prof. dr hab. n. mat. Jerzy Gawinecki, dr inż. Michał Misztal
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Nowe trendy i kierunki badań w kryptografii i kryptoanalizie na świecie i w Polsce

Aktualne trendy badań kryptografii i kryptoanalizy na świecie: ECRYPT — Europejska Sieć Doskonałości Kryptologii, eSTREAM — konkurs na nowy szyfr strumieniowy, przełom w kryptoanalizie funkcji skrótu. Udział polski w projekcie ECRYPT. Przewidywane dalsze kierunki badań w kryptografii i kryptoanalizie: nowy standard funkcji skrótu SHA-3, kontynuacja projektu ECRYPT? Aktualne możliwości naukowo-badawcze w zakresie kryptologii uczelni, instytucji naukowo-badawczych oraz firm kryptograficznych i informatycznych w Polsce.