

ČESKÁ TECHNICKÁ NORMA

ICS 35.040

2004

Říjen

	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce	ČSN ISO/IEC 10118-3 36 9930
--	--	---------------------------------------

Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions

Technologies de l'information - Techniques de sécurité - Fonctions de brouillage - Partie 3: Fonctions de brouillage dédiées

Informationstechnik - Sicherheitsverfahren - Hash-Funktionen - Teil 3: Dedizierte Hash-Funktionen

Tato norma je českou verzí mezinárodní normy ISO/IEC 10118-3:2004. Mezinárodní norma ISO/IEC 10118-3:2004 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10118-3:2004. The International Standard ISO/IEC 10118-3:2004 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 10118-3 (36 9930) z června 2000.

© Český normalizační institut,

2004

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

71127

Národní předmluva

Změny proti předchozí normě

Ve třetím vydání ISO/IEC 10118-3 je uveden popis celkem sedmi odlišných dedikovaných hašovacích funkcí oproti původním třem.

Citované normy

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

Vysvětlivky k textu převzaté normy

Pro účely této normy se anglický termín round function překládá jako cyklická funkce.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky -
Hašovací funkce - Část 3: Dedikované hašovací funkce

ISO/IEC 10118-3
Třetí vydání
2004-03

Odmítavé stanovisko k manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, ledaže by typy písma, které jsou vloženy, byly používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřejímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytváření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopíí a mikrofilmu, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office
Case postale 56, CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Strana 4

Obsah

Strana

Úvod

.....	9
1 Předmět normy 10	
2 Normativní odkazy 10	
3 Termíny a definice 10	
4 Symboly (a zkrácené termíny)	10
4.1 Symboly specifikované v ISO/IEC 10118-1.....	10
4.2 Symboly specifické pro tuto část ISO/IEC 10118.....	11
5 Požadavky	

.....	12
6	Model pro dedikované hašovací funkce..... 12
7	Dedikovaná hašovací funkce 1 (RIPEMD-160)..... 13
7.1	Parametry, funkce a konstanty..... 13
7.1.1	Parametry..... 13
7.1.2	Konvence řazení bytů..... 13
7.1.3	Funkce..... 13
7.1.4	Konstanty..... 13
7.1.5	Inicializační hodnota..... 13
7.2	Metoda doplnění..... 15
7.3	Popis cyklické funkce..... 16
8	Dedikovaná hašovací funkce 2 (RIPEMD-128)..... 17
8.1	Parametry, funkce a konstanty..... 17

8.1.1	Parametry 17
8.1.2	Konvence řazení bytů 17
8.1.3	Funkce 17
8.1.4	Konstanty 17
8.1.5	Inicializační hodnota 18
8.2	Metoda doplnění 18
8.3	Popis cyklické funkce 18
9	Dedikovaná hařovací funkce 3 (SHA-1).....	19
9.1	Parametry, funkce a konstanty 19
9.1.1	Parametry 19
9.1.2	Konvence řazení bytů 19
9.1.3		

Funkce	20
9.1.4 Konstanty	20
9.1.5 Inicializační hodnota	20
9.2 Metoda doplnění	20
9.3 Popis cyklické funkce	21
10 Dedikovaná hašovací funkce 4 (SHA-256)	22
10.1 Parametry, funkce a konstanty	22
10.1.1 Parametry	22
10.1.2 Konvence řazení bytů	22
10.1.3 Funkce	22

Konstanty	22
10.1.5 Inicializační hodnota	23
10.2 Metoda doplnění	23
10.3 Popis cyklické funkce	23
11 Dedikovaná hašovací funkce 5 (SHA-512)	24
11.1 Parametry, funkce a konstanty	24
11.1.1 Parametry	24
11.1.2 Konvence řazení bytů	24
11.1.3 Funkce	24
11.1.4 Konstanty	25
11.1.5 Inicializační hodnota	25
11.2 Metoda doplnění	

.....	26
11.3 Popis cyklické funkce
.....	26
12 Dedikovaná hašovací funkce 6 (SHA-384).....	27
12.1 Parametry, funkce a konstanty
.....	27
12.1.1 Parametry
.....	27
12.1.2 Konvence řazení bytů
.....	27
12.1.3 Funkce
.....	27
12.1.4 Konstanty
.....	27
12.1.5 Inicializační hodnota
.....	27
12.2 Metoda doplnění
.....	28
12.3 Popis cyklické funkce
.....	28
13 Dedikovaná hašovací funkce 7 (WHIRLPOOL).....	28

13.1	Parametry, funkce a konstanty	28
13.1.1	Parametry	28
13.1.3	Funkce	28
13.1.4	Konstanty	30
13.1.5	Inicializační hodnota	30
13.2	Metoda doplnění	30
13.3	Popis cyklické funkce	30
Příloha A	(informativní) Příklady	32
A.1	Dedikovaná hašovací funkce	32
A.1.1	Příklad 1	32
A.1.2	Příklad 2	32
A.1.3	Příklad 3	

.....	32
A.1.4 Příklad	
4	
.....	
.....	33
A.1.5 Příklad	
5	
.....	
.....	33
A.1.6 Příklad	
6	
.....	
.....	34
A.1.7 Příklad	
7	
.....	
.....	34
A.1.8 Příklad	
8	
.....	
.....	34
A.1.9 Příklad	
9	
.....	
.....	36
A.1.10 Příklad	
10	
.....	
.....	36
A.1.11 Příklad	
11	
.....	
.....	37

A.2 Dedikovaná hašovací funkce	
2.....	41
A.2.1 Příklad	
1	
.....	
.....	37
A.2.2 Příklad	

2	37
A.2.3	Příklad	
3	37
A.2.4	Příklad	
4	38
A.2.5	Příklad	
5	38
A.2.6	Příklad	
6	38
A.2.7	Příklad	
7	39
A.2.8	Příklad	
8	39
A.2.9	Příklad	
9	41
A.2.10	Příklad	
10	41
A.2.11	Příklad	
11	41
A.3	Dedikovaná hašovací funkce	
3	41
A.3.1	Příklad	

1

.....
..... 41

A.3.2 Příklad

2

.....
..... 42

A.3.3 Příklad

3

.....
..... 42

A.3.4 Příklad

4

.....
..... 43

A.3.5 Příklad

5

.....
..... 43

A.3.6 Příklad

6

.....
..... 43

A.3.7 Příklad

7

.....
..... 43

A.3.8 Příklad

8

.....
..... 44

A.3.9 Příklad

9

.....
..... 46

A.3.10 Příklad

10

.....
..... 46

A.3.11 Příklad

11

.....

.....	47
A.4 Dedikovaná hašovací funkce	
4.....	47
A.4.1 Příklad	
1	
.....	
.....	47
A.4.2 Příklad	
2	
.....	
.....	47
A.4.3 Příklad	
3	
.....	
.....	47
A.4.4 Příklad	
4	
.....	
.....	49
A.4.5 Příklad	
5	
.....	
.....	49
A.4.6 Příklad	
6	
.....	
.....	49
A.4.7 Příklad	
7	
.....	
.....	49
A.4.8 Příklad	
8	
.....	
.....	49
A.4.9 Příklad	
9	
.....	
.....	52
A.4.10 Příklad	
10	
.....	

.....	52
A.4.11 Příklad	
11	
.....	
.....	52
A.5 Dedicovaná hašovací funkce	
5.....	52
A.5.1 Příklad	
1	
.....	
.....	52
A.5.2 Příklad	
2	
.....	
.....	53
A.5.3 Příklad	
3	
.....	
.....	53
A.5.4 Příklad	
4	
.....	
.....	56
A.5.5 Příklad	
5	
.....	
.....	56

A.5.6 Příklad	
6	
.....	
.....	56
A.5.7 Příklad	
7	
.....	
.....	56
A.5.8 Příklad	
8	

.....
..... 57

A.5.9 Příklad
9

.....
..... 57

A.5.10 Příklad
10

.....
..... 57

A.5.11 Příklad
11

.....
..... 63

A.6 Dedikovaná hašovací funkce

6..... 63

A.6.1 Příklad
1

.....
..... 63

A.6.2 Příklad
2

.....
..... 64

A.6.3 Příklad
3

.....
..... 64

A.6.4 Příklad
4

.....
..... 67

A.6.5 Příklad
5

.....
..... 67

A.6.6 Příklad
6

.....
..... 67

A.6.7 Příklad
7

.....	67
A.6.8 Příklad	
8	
.....	68
A.6.9 Příklad	
9	
.....	68
A.6.10 Příklad	
10	
.....	68
A.6.11 Příklad	
11	
.....	74
A.7 Dedikovaná hašovací funkce	
7.....	74
A.7.1 Příklad	
1	
.....	74
A.7.2 Příklad	
2	
.....	74
A.7.3 Příklad	
3	
.....	75
A.7.4 Příklad	
4	
.....	77
A.7.5 Příklad	
5	
.....	77
A.7.6 Příklad	
6	

.....	78
A.7.7 Příklad	
7	
.....	78
A.7.8 Příklad	
8	
.....	78
A.7.9 Příklad	
9	
.....	83
Příloha B (informativní) Formální	
specifikace.....	84
B.0	
Úvod	
.....	84
B.1 Specifikace dedikované hašovací funkce	
1.....	84
B.1.1 Pomocné	
funkce	
.....	91
B.2 Specifikace Dedikované hašovací funkce	
2.....	91
B.3 Specifikace Dedikované hašovací funkce	
3.....	93
Příloha C (normativní) Modul	
ASN.1	
.....	97
Bibliografie	
.....	100

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 příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

ISO/IEC 10118-3 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

Toto třetí vydání ruší a nahrazuje druhé vydání (ISO/IEC 10118-3:2003), které bylo technicky revidováno.

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

- Část 1: Všeobecně
- Část 2: Hašovací funkce používající *n*-bitovou blokovou šifru
- Část 3: Dedikované hašovací funkce
- Část 4: Hašovací funkce používající modulární aritmetiku

Strana 9

Úvod

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že některé prvky této mezinárodní normy mohou být předmětem patentových práv.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je prohlášení držitele tohoto patentovaného práva registrováno u ISO a IEC. Informace lze získat u:

ISO/IEC JTC1/SC27 Standing Document 8 (SD8) "Patent Information"

Standing Document 8 (SD8) je veřejně přístupný na: <http://www.ni.din.de/sc27>.

Je třeba upozornit, že některé prvky této části mezinárodní normy mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřijímají odpovědnost za identifikaci některých nebo všech patentových práv.

Strana 10

1 Předmět normy

Tato část ISO/IEC 10118 specifikuje dedikované hašovací funkce, tj. specificky navržené dedikované funkce. Hašovací funkce v této části ISO/IEC 10118 jsou založeny na iterativním použití cyklické funkce. Je specifikováno sedm odlišných cyklických funkcí, z nichž vzniknou odlišné dedikované hašovací funkce.

První a třetí dedikované hašovací funkce popsané v kapitole 7 a 9 poskytují hašovací kódy dlouhé až 160 bitů; druhá funkce uvedená v kapitole 8 poskytuje hašovací kódy dlouhé až 128 bitů; čtvrtá funkce uvedená v kapitole 10 poskytuje hašovací kódy dlouhé až 256 bitů; šestá funkce uvedená v kapitole 12 poskytuje hašovací kódy pevné délky 384 bitů; a pátá a sedmá funkce uvedené v kapitolách 11 a 13 poskytují hašovací kódy dlouhé až 512 bitů.

-- Vynechaný text --