- 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 $2\pi$. 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