje zapewnienie, że w jego ofercie znajdują się książki „autorstwa badaczy i znawców tematu”. Pozwala to oczekiwać wysokiego poziomu merytorycznego wydawnictw. Publikację Przemysława Słowińskiego pt. *Geniusze szyfrów. Historia tajnych kodów od egipskich hieroglifów do komputerów kwantowych*, wydaną również przez Zona Zero, trudno jednak zaliczyć do wartościowych książek popularnonaukowych.

Geniuszy szyfrów Słowińskiego można znaleźć na półkach najpopularniejszych polskich księgarni, m.in. Empiku. Obwoluta książki, przygotowana jest bardzo profesjonalnie, przyciąga wzrok i zachęca do kupna. Uwagę przykuwają zdjęcia przyrządów do szyfrowania. Centralną część przedniej karty okładki zajmuje dysk do szyfru z odwróconym alfabetem. Na karcie tylnej, obok streszczenia książki, zostały umieszczone zdjęcia współczesnej repliki Skytale, czyli przyrządu do szyfrowania przestawnego (stosowanego w starożytnej Grecji) oraz maszyny szyfrującej Enigma.

Niestety, to dobre wrażenie znika, gdy zajrzymy do wnętrza książki. Na przykład, na s. 77 znajdziemy zdjęcie przyrządu do szyfrowania Cezarem (litery na obu tarczach są zapisane w kolejności alfabetycznej), a Autor podpisał je — „Dysk Albertiego”.

Zanim poddamy analizie sprawy merytoryczne, należy ocenić sposób przygotowania pozycji pod względem redakcyjnym i korektorskim, a w tym aspekcie pozostawia ona jednak wiele do życzenia. W niniejszej recenzji poddano analizie wersję papierową książki oraz wydaną miesiąc później jej wersję elektroniczną (przygotowaną przez Epubeum).

Ze świadectwem niskiej jakości wkładu redakcyjnego i korektorskiego w powstanie wersji papierowej spotykamy się już w spisie treści. Tytuł podrozdziału II.3. zapisano następująco *Skytale — szyfry starożytnej Grecji. Szyfr Polibiusza. Początki stenografii*. Oczywiście zamiast „stenografii” powinno być „steganografii”. W pierwszym akapicie tekstu jest „Ta książka to fascynująca podróż” („ą” zamiast „a”), a chwilę później „ich osiągnięcia stanowiły pilnie strzeżone państw rządowe tajemnice” („państw” powinno być usunięte albo przeniesione na koniec twierdzenia). Niestety w publikacji napotkamy ogromną liczbę literówek i pomyłek, które powinny być usunięte podczas korekty. Kilka kolejnych przykładów: „Jezrzego” (zamiast „Jerzego”) na s. 33, „palety jednym z” zamiast „jednym z palety” na s. 71, „toi” (zamiast „to”) na s. 78, „Każda litera tekstu jawnego” zamiast „Każda litera tekstu tajnego” na s. 81, „<?>” zamiast „14” na stronie 202. Pojawiają się też sytuacje, w których między akapitami jest światło (wolna przestrzeń) zamiast ilustracji, o których mowa w tekście (s. 151, 152 i 174). Większość z tych niedociągnięć nie została poprawiona w wersji elektronicznej książki — z wcześniej wymienionych, poprawiono jedynie literówkę w spisie treści, „<?>” oraz dodano ilustracje.

W książce znajduje się blisko 50 ilustracji i tabel ułatwiających zrozumienie tematu. Wprawdzie zdarzają się dość obszerne fragmenty bez grafik (s. 9–40, 175–210), tym niemniej nie można odczytywać tego jako mankament publikacji, ponieważ w żaden sposób nie zakłóca to zrozumienia materiału. Minusem jest natomiast brak spisu ilustracji i indeksu, co zdecydowanie utrudnia lekturę. W książce nie ma też przedmowy ani posłowia. Rolę wstępu pełni pierwszy rozdział pt. *Wprowadzenie do szyfrów*, gdzie Autor najpierw naszkicował znaczenie

szyfrów, m.in. w komunikacji za pośrednictwem Internetu, a na kolejnych 15 stronach streścił materiał zawarty w publikacji.

Oceniając recenzowaną pozycję pod względem merytorycznym, należy podkreślić, że mamy do czynienia z kompilacją w dosłownym znaczeniu tego słowa (łac. *compilatio*). Tekst książki w dużym stopniu składa się z fragmentów innych utworów na temat historii szyfrów i kryptografii, dostępnych w języku polskim oraz angielskim (m.in. artykułów Wikipedii). Autor wymienia je w bibliografii, jednakże w tekście zazwyczaj nie posługuje się cytataми, nie informuje też czytelnika, gdy odwołuje się do nich jako źródeł.

Podaję poniżej kilka przykładów, które ukazują rzeczony proces kompilowania.

W podrozdziale II.2. Autor omawia szyfr Atbash (w literaturze nazywany też „odwróconym alfabetem”) i tutaj, na s. 40 książki znajdziemy akapit, który w dużej mierze jest przekładem fragmentu angielskojęzycznego artykułu Wikipedii — przekładem literalnym. W artykule z Wikipedii napisano:

Atbash [...] is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

Encryption

The Atbash cipher is [...] formed by taking the alphabet (or abjad, syllabary, etc.) and mapping it to its reverse, so that the first letter becomes the last letter, the second letter becomes the second to last letter, and so on.

Źródło: <https://en.wikipedia.org/wiki/Atbash> [dostęp: 9.11.2024].

W publikacji Słowińskiego jest (w poniższym fragmencie zostały wyróżnione sformułowania, które nie pochodzą z powyższego źródła):

[...] to prosty, monoalfabetyczny szyfr podstawieniowy, pierwotnie używany do kodowania alfabetu hebrajskiego, **opracowany prawdopodobnie około 500 p.n.e.** Można go używać do ukrywania tekstu oryginalnego za pomocą dowolnego systemu zapisu ze standardowym porządkiem sortowania. **Oryginalny system wykorzystuje alfabet hebrajski, który zawiera 22 litery, i proste ich zastępowanie według zasady: pierwsza z ostatnią, druga z przedostatnią i tak dalej.** [...] Szyfr Atbash tworzy się przez wzięcie alfabetu odwzorowanie go na jego odwrotnej stronie, tak że pierwsza litera staje się ostatnią, druga — przedostatnią literą i tak dalej [...].

Źródło: P. Słowiński, *Geniusze szyfrów. Historia tajnych kodów od egipskich hieroglifów do komputerów kwantowych*, Warszawa 2024, s. 40.

Zauważmy, że Autor i redaktor przeoczyli, że powyższy fragment zawiera dwa jednakowe objaśnienia działania szyfru Atbash (najpewniej pochodzące z różnych źródeł), które rozdzielało tylko jedno zdanie. Można też zauważyć, że korekta przeoczyła potrzebę wstawienia spójnika pomiędzy „alfabetu” i „odwzorowanie”. Brak spójnika w wersji przed redakcją wynika zapewne z faktu, że z oryginalnego tekstu „taking the alphabet (or abjad, syllabary, etc.) and mapping it” usunięto nie tylko informację zapisaną w nawiasie, ale też „and”.

W tym samym podrozdziale, na s. 39, znajdziemy przypis, który niemalże w całości jest kopią fragmentu kolejnego artykułu Wikipedii:

Septuaginta (z łac. *siedemdziesiąt*; oznaczana rzymską liczbą LXX oznaczającą 70, w wydaniach krytycznych przez symbol Ⲛ) — pierwsze tłumaczenie Biblii hebrajskiej i innych religijnych tekstów judaizmu z hebrajskiego i aramejskiego na grekę. Nazwa pochodzi od liczby tłumaczy, którzy mieli brać udział w pracach nad przekładem Tory. **Przekład ten** powstawał stopniowo pomiędzy 250 a 150 rokiem p.n.e. w Aleksandrii, i jest dziełem wielu tłumaczy^[1].

Od czasu powstania tego tłumaczenia aż do wieku IV n.e., z którego pochodzą najstarsze prawie pełne odpisy Septuaginty (Kodeks Watykański i Synajski z IV wieku oraz Aleksandryjski z wieku V), jej tekst przeszedł długą drogę **kolejnych kopii, wersji, dokonanych recenzji, korekt, uzupełnień oraz prób ujednolicenia treści**.

Źródło: <https://pl.wikipedia.org/wiki/Septuaginta>
[data dostępu: 9.11.2024].

Septuaginta (z łac. *siedemdziesiąt*; oznaczana rzymską liczbą LXX, w wydaniach krytycznych przez symbol Ⲛ) — pierwsze tłumaczenie Biblii hebrajskiej i innych religijnych tekstów judaizmu z hebrajskiego i aramejskiego na grekę. Nazwa pochodzi od liczby tłumaczy, którzy mieli brać udział w pracach nad przekładem Tory. **Tłumaczenie owo** powstawało stopniowo pomiędzy 250 a 150 rokiem p.n.e. w Aleksandrii. Od czasu jego powstania aż do wieku IV n.e., z którego pochodzą najstarsze prawie pełne odpisy Septuaginty (Kodeks Watykański i Synajski z IV wieku oraz Aleksandryjski z wieku V), jej tekst przeszedł długą drogę — **był wielokrotnie kopiowany, sporządzono wiele jego wersji, powstały recenzje, dokonywano korekt i uzupełnień, miało też miejsce wiele prób ujednolicenia treści**.

Źródło: P. Słowiński, *Geniusze szyfrów*, s. 39.

Kolejny przykład można znaleźć na s. 45. Tutaj Słowiński „wzorował się” na fragmencie książki *Podstawy kryptografii* Marcina Karbowskiego.

W II w. p.n.e. grecki historyk Polibiusz opracował system szyfrowania oparty na tablicy przyporządkowującej każdej literze parę cyfr.

W późniejszych **czasach** tablica ta stała się **podstawą** wielu systemów szyfrowania. Przekształcenie liter w liczby **dawało możliwość wykonywania dalszych przekształceń**. Za pomocą prostych obliczeń lub funkcji matematycznych. Metodę Polibiusza **uzupełnioną kilkoma** dodatkowymi utrudnieniami kryptoanalitycznymi zastosowała m.in. niemiecka armia **przy opracowywaniu** [...] systemu **szyfrującego** ADFGX oraz jego udoskonalonej wersji ADFGVX.

Źródło: M. Karbowski, *Podstawy kryptografii*.
Wydanie II, Warszawa 2008, s. 18.

W II **wieku** p.n.e. grecki historyk i **kronikarz Imperium Rzymskiego** Polibiusz z **Megalopolis** opracował system szyfrowania oparty na tablicy przyporządkowującej każdej literze parę cyfr. (...)

W późniejszych **okresach** ta tablica stała się **fundamentem** wielu systemów szyfrowania. Przekształcenie liter w liczby **umożliwiało dalsze manipulacje** za pomocą prostych obliczeń lub funkcji matematycznych. Metodę Polibiusza **wzbogaconą o kilka** dodatkowych utrudnień kryptoanalitycznych zastosowała m.in. niemiecka armia **do opracowania** systemu **szyfrowania** ADFGX oraz jego udoskonalonej wersji ADFGVX.

Źródło: P. Słowiński, *Geniusze szyfrów*, s. 45.

Warto w tym momencie wyjaśnić, że informacja podana przez Marcina Karbowskiego nie jest zgodna z prawdą — tablica Polibiusza nie była wymyślona w celu utajniania informacji, ale jako kod telegraficzny (gr. *τῆλέ* — daleko, *γραφω* — piszę), który pozwalał przysyłać informacje na odległość między latarniami morskimi, z użyciem pochodni. Szkoda, że Przemysław Słowiński nie weryfikował informacji w niezależnych źródłach, wówczas uniknąłby powielania tego rodzaju błędów.

Kolejny przykład zbyt daleko idącego wzorowania się na innej publikacji, można znaleźć na s. 102. Tutaj Słowiński tłumaczy na język polski następujące zdania:

The second type of cipher was the “Cardano’s grille”. In fact, it was the steno-graphic method, where the message was hidden in a number of other letters.

Źródło: J. Kolek, *History of cryptology*,
www.posterus.sk/?p=14100 [dostęp: 9.11.2024].

Drugim zaproponowanym przez Cardano rodzajem szyfru była tzw. „Kratka Cardano”. W istocie była to metoda stenograficzna, w której przekaz ukryto w szeregu innych listów.

Źródło: P. Słowiński, *Geniusze szyfrów*, s. 102.

Błąd w oryginalnym tekście — „stenographic”, powielono w przekładzie na język polski. Zamiast „stanograficzny” powinno być „steganograficzny”. Wyraz „letters” przetłumaczono jako „listy”, a powinno być „lityry”. W polskiej nazwie metody („grille”) użyto dosłownego przekładu „kratka”, choć w polskiej literaturze tematu używa się innego terminu — matryca. Ani Autor podczas opracowywania książki, ani redaktor podczas korekty nie usunęli tych błędów. Warto też zaznaczyć, że Słowiński wykorzystał w książce ilustrację matrycy pochodzącą z tekstu J. Kolka (tekst jawny: CARDANOSGRILLE), ale nie wskazał źródła.

Autor w przekładzie angielskojęzycznych artykułów na język polski, wielokrotnie poprzestawał na efektach tłumaczenia maszynowego. W konsekwencji, w książce *Geniusze szyfrów* jest dużo tekstu niezrozumiałego dla czytelnika, zwłaszcza w części dotyczącej teorii kryptografii.

Oto fragment (s. 380–381) streszczający osiągnięcia C. Shannona:

Większość prac Shannona skupiała się wokół tajemnicy teoretycznej; w tej dziedzinie wprowadził definicję „niezniszczalności” szyfru. Jeśli szyfr uznano za „nie do złamania”, zatrutowano [ortografia z książki — przyp. P.P.] go jako zapewniający „tajemnicę doskonałą”. Aby udowodnić jej odporność na „odkrycie”, Shannon ustalił, że można ją ujawnić: jedynie za pomocą klucza tajnego, którego długość podana w postaci binarnej jest większa lub równa liczbie bitów zawartych w zaszyfrowanej informacji. Co więcej, stworzył pojęcie tzw. „odległość jednolitości”, zdefiniowanej jako „ilość tekstu jawnego, która określa tajny klucz”.

Źródło: P. Słowiński, *Geniusze szyfrów*, s. 380–381.

Jaki jest sens powyższych zdań? Czym jest „tajemnica teoretyczna”? Czym jest „tajemnica doskonała”? Co to znaczy, że szyfr jest „niezniszczalny”? Jak rozumieć sformułowanie, że „tajemnica doskonała” jest odporna na „odkrycie”? W jaki sposób ilość tekstu jawnego określa tajny klucz? Dlaczego w tym kontekście łączy się słowa „odległość” i „jednolitość”? Co dociekliwy czytelnik zrozumie z tego fragmentu książki? Czy Autor nie znał polskojęzycznej terminologii w zakresie kryptografii XX w., a może tłumaczenie zostało wykonane maszynowo (bez późniejszej korekty)?

Można odnaleźć oryginalny angielskojęzyczny tekst, który był podstawą cytowanego przekładu na język polski — to odpowiednie akapity artykułu Wikiped-

dii pt. *History of cryptography*: https://en.wikipedia.org/wiki/History_of_cryptography [dostęp: 9.11.2024].

Nie dociekałem, skąd Przemysław Słowiński czerpał informacje na temat historii złamania szyfru Enigmy. Na stronach jego książki informacje zgodne z prawdą są wymieszane z nieprawdziwymi. Na przykład, na s. 270 czytelnik znajdzie następujący tekst o polskich kryptologach: „Trójka matematyków pracujących nad złamaniem kodu wojskowej odmiany urządzenia założyła, że wariant, nad którym pracują, nie może za bardzo odbiegać od tamtej [handlowej, czyli cywilnej — przyp. P.P.] odmiany. I mieli rację. Różnił się tylko jednym elementem, a mianowicie układem klawiatury — wersja cywilna miała klawiaturę o standardowym [dla języka niemieckiego — przyp. P.P.] układzie maszyny do pisania QWERTZ”. Z dalszej części wywodu czytelnik dowiaduje, że klawiatura wojskowej wersji maszyny Enigma miała układ ABCDEF. Gdzie Autor książki znalazł taką informację? Dlaczego jej nie sprawdził w źródłach z zakresu historii nauki?

Nie można wykluczyć, że publikacja *Geniusze szyfrów. Historia tajnych kodów od egipskich hieroglifów do komputerów kwantowych* została przygotowana z użyciem tłumaczenia automatycznego (bez udziału człowieka), aby przyspieszyć proces powstawania książki. W 2024 r. ukazały się wszak trzy (obszerne) pozycje wydawnicze autorstwa Przemysława Słowińskiego.

Jak to jest możliwe, że taka publikacja znalazła się w ogóle w katalogu wydawcy?

Co więcej, fragmenty książki są dostępne w Internecie (np. na portalu WielkaHISTORIA, <https://wielkahistoria.pl/author/przemyslawslowinski/> [dostęp: 9.11.2024]), w postaci artykułów popularnonaukowych, wydaje się, że za zgodą wydawcy. Łatwo sprawdzić, że ten tekst został zaindeksowany przez popularną wyszukiwarkę i jest ogólnodostępnym źródłem informacji.