ISIRI
10824-3
1st.edition

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان استاندارد و تحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۰۸۲۴ -۳
چاپ اول

فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمز نگاری- قسمت ۳: رمزهای بلوکی

Information technology- Security techniques - Encryption algorithms - Part 3: Block ciphers

به‌نام خدا

آشنایی با سازمان استاندارد و تحقیقات صنعتی ایران

سازمان استانداردوتحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱ تنها مرجع رسمی کشوراست که وظیفه تعیین، تدوین ونشراستانداردهای ملی(رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان* صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین‌ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان استاندارد تشکیل می‌دهد به تصویب رسیده باشد.سازمان استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد(ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی(OIML) [3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی(CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای‌عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان استاندارد این‌گونه سازمان-ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آنها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است

---

* سازمان استاندارد و تحقیقات صنعتی ایران

1 - International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization for Legal Metrology (Organization International de Metrologie Legal)
4 - Contact point
5 - Codex Alimentarius Commission

سازمان استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱)
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه : www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱) ، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۹۰۰۰ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Price 9000 Rls.

کمیسیون فنی تدوین استاندارد

" فناوری اطلاعات- فنون امنیتی-الگوریتم‌های رمز نگاری- قسمت سوم: رمزهای بلوکی"

رئیس:	**سمت یا نمایندگی**
خالقی، محمود (فوق لیسانس مخابرات)	عضو هیأت علمی مرکز تحقیقات مخابرات ایران
دبیر:	
تدین، محمد حسام (دکتری ریاضی کاربردی)	عضو هیأت علمی مرکز تحقیقات مخابرات ایران
اعضاء:	
سلماسی زاده، محمود (دکتری کامپیوتر)	عضو هیأت علمی دانشگاه صنعتی شریف
میرقدری، عبدالرسول (دکتری آمار و ریاضی)	عضو هیأت علمی دانشگاه امام حسین (ع)
طباطبایی، سید امیر حسین (فوق‌لیسانس ریاضی کاربردی)	کارشناس شرکت صنایع الکترونیک زعیم
خراسانی، شاهین (لیسانس کامپیوتر)	کارشناس شرکت امن افزار گستر شریف
آزادی ابد، سیامک (لیسانس کامپیوتر)	کارشناس شرکت کیش ویر
رمضان زاده، محمد تقی (لیسانس کامپیوتر)	کارشناس شرکت کیش ویر
پیری، بهرام (لیسانس کامپیوتر)	کارشناس شرکت سامانه‌های امن
حبیبی، هاشم (فوق‌لیسانس کامپیوتر-امنیت شبکه)	کارشناس ارشد صنایع هوافضا
بلندقامت آذر، حسین (فوق‌لیسانس کامپیوتر-امنیت شبکه)	کارشناس ارشد شرکت سهامی بیمه ایران
صابری، جواد (فوق‌لیسانس مخابرات رمز)	کارشناس گروه فناوری امنیت اطلاعات و سامانه‌ها- مرکز تحقیقات مخابرات ایران
عمرانی، آزاده	کارشناس گروه فناوری امنیت اطلاعات و سامانه‌ها- مرکز

(فوق لیسانس امنیت فناوری اطلاعات) تحقیقات مخابرات ایران

برزگر، مریم کارشناس گروه فناوری امنیت شبکه- مرکز تحقیقات مخابرات
(فوق لیسانس کامپیوتر) ایران
عنایتی، علیرضا کارشناس گروه فناوری امنیت شبکه- مرکز تحقیقات مخابرات
(فوق لیسانس مخابرات) ایران

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی-الگوریتم‌های رمز نگاری- قسمت سوم: رمزهای بلوکی» که پیش‌نویسِ آن توسط مرکز تحقیقات مخابرات ایران و **بر اساس راهنمای ۲۱ ایزو" پذیرش منطقه‌ای یا ملی استانداردهای بین المللی و دیگر مدارک استاندارد"** درکمیسیون‌های مربوط تهیه و تدوین شده و در ۵۷ امین جلسه‌ی کمیته‌ی ملی رایانه و فرآوری داده‌ها مورخ ۸۷/۹/۲۵ مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات موسسه‌ی استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱ به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر گونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارایه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین همواره از آخرین تجدیدنظر آنها استفاده می‌گردد.

در تدوین این استاندارد ملی ایران و استاندارد زیر به‌صورت الزام‌آور مورد ارجاع قرار گرفته است:

1. ISO/IEC 18033-3:2005(E), Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.

فناوری اطلاعات- فنون امنیتی-الگوریتم‌های رمز نگاری- قسمت سوم: رمزهای بلوکی

هدف و دامنه کاربرد

هدف از تدوین این استاندارد، که قسمت سوم از مجموعه استانداردهای ملی ۱۰۸۲۴ است، معرفی رمزهای بلوکی است. یک رمز بلوکی، تحت کنترل یک کلید k بیتی، قالب‌های n بیتی را به قالب‌های n بیتی نگاشت می-کند. در مجموع شش رمز بلوکی مختلف ارایه می‌شوند که طبق جدول زیر دسته بندی شده‌اند.

طول بلوک	نام الگوریتم	طول کلید
۶۴ بیت	TDEA	۱۲۸ یا ۱۹۲ بیت
	MISTY1	۱۲۸ بیت
	CAST-128	
۱۲۸ بیت	AES	۱۲۸، ۱۹۲یا ۲۵۶ بیت
	Camellia	
	SEED	۱۲۸ بیت

به هر یک از الگوریتم‌های معرفی شده در این قسمت از این مجموعه استانداردهای ملی ، یک شناسه شی[۲] نسبت داده می‌شود که مطابق با استاندارد ISO/IEC 9834 است. فهرست شناسه اشیای منتسب، در ضمیمه B استاندارد آورده شده است. هر تغییری در مشخصات الگوریتم که منتج به تغییر رفتار عملکردی الگوریتم شود، شناسه شی منتسب به الگوریتم را تغییر خواهد داد.

به‌کارگیری سایر بندهای استاندارد بین‌المللی ISO/IEC 18033-3:2005(E) در مورد این استاندارد ملی الزامی می‌باشد.

2 - Object Identifier