ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Červen

2001

	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku	ČSN ISO/IEC 10118-4 36 9930

Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic

Technologies de l’information - Techniques de sécurité - Fonctions de brouillage - Partie 4: Fonctions de hachage utilisant l’arithmetic modulaire

Informationstechnik - Sicherheitsverfahren - Hash-Funktionnen - Teil 4: Hash-Funktionnen auf Basis modularer Arithmetik

Tato norma je českou verzí mezinárodní normy ISO/IEC 10118-4:1998. Mezinárodní norma ISO/IEC10118-4:1998 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10118-4:1998. The International Standard ISO/IEC 10118-4:1998 has the status of a Czech Standard.

61283

Národní předmluva

Citované normy

ISO/IEC 10118-1 zavedena v ČSN ISO/IEC 10118-1:1996 (36 9930), Informační technologie - Bezpečnostní techniky - Hash funkce - Část 1: Všeobecně, nahrazena ISO/IEC 10118-1:2000

Vysvětlivky k textu převzaté normy

Po diskusi s odborníky byla přijata změna slova **hash** na slovo **hašovací.**

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku

ISO 10118-4
První vydání
1998-12-15

ICS 35.040

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie 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% hlasujících členů.

Mezinárodní norma ISO/IEC 10118-4 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 10118 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Hash funkce:*

– *Část 1: Všeobecně*

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

– *Část 3: Dedikované hash funkce*

– *Část 4: Hašovací funkce používající modulární aritmetiku*

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

1 Předmět normy

Tato část ISO/IEC 10118 specifikuje dvě hašovací funkce (hash funkce), využívající modulární aritmetiku. Tyto hašovací funkce, které jsou považovány za odolné proti kolizi, komprimují zprávy

libovolné, přitom však omezené délky na hašovací kód (hash kód), jehož délka je určena délkou prvočísla použitého v redukční funkci definované v 7.3. Takto se hašovací kód snadno uzpůsobí na délku vstupu pro jakýkoliv mechanismus (např. algoritmus podpisu, identifikační schéma).

Hašovací funkce specifikované v této části ISO/IEC 10118, nazývané MASH-1 a MASH-2 (Modular Arithmetic Secure Hash) jsou zejména vhodné pro prostředí, ve kterých jsou implementace modulární aritmetiky dostatečné délky již k dispozici. Tyto dvě hašovací funkce se liší pouze exponentem používaným ve funkci zaokrouhlení.

-- Vynechaný text --