

## Abstrakt

Koncem 70. let začal vznikat pojem, který dnes označujeme jako kryptografická hašovací funkce. V současnosti jsou tyto funkce spojovány zejména s digitálním podpisem. V roce 2005 byla prolomena celosvětově nejpoužívanější funkce SHA-1. Tato skutečnost vedla k tomu, že v roce 2007 vyhlásil NIST soutěž o vytvoření nového bezpečného hašovacího algoritmu. Práce pojednává problematiku kryptografických hašovacích funkcí od počátku jejich teoretické formulace až po současné dění v této oblasti.

**Klíčová slova:** Kryptografické hašovací funkce, SHA-1, MD5, soutěž NIST