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

Kryptograficzne funkcje skrótu — aktualny stan badań

Definicja i własności funkcji skrótu. Wymagania bezpieczeństwa i przykłady zastosowań funkcji skrótu. Przykłady funkcji skrótu i typy ich konstrukcji. Najnowsze ataki oraz aktualny stan bezpieczeństwa. Konkurs na nowy standard funkcji skrótu AHS (Advanced Hash Standard): przewidywane wymagania, planowany przebieg, oczekiwane wyniki.