Księgi tajemnych przekazów

Często zadaje się matematykom pytanie, do czego mogą przydać się rezultaty ich abstrakcyjnych badań. Odpowiedź, że problemy rozwiązuje się po to, żeby więcej wiedzieć, nie zawsze jest zadowalająca, szczególnie dla tych, którzy finansują takie badania. W nauce jest jednak tak, że trudno jednoznacznie przewidzieć, który rezultat znajdzie szybko praktyczne zastosowanie.

W matematyce wiele teorii powstało niejako na zamówienie konkretnych dziedzin nauki, w szczególności fizyki. Wiele innych jednak było wynikiem naturalnych uogólnień znanych już rezultatów.

Całe działy powstawały przy okazji atakowania problemów nurtujących samych matematyków. Dziedziną uznawaną za najczystszą z czystych w samej matematyce była teoria liczb. Z jednej strony może to się wydawać trochę dziwne, gdyż trudno sobie wyobrazić jakąkolwiek dziedzinę działalności ludzkiej bez liczb, ale z drugiej strony studiowanie abstrakcyjnych własności liczb pierwszych, względnie innych wybranych rodzin liczbowych, wydaje się rzeczywiście sztuką dla sztuki. Gotfryd H. Hardy jeden z najwybitniejszych teorioliczbowców był przekonany, że zajmował się problemami, które nie mogły nikomu zaszkodzić. Dziś, w niecałe pięćdziesiąt lat później, teoria liczb i jej wyszukane techniki doczekały się bardzo praktycznych zastosowań i znalazły się w centrum zainteresowania wojskowych, bankowców oraz wszystkich, którym zależy na ochronie danych.

Rozwój techniki komputerowej i internetu, powstanie elektronicznych baz danych, elektronicznych banków, sklepów oraz innych „e-instytucji" zmusiły specjalistów do zapewnienia bezpieczeństwa osób, pragnących skorzystać z usług komputerowych. Pojawiło się mnóstwo ważnych problemów związanych z identyfikacją osoby bez ujawniania jej danych. Niemal każdy zetknął się już z jakimś PIN-em czy innym numerem znanym tylko jednej osobie, a jednak rozpoznawalnym przez rozmaite urządzenia elektroniczne. Dużo się słyszy ostatnio o podpisie elektronicznym. Jak to wszystko działa? Na czym polegają pomysły związane z szyfrowaniem informacji? Historia problemów ochrony informacji jest niemal tak stara jak historia pisma.

Pismo zostało wymyślone między innymi po to, aby przekazywać i zachowywać informacje. Z początku znajomość pisma była oznaką wtajemniczenia, a umiejętność odczytywania napisanych tekstów graniczyła z magią. Wraz z upowszechnieniem pisma, pojawiły się problemy z takim przekazywaniem informacji, żeby nie dostała się w niepowołane ręce. Należało tekst zapisać w taki sposób, żeby odczytał go tylko adresat – tak narodziły się szyfry.

Jednym z pierwszych udokumentowanych szyfrów był szyfr zastosowany przez Cezara w listach do Cycerona. Jak wyglądał? Czym się charakteryzował? Czy był trudny do złamania? Czy rzeczywiście był to pierwszy szyfr znany w historii? Na te i wiele jeszcze innych pytań odpowiedzi można znaleźć w dwóch książkach poświęconych problemom szyfrowania i kodowania informacji.

Wcześniej ukazała się (w oryginale i w polskim przekładzie) książka *Tajemne przekazy* Rudolfa Kippenhahna, nieco później światło dzienne ujrzała *Księga szyfrów* Szymona Singha. Czytelnik ma niezwykłą okazję porównania niezależnego podejścia obu autorów do zagadnienia szyfrowania w przeszłości i w czasach współczesnych. Singha uważny czytelnik miał okazję poznać już wcześniej – jest on bowiem autorem książki poświeconej Wielkiemu Twierdzeniu Fermata będącej podstawą scenariusza filmu o A. Wilesie i jego zmaganiu się z tym Twierdzeniem.

Obaj autorzy, każdy jednak na swój sposób, opowiadają o najważniejszych wydarzeniach w historii tworzenia i łamania szyfrów. Dowiadujemy się więc o tym, co przyczyniło się do wydania wyroku przez Elżbietę I na Marię Stuart, co to był Wielki Szyfr i czego dotyczył, jak wygląda tajemnica Żelaznej Maski. Ujawnione są kulisy włączenia się Stanów Zjednoczonych do I wojny światowej.

Poznajemy różnicę pomiędzy kryptografią a kryptoanalizą oraz szyfrowaniem a kodowaniem. Dość dokładnie omówiony jest problem słynnej Enigmy; jak działała i w jaki sposób doszło do rozpracowania jej tajemnicy. Należy zaznaczyć, że zarówno Kippenhahn jak i Singh nie zapomnieli o roli polskich matematyków w rozgryzieniu szyfrów tworzonych za pomocą Enigmy. Nazwiska Jerzego Różyckiego, Henryka Zygalskiego i przede wszystkim Mariana Rejewskiego nie są tylko wymieniane „dla porządku". Naturalnie przedstawione są dramatyczne losy innego poskramiacza Enigmy – Allana Turinga.

Mamy okazję przekonać się na czym polega łamanie szyfrów od tych najprostszych – monoalfabetycznych do, wydawałoby się, zupełnie bezpiecznych, uważanych za absolutnie nie do rozpracowania.

Singh opisuje mało znany epizod z życia Charlesa Babbage'a dotyczący złamania przez niego szyfru Vigenère'a, szyfru opierającego się atakom przez ponad trzy stulecia. Babbage najczęściej wspominany jest przy omawianiu historii komputerów jako pomysłodawca maszyny programowanej. W *Księdze szyfrów* znajdziemy też historię odczytania hieroglifów egipskich i tak zwanego pisma linearnego B cywilizacji kreteńskiej epoki brązu, co jest niewątpliwym sukcesem specjalistów zajmujących się kryptografią archeologiczną. Autor wspomina też o przyszłości metod szyfrowania, czyli o kryptografii kwantowej. Na końcu książki jest kilka zadań-wyzwań dla czytelników pragnących sprawdzić swoje umiejętności. Umieszczony

jest też słowniczek najważniejszych pojęć i literatura uzupełniająca, a także adresy najważniejszych stron internetowych.

Kippenhahn inaczej rozkłada akcenty. Więcej dowiadujemy się o Edgarze Allanie Poe i jego zamiłowaniu do łamania szyfrów. Z innej strony poznajemy historie rozpracowania szyfru Vigenère'a – tu głównym bohaterem jest oficer pruskiej armii Friedrich W. Kasiski. Dokładniej opisany jest polski wątek Enigmy. W *Tajemnych przekazach* bardziej szczegółowo omówione są sposoby łamania klasycznych szyfrów. Czytelnik pragnący się sprawdzić też znajdzie zadania do rozwiązania, ale w tej książce na końcu są odpowiedzi.

Nie mogło naturalnie zabraknąć w obu książkach historii powstania szyfrów z kluczem publicznym, przeboju ostatnich lat. Singh poświęca tym problemom niemal pół książki; wyczerpująco i bardzo ciekawie omówiona jest historia powstania szyfrów z kluczem publicznym, przedstawione są zasady działania oraz najważniejsze zastosowania. Kippenhahn mniej zajmuje się historią, choć najważniejsze fakty również zostały umieszczone. Poruszony jest za to temat dotyczący kart chipowych, PIN-ów i elektronicznych podpisów. Pouczające jest porównanie sposobu prezentacji obu autorów; jedna książka jest jakby uzupełnieniem drugiej. Szczególnie interesujące jest przedstawienie systemu PGP (Pretty Good Privacy) służącego do szyfrowania osobistych listów w poczcie elektronicznej. *Tajemne przekazy* zawierają nawet specjalny dodatek dla czytelników chcących używać PGP napisany przez Michała Sokoła.

Zarówno *Księgę szyfrów* jak i *Tajemne przekazy* można śmiało polecić uczniom gimnazjów, a nawet zainteresowanym uczniom starszych klas szkół podstawowych. Ciekawe połączenie historii z kompetentnym przedstawieniem konkretnych problemów czyni z obu książek pasjonującą lekturę dostępną dla wszystkich, którzy nie boją się logicznego myślenia na najbardziej elementarnym poziomie.

Zupełnie inny charakter ma książka Neala Koblitza *Algebraiczne aspekty kryptografii*. O ile obie wyżej wspomniane książki są pasjonującymi zbiorami historyjek o różnych szyfrach, ich zastosowaniach itp., to podręcznik Koblitza wymaga od czytelnika pewnego obycia z tekstami matematycznymi. Są tu omówione teoretyczne podstawy i matematyczne narzędzia znajdujące zastosowania w kryptografii. A zatem sporo jest informacji o ciałach skończonych i pierścieniach wielomianów. Autor przypomina twierdzenia Hilberta: o bazie i o zerach. Pojawiają się bazy Gröbnera, krzywe eliptyczne i hipereliptyczne oraz dywizory.

Nie jest to jednak podręcznik algebry i wybranych zagadnień teorii liczb. Wszystko podporządkowane jest potrzebom współczesnej kryptografii. Omówione są więc najistotniejsze problemy związane z szyframi z kluczami publicznymi. Obok najważniejszego – poufnego przekazu informacji, poruszone są zagadnienia uwierzytelniania (np. potwierdzenia, że wiadomość została wysłana przez daną osobę, podpisu cyfrowego), bezpiecznej wymiany kluczy, dzielenia sekretów, dowodu „wiedzy zerowej" czy też rzutu monetą na odległość. Wszystkie te problemy mają swoje matematyczne modele wykorzystujące algebrę, kombinatorykę i teorię liczb. Neal Koblitz sprytnie łączy ścisły wykład matematyczny z popularnonaukową prezentacją zastosowań, przez co książka jest dostępna dla osób bez większego przygotowania matematycznego, choć prezentowane pojęcia i twierdzenia należą do tzw. „twardej" matematyki.

Można przypuszczać, że ambitni czytelnicy pierwszych dwóch prezentowanych tu książek zechcą uzupełnić swoją wiedzę i poznać lepiej teoretyczne podstawy współcześnie tworzonych szyfrów, wtedy *Algebraiczne aspekty kryptografii* z pewnością będą dla nich lekturą godną polecenia choć wymagającą.

Zdzisław POGODA

Rudolf Kippenhahn, *Tajemne przekazy Szyfry, Enigma i karty chipowe*, Prószyński i S-ka, Warszawa 2000. Tłumaczenie Adam Sumera.

Simon Singh, *Księga szyfrów. Nauka skrywania tajemnic od starożytnego Egiptu do kryptografii kwantowej*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa 2001. Tłumaczenie Piotr Amsterdamski.

Neal Koblitz, *Algebraiczne aspekty kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa 2000. Tłumaczenie Witold Karaśkiewicz.