

dr inż. Michał Misztal
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Nowe funkcje skrótu w konkursie SHA-3

Definicja, wymagane własności i zastosowania funkcji skrótu. Wymagania bezpieczeństwa. Przykłady funkcji skrótu. Aktualny stan bezpieczeństwa. Konkurs SHA-3: założenia konkursu, planowany przebieg, zgłoszone algorytmy i ich porównanie.