ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XXXVI (2000)

Recenzje

Neal K o b l i t z, *Algebraiczne aspekty kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa 2000, ISBN 83-204-2418-6.

Jest to drugi podręcznik amerykańskiego kryptologa ukazujący się na polskim rynku. W pierwszym ("Wykład z teorii liczb i kryptografii") autor naświetlił teorioliczbową problematykę szyfrowania. Drugi, zgodnie z tytułem, jest poświęcony algorytmom kryptograficznym, które wynikają z trudności obliczeniowych związanych z rozwiązywaniem niektórych zagadnień algebraicznych. Wykłady rozpoczynają się od nakreślenia zadań, metod i historii kryptografii. Zagadnieniom tym poświęcony jest pierwszy rozdział podręcznika – swoiste minikompendium wiedzy kryptologicznej. Podobną rolę spełniają dwa następne rozdziały: drugi, poświęcony problematyce złożoności obliczeniowej i trzeci, zapoznający czytelnika z podstawami algebraicznymi współczesnych algorytmów szyfrujących. Kolejne trzy wykłady analizują konkretne kryptosystemy zbudowane na bazie trudnych zagadnień algebraicznych. Nie są to kryptosystemy powszechnie stosowane. Autor raczej próbuje nakreślić współczesne tendencje kryptografii teoretycznej, niż daje gotowe recepty algorytmów szyfrujących. Kryptosystemy niejawnie wielomianowe i ich kryptoanaliza są przedmiotem rozważań rozdziału czwartego podręcznika. System Imaiego–Matsumota (związany z problematyką rozszerzeń algebraicznych ciał skończonych) zostaje poddany gruntownej analizie, która owocuje systemami o większej złożoności obliczeń kryptoanalitycznych i projektem bezpiecznego systemu szyfrującego. Rozdział piąty, to analiza twierdzenia Brassarda. Twierdzenie to, stosowane bez rygorystycznej logiki, neguje istnienie bezpiecznego kryptosystemu kombinatoryczno-algebraicznego. Autor kładzie nacisk na założenia Brassarda i buduje system, który tych założeń nie spełnia. System taki, mimo swej kombinatoryczno-algebraicznej struktury, nie podlega regułom brassardowskiej kryptoanalizy i wydaje się być systemem bezpiecznym. Ostatni rozdział jest celem całego cyklu wykładów. Szyfry w nim rozważane wynikają z trudności obliczeniowych związanych z badaniami krzywych eliptycznych i hipereliptycznych nad ciałami o dowolnej charakterystyce. Książka kończy się dodatkiem "Elementarny wstęp do krzywych hipereliptycznych", ściśle związanym z treścią rozdziału piątego.

Po każdym podrozdziale następuje zestaw ćwiczeń (odpowiedzi do nich umieszczone są na końcu podręcznika). Pozwala on sprawdzić czytelnikowi stopień przyswojenia wiedzy kryptologicznej oraz naświetla niektóre problemy, które w głównym tekście poruszone są jedynie szkicowo.

Pierwsze trzy rozdziały książki można śmiało polecić każdemu, kto dysponując pewnym zasobem matematycznej wiedzy chciałby zorientować się w przedmiocie współczesnej kryptografii. Trzy kolejne wymagają większego zaangażowania czytelnika i mogą być doskonałym materiałem do monograficznego wykładu. *Wiesław Cupała*