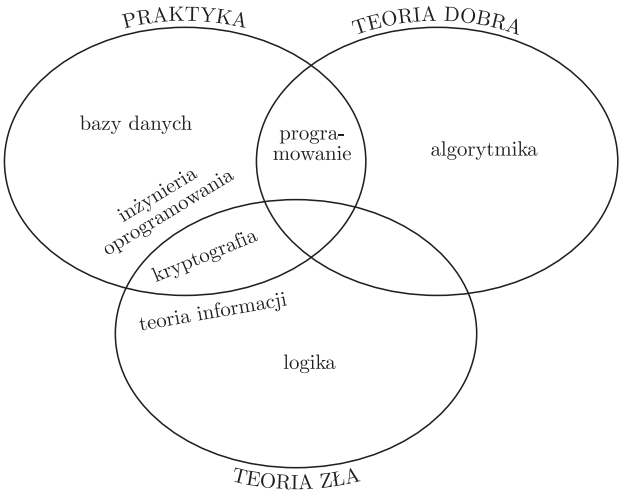
A jednak się da!
czyli o współczesnej kryptologii

Tomasz KAZANA[*]

Lubię próżnie mówić o sobie, że jestem matematykiem. Bardziej precyzyjnie to jestem informatykiem, ale przecież informatyka to gałąź matematyki, więc w zasadzie nie oszukuję. Czasem, gdy ktoś mnie ciągnie za język, i pojawi się to, z niejasnych powodów nielubiane przeze mnie, słowo na „i", to i tak od razu uściślam: tak, jestem informatykiem, ale informatykiem teoretycznym. Zawsze miałem to dziwne przekonanie, że „teoretyczny" znaczy w jakimś sensie lepszy, ważniejszy, mądrzejszy, głębszy.

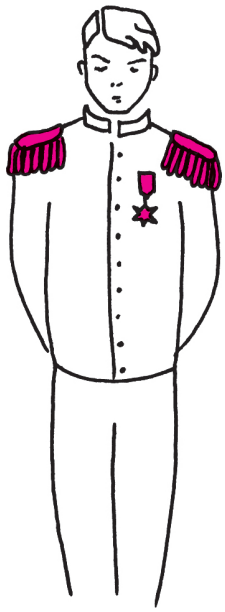
Podobne buńczuczne myślenie o sobie ma chyba spore grono matematyków. Chociażby Karol Gauss (już za życia zwany Księciem Matematyków), który choć badał bardzo różne dziedziny wiedzy, to ponoć najbardziej cenił sobie zgłębianie sekretów teorii liczb. To właśnie ona wydawała mu się zupełnie niepraktyczna, a zatem nieziemsko piękna. *L'art pour l'art!*



I tak to przez długi czas świat nauk ścisłych dzieliłem na teorię (bosko piękną) i praktykę (ludzko konieczną). Dziś widzę to trochę inaczej, w dużej mierze dzięki kryptologii – dziedzinie wiedzy, którą się zajmuję. Wizja ta ewoluowała, a aktualny stan mojego umysłu żartobliwie przedstawiam obok jako diagram Venna.

Jak widać, podzieliłem teorię na tę badającą zło (negatywne wyniki) i tę badającą dobro. Ta druga to wyniki pozytywne – dla mnie nuda, bo najfajniejsze są przecież wszelkie twierdzenia o niemożności lub szacowania z dołu, czyli pokazywanie ściśle, że czegoś się nie da. I, o ile dopuściłem, że teoretyczne wyniki pozytywne (np. algorytmy) mogą być praktyczne, to najgłębsza (czyli niepraktyczna) nauka musi się znajdować w części mrocznej. Kurt Gödel, Paul Cohen – to byli więc idole mojej młodości, a w głowie miałem tylko *saeculum obscurum* matematyki.

Wszystko to zburzyła współczesna kryptologia, dzięki której zrozumiałem, że wyniki negatywne (czegoś na pewno się nie da i nigdy to się nie zmieni) też mogą być praktyczne. No bo przecież, jeśli udowodnimy (formalnie!), że podsłuchiwacz, pomimo przechwycenia szyfrogramu, nigdy nie dowie się niczego na temat wysyłanej wiadomości, to jest to przecież ogromnie praktyczne.



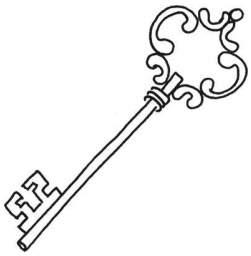
I ja tak właśnie patrzę na kryptologię: jako na część twardej matematyki ulokowanej gdzieś między klasycznymi twierdzeniami o niemożności a teorią obliczeń. Nic nie poradzę, że wolę myśleć o maszynie Turinga niż o maszynie Apple'a (choć na swój sposób cenię obie).

Kończę ten przydługi wstęp, licząc, że dostatecznie się zaasekurowałem i wytłumaczyłem, dlaczego w tym tekście tak mało będzie trzyliterowych skrótów, a tak dużo twierdzeń. Po prostu wszedłem na ten statek tylnymi drzwiami i, być może, patrzę przez inne okulary. Czytelnik sam oceni, czy takie spojrzenie mu odpowiada.

Dla mnie prawdziwa współczesna kryptologia zaczyna się w listopadzie 1976 roku, kiedy to w czasopiśmie *IEEE Transactions on Information Theory* ukazuje się artykuł *New directions in cryptography* autorstwa Whitfielda Diffiego i Martina Hellmana. W tym samym czasie w kioskach mamy *Deltę* numer 35, pierwszym sekretarzem jest Edward Gierek, a Polska jest potentatem w sportach zespołowych (złoto siatkarzy i srebro piłkarzy na letnich igrzyskach olimpijskich w Montrealu). A wspomniani wyżej autorzy publikują rewolucyjny pomysł kryptografii klucza publicznego.

Jest to dla mnie rewolucja, bo pojawia się pomysł, który jest zupełnie, ale to zupełnie nieoczywisty. Ba, podobno Oded Goldreich zawsze swój kurs kryptologii (w Instytucie Nauki Weizmanna w Izraelu) zaczyna od pracy domowej, w której

[*]Instytut Informatyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski



prosi studentów o wykazanie, że kryptografia klucza publicznego jest niemożliwa. Dopiero na kolejnym wykładzie pokazuje, że jednak się da!

O co chodzi w tej idei?

Kryptografia klucza publicznego. Pomyślmy chwilę o zwykłym, klasycznym szyfrowaniu. Nieśmiertelna w tej branży Alicja chce wysłać wiadomość m do Boba. Nie chcą oni, by wiadomość wpadła w niepowołane ręce, a, niestety, kanał komunikacyjny jest podsłuchiwany przez Ewę. W ogólności problem rozwiązujemy następująco: Alicja i Bob zawczasu ustalają między sobą tajny klucz k. I teraz, gdy Alicja chce wysłać wiadomość, to wysyła do Boba wartość pewnej funkcji $E(m,k)$. Natomiast gdy Bob odbierze c, to oblicza $D(c,k)$. Wszystko jest poprawne, gdy:

- $D(E(m,k),k) = m$;
- znajomość $c = E(m,k)$ nie umożliwia obliczenia m (bądź umożliwia, ale konieczne obliczenia trwałyby niesłychanie długo).

Opisany wyżej model jest znany i (mniej lub bardziej skutecznie) stosowany od tysięcy lat. W ten schemat wpisuje się zarówno szyfr Cezara, szyfr Vigenère'a czy maszyna szyfrująca Enigma. Pewną niedogodnością jest tu jednak konieczność ustalenia klucza k przed komunikacją. Pomysł Diffiego i Hellmana ociera się o bezczelność. Zapytali oni, czy da się przeprowadzić powyższą procedurę, ale bez klucza k. Innymi słowy, chcemy, aby Alicja mogła szyfrować wiadomości do Boba bez uprzedniego spotkania i ustalania jakiegokolwiek sekretu. Innymi słowy, funkcja E ma być publicznie znana (także Ewie) i nie zależeć od k.

„Na oko" widać, że zrobić się tego nie da. Przecież wystarczy, że Ewa, podsłuchawszy $c = E(m)$, obliczy odwrotność $E^{-1}(c)$ i pozna wiadomość!

A jednak, czasem się da! Powodem jest fakt, że dla pewnych funkcji E obliczenie funkcji odwrotnej E^{-1} może być dla Ewy koszmarnie trudne. Z drugiej strony Bob da sobie radę, bo zna pewną tajemnicę na temat E, której nikomu (nawet Alicji) nie ujawnił. Szczegóły tej magii zostawiam Czytelnikowi Zaciekawionemu do własnych poszukiwań. Dodam tylko, że w jednym z rozwiązań (RSA) korzysta się (o ironio!) ze zdobyczy teorii liczb, tak wielbionej przez Gaussa za niepraktyczność!

Dziś w matematyce urzeka mnie chyba najbardziej właśnie to – dowody faktów nieoczywistych, sprzecznych z intuicją. Nazywam to efektem „A jednak się da!" i dostrzegam ogrom takich rozumowań w kryptologii. Ostatnie 500 miesięcy to wręcz wysyp takich cudownych perełek, o których spróbuję trochę opowiedzieć.

Dowody z wiedzą zerową. Wyobraź sobie Czytelniku Sekretny, że udowodniłeś, iż $P \neq NP$ albo pokazałeś prawdziwość hipotezy Riemanna. Chcesz teraz:

- przekonać świat, że rozważana hipoteza faktycznie jest prawdziwa;
- zachować szczegóły dowodu tylko dla siebie.

Sprzeczne? A jednak się da! Prace z lat 80. XX wieku takich kryptologów jak Oded Goldreich czy Shafrira Goldwasser opisują, jak to zrobić.

Szyfrowanie homomorficzne. Tym razem, Czytelniku Ciekawski, wyobraź sobie, że chcesz wyszukać w Internecie informację na jakiś temat T. Znasz wiele wyszukiwarek (choćby tę na literę G), które znajdą listę interesujących Cię stron w ułamku sekundy. Jednakże Ty chciałbyś więcej:

- poznać listę stron na temat T;
- mieć gwarancję, że dostawca usługi (wyszukiwarka G) zupełnie nic się nie dowie, czego szukałeś (czyli T pozostanie dla niego tajne).

Innymi słowy, usługodawca poprawnie odpowiada na Twoje pytanie, pomimo że nie zna pytania. Jak poprzednio: da się, choć, póki co, nie jest to bardzo efektywne. I żadna wyszukiwarka tego nie oferuje. Czytelnik Zainteresowany niech wpisze w G hasło *fully homomorphic encryption*. No, chyba że nie chce, żeby ktokolwiek dowiedział się, czego szuka. W takiej sytuacji pozostaje zwykła czytelnia.

E-gotówka. Czytelnik Kapitalista zapewne zna podstawową zaletę gotówki. Anonimowość! A teraz wyobraźmy sobie, że mamy cyfrowy odpowiednik monet i banknotów – specjalne pliki, które spełniają następujące, pozornie sprzeczne, warunki:

- posiadanie pojedynczej kopii takiego pliku nie zdradza (nawet bankowi!) tożsamości osoby, która posiadała ten plik wcześniej;
- jeśli (nielegalnie) przekażemy nasz plik dwóm różnym osobom, to w przyszłości bank to wykryje i odkryje naszą tożsamość.

W rzeczywistości podczas procesu przekazywania plik się lekko zmienia, za każdym razem trochę inaczej.

Że się da, proszę się przekonać, sięgając do pracy Stefana Brandsa *Electronic Cash* z roku 1996.

Poker przez Internet. Możliwość brania udziału w grach hazardowych przez Internet nie jest zaskakująca. Dobrze, ale co, jeśli chcemy grać bez zaufanej trzeciej strony (serwera)? Pomyślmy chociażby o znacznie łatwiejszym pytaniu: jak „rzucić monetą przez Internet" bez zaufanej trzeciej strony tak, aby żaden z graczy nie mógł złośliwie wpłynąć na wynik. Intuicja podpowiada, że z pewnością się nie da! A jednak: zachęcam do sięgnięcia do pracy Manuela Bluma *Coin Flipping by Telephone* z roku 1981 czy późniejszej pracy Moniego Naora *Bit Commitment Using Pseudo-Randomness* z roku 1991. Oczywiście, nikogo nie zaskoczę, gdy dodam, że poker przez Internet bez zaufanych trzecich stron też jest możliwy.

Wiele przykładów, które pokazałem w tym artykule, to, prawdę powiedziawszy, trochę rubieże (ale jakże piękne) klasycznej kryptologii. Spośród tego, co wydarzyło się w ciągu ostatnich 500 miesięcy, wybrałem to, co, moim zdaniem, najciekawsze, ale, być może, nie najważniejsze dla bezpieczeństwa cyfrowego świata. Należy dodać, że klasyczna kryptologia jako taka też znakomicie rozwijała się w tym czasie. Przede wszystkim omawiana dziedzina zaczęła być przedstawiana w rygorze formalizmów matematycznych. Definicje stały się ostre, często pomysłowe.

Oczywiście, motywacja do rozwoju jest zupełnie jasna: w XXI wieku informacja ma dużą wartość, a więc jej ochrona staje się niezwykle kluczowa. Ludzie chcą bezpiecznie trzymać, wysyłać, podpisywać czy odbierać wiadomości. Przy tym chcą również chronić swoją prywatność, nawet gdy wszystko dzieje się „w chmurze". A w epoce *digital natives* te problemy będą jeszcze ważniejsze.

Tym bardziej jest pocieszające, że przy tej okazji rozwija się ciekawa gałąź prawdziwej matematyki, z niebanalnymi modelami, twierdzeniami i hipotezami.

Zadania

Redaguje Tomasz TKOCZ

M 1480. Udowodnić, że dla dowolnej liczby nieujemnej x i dowolnej liczby całkowitej dodatniej n prawdziwa jest nierówność

$$\lfloor nx \rfloor \geqslant \frac{\lfloor x \rfloor}{1} + \frac{\lfloor 2x \rfloor}{2} + \ldots + \frac{\lfloor nx \rfloor}{n},$$

gdzie $\lfloor a \rfloor$ oznacza największą liczbę całkowitą nie większą od a.
Rozwiązanie na str. 5

M 1481. W tablicę $n \times n$ wpisano w pewnej kolejności liczby $1, 2, \ldots, n^2$. Powiemy, że para liczb *sąsiaduje*, jeśli znajdują się one obok siebie w pewnym wierszu lub w pewnej kolumnie. Wykazać, że istnieje para sąsiadujących liczb, które różnią się co najmniej o n.
Rozwiązanie na str. 18

M 1482. Na sferze o promieniu 1 dana jest krzywa zamknięta o długości mniejszej niż 2π. Wykazać, że ta krzywa jest zawarta w pewnej półsferze.

Uwaga. Można uważać za oczywiste następujące stwierdzenie: *najkrótsza krzywa łącząca dwa punkty na sferze to łuk okręgu wielkiego.*
Rozwiązanie na str. 3

Przygotował Andrzej MAJHOFER

F 895. (a) Ile elektronów zawiera średnio 1 g ciała człowieka?
(b) Ile elektronów zawiera średnio 1 g otaczającej nas materii?
Rozwiązanie na str. 15

F 896. Kondensator powietrzny o pojemności $C = 100$ pF wypełniono roztworem soli kuchennej o oporze właściwym $\rho = 0{,}15\ \Omega$m. Ile wynosi opór elektryczny R między elektrodami tak otrzymanego opornika? Przenikalność elektryczna próżni to $\varepsilon_0 \approx 8{,}85 \cdot 10^{-12}$ F/m.
Rozwiązanie na str. 17