

2005

	Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně	ČSN ISO/IEC 15946-1 36 9794
---	---	---------------------------------------

Information technology - Security techniques - Cryptographic techniques based on elliptic curves -
Part 1: General

Technologies de l'information - Techniques de sécurité - Techniques cyrptographiques basées sur les
courbes
elliptiques - Partie 1: Généralités

Informationstechnik - IT-Sicherheitsverfahren - Kryptographische Techniken auf Basis von eliptischen
Kurven -
Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-1:2002. Mezinárodní norma
ISO/IEC 15946-1:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15946-1:2002. The
International
Standard ISO/IEC 15946 -1:2002 has the status of a Czech Standard.

© Český normalizační institut,
2005

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

71863

Národní předmluva

Citované normy

ISO/IEC 9796 (všechny části) zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Digitální podpisy umožňující obnovu zprávy

ISO/IEC 9797 (všechny části) zavedena v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC)

ISO/IEC 10118 (všechny části) zavedena v ČSN ISO/IEC 10118 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 11770-3 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 14888 (všechny části) zavedena v ČSN ISO/IEC 14888 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem

ISO/IEC 15946-2:2002 dosud nezavedena

ISO/IEC 15946-3:2002 dosud nezavedena

ISO/IEC 15946-4:2004 dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky -
Kryptografické techniky založené na eliptických křivkách -
Část 1: Všeobecně

ISO/IEC 15946-1
První vydání
2002-12

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 nepřijímá 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 fotokopí 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

..... 6

1 Předmět
normy

..... 7

2 Normativní
odkazy

..... 7

3 Symboly (a zkrácené
termíny)

..... 8

4 Definice polí a
křivek

..... 8

4.1 Konečná
pole

..... 8

4.1.1 Konečná prvočíselná
pole

..... 8

4.1.2 Konečná pole řádu

2^m	9
4.1.3 Konečná pole $F(p^m)$	9
4.2 Eliptické křivky nad $F(p)$, $F(2^m)$ a $F(p^m)$	10
4.2.1 Definice eliptických křivek nad $F(p)$	10
4.2.2 Definice eliptických křivek nad $F(2^m)$	10
4.2.3 Definice eliptických křivek nad $F(p^m)$	10
4.2.4 Definice termínu slabá křivka	11
4.2.5 Zákon grupy u eliptických křivek	11
4.2.6 Opačný bod nad $F(p)$ a $F(p^m)$)	11
4.2.7 Opačný bod na eliptické křivce nad $F(2^m)$	11
4.2.8 Násobení celých čísel a problém diskretních logaritmů eliptických křivek	11
4.2.9 Bod eliptické křivky jako předmět konverze na celé číslo	11
5 Parametry domény eliptické křivky a jejich validace	11
5.1 Parametry domény eliptické křivky a jejich validace nad $F(p)$ a $F(p^m)$	12
5.1.1 Parametry domény eliptické křivky nad $F(p)$ a $F(p^m)$	12
5.2 Validace parametrů domény eliptické křivky nad $F(p)$ a $F(p^m)$ (Volitelné)	12
5.3 Parametry domény eliptické křivky a jejich validace nad $F(2^m)$	12
5.3.1 Parametry domény eliptické křivky nad $F(2^m)$	12

5.3.2	Validace parametrů domény eliptické křivky nad $F(2^m)$ (Volitelné).....	13
6	Generování dvojice klíčů eliptické křivky a validace veřejných klíčů.....	13
6.1	Generování klíče I.....	13
6.1.1	Generování klíče II.....	13
7	Validace veřejného klíče (Volitelná).....	14
Příloha A	(informativní) Základní informace o eliptických křivkách.....	15
Příloha B	(informativní) Příklady.....	27
	Bibliografie	29

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 3 Direktiv 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 15946-1 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

ISO/IEC 15946 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách*:

- Část 1: Všeobecně
- Část 2: Digitální podpisy
- Část 3: Ustavení klíčů
- Část 4: Digitální podpisy umožňující obnovu zprávy

Přílohy A a B této části mezinárodní normy ISO/IEC 15946 mají pouze informativní charakter.

Strana 6

Úvod

Jednou z nejzajímavějších alternativ k systémům založeným na RSA a $GF(p)$, které jsou v současné době dostupné, jsou kryptografické systémy založené na eliptických křivkách definovaných nad konečnými poli. Koncept kryptografického systému s veřejným klíčem založeného na eliptické křivce je poměrně jednoduchý:

- Každá eliptická křivka má binární operaci „+“, pomocí které vytváří konečnou abelovskou grupu.
- Zákon grupy se u eliptických křivek rozšiřuje přirozeným způsobem k „diskrétní exponenciaci“ bodové grupy eliptické křivky.
- Na základě diskrétní exponenciace eliptické křivky je možné snadno odvodit obdoby eliptické křivky z dobře známých schémat s veřejným klíčem Diffie-Hellmana a El Gamala.

Bezpečnost takového systému s veřejným klíčem závisí na obtížnosti určení diskrétních logaritmů v grupě bodů eliptické křivky. Tento problém je - při současné úrovni znalostí - mnohem obtížnější než faktorizace celých čísel nebo výpočet diskrétních logaritmů v konečném poli. Ve skutečnosti od té doby, co Miller a Koblitz v r. 1985 nezávisle navrhli použití eliptických křivek u kryptografických systémů s veřejným klíčem, nebyl zaznamenán žádný významný pokrok ve vypořádání se s problémem diskrétního logaritmu eliptických křivek. Obecně platí, že určit diskrétní logaritmy eliptických křivek jsou schopné pouze algoritmy, které vyžadují exponenciální čas. Je proto možné u systémů s veřejným klíčem založených na eliptických křivkách použít daleko kratší parametry než je tomu u systému RSA nebo klasických systémů založených na diskrétních logaritmech, které využívají multiplikativní grupu některého konečného pole. To přináší významně kratší digitální podpisy a systémové parametry a vyhýbá se použití výpočtů s mimořádně velkými celými čísly.

Tato část ISO/IEC 15946 popisuje matematický základ a všeobecné techniky nutné pro implementaci jakéhokoliv mechanismu popsaného v dalších částech ISO/IEC 15946.

Cílem tohoto dokumentu je uspokojit rostoucí zájem o technologie s veřejným klíčem založené na eliptických křivkách a popsat komponenty, které jsou nutné pro implementaci systému bezpečného digitálního podpisu založeného na eliptických křivkách. Jsou popsána schémata pro výměnu klíčů, transport klíčů a digitální podpisy, které jsou založeny na problému diskrétních logaritmů eliptických křivek.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této mezinárodní normě může

zahrnovat použití patentů.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu jsou prohlášení držitelů těchto patentovaných práv registrována u ISO a IEC. Informace lze získat u:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) "Patent Information"

SD 8 je veřejně dostupný na: <http://www.din.de/ni/sc27>

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

Strana 7

1 Předmět normy

Mezinárodní norma ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách. Tyto techniky zahrnují ustavení klíčů pro systémy s tajným klíčem a mechanismy digitálního podpisu.

Tato část ISO/IEC 15946 popisuje matematický základ a všeobecné techniky nezbytné pro implementaci kteréhokoliv mechanismu popsaného v dalších částech ISO/IEC 15946.

Předmět této normy je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli mocnin řádu prvočísel (včetně speciálních případů řádu prvočísel s charakteristikou dvě). Reprezentace prvků vlastních konečných polí (tj. jejichž báze je použita) je mimo rozsah této normy.

Mezinárodní norma ISO/IEC 15946 nespecifikuje implementaci technik, které definuje. Není tedy zaručena interoperabilita produktů vyhovujících této mezinárodní normě.

-- Vynechaný text --