Notka biograficzna

Dr hab. inż. Czesław Kościelny jest profesorem Wrocławskiej Wyższej Szkoły Informatyki Stosowanej. Pracował na wielu uczelniach m. in. Politechnice Wrocławskiej, Uniwersytecie Zielonogórskim, Politechnice Zielonogórskiej, Wyższej Szkole Inżynierskiej w Zielonej Górze, Instytucie Automatyki Systemów Energetycznych we Wrocławiu, a także w Algierii w charakterze wykładowcy. Jest autorem ponad 80 publikacji. Naukowo zajmuje się m. in. kryptografią, a jego najnowsze prace aplikacyjne można znaleźć pod adresem: $http : //www.maplesoft.com/applications/app\_center_advanced\_search.aspx?ABA = 16738$

Dr Mirosław Kurkowski jest z wykształcenia matematykiem, doktorat z informatyki obronił w Instytucie Podstaw Informatyki PAN w Warszawie. Przez kilkanaście lat pracował w Instytucie Matematyki i Informatyki Akademii Jana Długosza w Częstochowie. Obecnie jest adiunktem w Instytucie Informatyki Teoretycznej i Stosowanej Politechniki Częstochowskiej. Od 2000 jest członkiem grupy badawczej zajmującej się weryfikacją systemów ochrony danych przy IPI PAN. Jest autorem lub współautorem ponad dwudziestu prac naukowych i popularnonaukowych głównie z zakresu kryptografii i jej zastosowań.

Dr hab. Marian Srebrny jest profesorem w Wyższej Szkole Handlowej im. Bolesława Markowskiego w Kielcach i docentem w Instytucie Podstaw Informatyki PAN w Warszawie. Pracował w University of Michigan, Ann Arbor, USA, i w University of Manchester, Wielka Brytania. Realizuje zadania badawcze w IPI PAN na temat Ochrony Danych i Transakcji w Sieciach Teleinformatycznych. Specjalista w zakresie projektowania i weryfikacji poprawności protokołów kryptograficznych, podpisu elektronicznego, wzmocnionej ochrony dostępu, audytu. Był ekspertem Polskiego Towarzystwa Informatycznego, Polskiej Izby Informatyki i Telekomunikacji, sejmowej komisji d.s. podpisu elektronicznego, Departamentu Społeczeństwa Informacyjnego w Ministerstwie Infrastruktury, międzyresortowego zespołu ds. opracowania aktów wykonawczych do ustawy o podpisie elektronicznym. Współautor ustawy o usługach świadczonych drogą elektroniczną. Autor lub współautor kilkunastu artykułów naukowych i popularno-naukowych związanych z ww. tematyką.

Streszczenie

Celem książki jest wielostronne i przystępne przedstawienie najważniejszych obecnie i najciekawszych zagadnień współczesnej kryptografii wraz z zastosowaniami w sieciach komputerowych. Prezentowane są podstawowe pojęcia kryptografii i zasady konstruowania algorytmów szyfrujących. Przedstawiono w sposób przystępny niezbędne do zrozumienia tych algorytmów podstawy matematyczne. Książka omawia stosowane w praktyce algorytmy symetryczne i asymetryczne wraz z ich zastosowaniami. Materiał może stanowić bazę do semestralnego lub rocznego wykładu z kryptografii stosowanej.