ČESKÁ NORMA

ICS 35.040

Červen 1996

Informační technologie - Bezpečnostní techniky - Hash funkce -
Část 1: Všeobecně

ČSN ISO/IEC 10118-1

36 9930

Information technology - Security techniques - Hash-functions - Part 1: General

Technologies de l'information - Techniques de sécurité - Fonctions de brouillage - Partie 1: Généralités

Informationstechnik - Sicherheitstechniken - Hash - Funktionen - Teil 1: Allgemeines Model

Tato norma je identická s ISO/IEC 10118-1:1994

This standard is identical with ISO/IEC 10118-1:1994

Národní předmluva

Citované normy

ISO/IEC 9797:1994 dosud nezavedena

Vypracování normy

Zpracovatel: INFO 7, Praha

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Prázdná strana!

MEZINÁRODNÍ NORMA
Informační technologie - bezpečnostní techniky - Hash funkce - Část 1: Všeobecně

ISO/IEC 10118-1
První vydání
1994-10-15

MDT 35.040.00

Deskriprory: data processing, information interchange, protection of information, security techniques, generalities.

Obsah strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se účastní tvorby mezinárodních norem prostřednictvím technických komisí ustavených příslušnou organizací pro práci v jednotlivých oblastech technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společného zájmu. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk.

V oblasti informační technologie založily ISO a IEC společnou technickou komisi ISO/IEC JTC 1. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Mezinárodní norma ISO/IEC 10118-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, Informační technologie, Subkomise SC 27, Bezpečnostní techniky.

ISO/IEC se skládá z následujících částí pod společným titulem Informační technologie - Bezpečnostní techniky - Hash funkce:

- Část 1: Všeobecně

- Část 2: Hash funkce používající algoritmus n-bitové blokové šifry

Přílohy A, B a C této části ISO/IEC 10118 mají pouze informativní charakter.

Úvod

Hash funkce mapují libovolné bitové řetězce na daný rozsah. Mohou se používat pro

- zredukování rozsahu zprávy na krátký otisk, určený jako vstup pro mechanismus digitálního podpisu,

- předání daného bitového řetězce uživateli, aniž by došlo k vyzrazení tohoto řetězce.

Účelem ISO/IEC 10118 je poskytnout různé druhy hash funkcí, které jsou vhodné pro bezpečnostní techniky. Hash funkce mohou být používány mimo rámec této mezinárodní normy i pro jiné účely, jako je např. simulace generátoru náhodných čísel.

1 Předmět normy

ISO/IEC 10118 specifikuje hash funkce a je proto použitelná pro zajištění služeb autentizace, integrity a neodmítnutí.

POZNÁMKA - Ve srovnání s výpočtem Kódu autentizace zprávy (Message Authentication Code (MAC)), jehož cílem je zajištění autentizace zprávy využitím tajného klíče, generování hash kódu tajný klíč nezahrnuje. Výpočet MACu nalezne uživatel v ISO/IEC 9797 [1]

Tato část ISO/IEC 10118 obsahuje definice, symboly, zkratky a požadavky, které jsou společné pro obě části ISO/IEC 10118.

-- Vynechaný text --