INSO-ISO-IEC
9797-1
1st. Edition
Identical with ISO/IEC 9797-1 : 2011
Apr.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران-ایزو-آی ای سی
۹۷۹۷-۱
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام (MAC) – قسمت ۱: ساز و کارهای های استفاده از رمزگذاری بلوکی

Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5]در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی 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 استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها 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 .

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

کمیسیون فنی تدوین استاندارد

" فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام (MAC) – قسمت ۱: ساز و کارهای استفاده از رمزگذاری بلوکی"

رئیس:	**سمت و/ یا نمایندگی**
نوری مطلق،محمد (فوق لیسانس مهندسی IT-سیستم های اطلاعاتی)	مدرس دانشکده فنی و مهندسی اسفراین
دبیر:	
حصاری، مجتبی (فوق لیسانس ریاضی کاربردی-کنترل بهینه و تحقیق در عملیات)	پژوهشکده کیمیاگران ارتیان
اعضاء: (اسامی به ترتیب حروف الفبا)	
افشاری، مریم (لیسانس مهندسی نساجی)	پژوهشگر شرکت پژوهشکده کیمیاگر-ان ارتیان
امیدوار، مهدی (لیسانس کامپیوتر)	رئیس اتحادیه شرکت های فنی مشاوره ای، خدمات رایانه، تایپ و تکثیر و کانون های تبلیغاتی
ثمینی، محمود (فوق لیسانس مدیریت)	کارمند استانداری خراسان شمالی
جان پرور، سهیل (لیسانس کامپیوتر-نرم افزار)	مدرس دانشکده دارالفنون بجنورد
جعفری، احسان (فوق لیسانس کامپیوتر-هوش مصنوعی)	هیئت علمی موسسه آموزش عالی اشراق
حاجیان، الهام	هیئت علمی دانشگاه مهندسی بجنورد

(فوق لیسانس کامپیوتر-معماری)	
حصاری، کیان (فوق لیسانس مهندسی مکانیک)	پژوهشگر شرکت پژوهشکده کیمیاگر-ان ارتیان
رحیمی، زکیه (لیسانس ریاضی-کاربردی)	پژوهشگر شرکت پژوهشکده کیمیاگر-ان ارتیان
رحیمی، علی اصغر (لیسانس فناوری اطلاعات)	کارمند پتروشیمی بجنورد
روانی فرد، راهبه (فوق لیسانس کامپیوتر-معماری)	هیئت علمی دانشگاه مهندسی بجنورد
گریوانی، زکیه (لیسانس شیمی)	مدیرعامل شرکت پژوهشکده کیمیا-گران ارتیان
لعل دشتی، راضیه (لیسانس کامپیوتر-مهندسی نرم افزار)	پژوهشگر شرکت پژوهشکده کیمیاگر-ان ارتیان
ملاک زاده، مهتاب (لیسانس مهندسی برق-الکترونیک)	کارشناس نگهداری تعمیرات شرکت آجر ماشینی بجنورد

فهرست مندرجات

پیش‌گفتار

استاندارد " فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام - قسمت ۱: ساز و کارهای استفاده از رمزگذاری بلوکی(MAC) " که پیش نویس آن در کمیسیون فنی مربوط، توسط شرکت پژوهشکده کیمیاگران ارتیان، بر مبنای روش تنفیذ مورد اشاره در راهنمای استاندارد بین‌المللی ISO/IEC Guide21 (پذیرش منطقه ای یا ملی استانداردهای "بین‌المللی / منطقه ای" به عنوان استاندارد ملی ایران، تهیه شده و در دویست و شصت و چهارمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۱/۲۳ مورد تصویب قرار گرفته است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱ به عنوان استاندارد ملی منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهند شد و هر گونه پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد ملی بر اساس پذیرش استاندارد "بین‌المللی" به شرح زیر است:

ISO/IEC 9797-1 : 2011, Information technology-Security techniques-Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher

" فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام (MAC) – قسمت۱:سازوکارهای استفاده از رمزگذاری بلوکی"

۱ هدف و دامنه کاربرد

این استاندارد ملی، بر اساس پذیرش استاندارد بین المللی ISO/IEC 9797-1 :2011 تدوین شده است.

هدف از تدوین این استاندارد تعیین شش الگوریتم کدهای احراز هویت پیام (MAC)[1] است که از یک کلید پنهان[2] و بلوک رمز گذاری nبیتی برای محاسبه mبیت MAC استفاده می کند.

این بخش از ISO/IEC 9797-1 می تواند در خدمت های امنیتی از هر معماری، روش های امنیتی یا کاربردهای امنیتی بکار برده شود.

ساز و کارهای مدیریت کلید، خارج از هدف این بخش از ISO/IEC 9797-1 هستند.

این استاندارد ملی شناسانه[3] شئ را تعیین می کند که در شناسایی هر ساز و کار مطابق با ISO/IEC 8825-1 بکار برده می شود. مثال های عددی و تحلیل های امنیتی از هریک از شش الگوریتم تعیین شده، تهیه شده است و ارتباط این بخش از استاندارد ISO/IEC 9797-1 با استانداردهای قبلی بیان شده است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات، جزئی از این استاندارد ملی ایران محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن، مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آنها مورد نظر است. استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms-Part 3: Block ciphers

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

1- Message Authentication code algorithm
2- Secret
3- Identifier

۱-۳

بلوک[۱]

رشته بیتی به طول n بیت است.

۲-۳

کلید رمزنگاری بلوک[۲]

کلیدی که عملیات رمزنگاری یک بلوک را کنترل می کند.

۳-۳

متن رمزنگاری شده[۳]

داده هایی، که برای مخفی کردن محتوای اطلاعاتشان، تبدیل یافته اند.

۴-۳

یکپارچگی داده[۴]

ویژگی که باعث می شود داده ها بر اثر یک رفتار غیرمجاز تغییر نیافته و خراب نشوند.

۵-۳

رمز گشایی[۵]

معکوس عمل رمزنگاری است.

۶-۳

رمزنگاری[۶]

عملیات برگشت پذیری توسط یک الگوریتم رمزنگاری جهت تبدیل داده ها به متن پیام مخفی[۷] است.

۷-۳

کلید[۸]

دنباله ای از نمادها که عملیات تبدیل رمزنگاری را کنترل می کند.

۸-۳

کلید االگوریتم MAC

کلیدی که عملیات یک الگوریتم MAC را کنترل می کند.

4- block
2 - block cipher key
2- ciphertext
4- data inegrity
5- decryption
5- encryption
6- hide
8- key

۹-۳

کد احراز هویت پیام (MAC)

رشته ای از بیت های خروجی یک الگوریتم MAC هستند.

۱۰-۳

الگوریتم کد احراز هویت پیام[1]

الگوریتمی برای محاسبه تابعی که اجرای آن رشته ای از بیت ها و کلید امنیتی را به رشته ای از بیت ها با طول ثابت نگاشت می کند که دو ویژگی زیر را برآورد می کند:

الف) برای هر کلید و هر رشته ورودی، تابع به طور کارآمدی قابل محاسبه است.

ب) برای هر کلید ثابت و درحالیکه هیچ دانش قبلی از کلید داده نشده است، محاسبه ی ارزش تابع بر روی هر رشته ورودی جدید ، از نظر محاسباتی غیر عملی است و حتی اگر دانشی برای یک گروه از رشته های ورودی ومقادیر متناظر با تابع نیز داده شده باشد، یعنی در جاییکه ارزش i امین رشته ورودی ممکن است پس از مشاهده اولین ارزشهای تابع i-1 (برای اعداد صحیح i>1) مشاهده شود نیز از نظر محاسباتی غیر عملی خواهد بود.

یادآوری ۱: گاهی اوقات به یک الگوریتم MAC ، یک تابع بررسی رمزنگاری نیز گفته می شود.

یادآوری ۲: امکان پذیری محاسباتی وابسته به محیط و نیازهای امنیتی مخصوص کاربر می باشد.

۱۱-۳

رمز گذاری بلوک n بیتی[2]

بلاک رمزگذاری شده با این ویژگی که، بلاک های پیام اصلی و بلاک های پیام رمز شده دارای طول n بیتی می باشند.

۱۲-۳

خروجی تبدیل[3]

تابعی که در پایان الگوریتم MAC قبل از عملیات کوتاه سازی بکار برده می شود.

۱۳-۳

پیام اصلی[4]

اطلاعات رمزنگاری نشده است.

کلیه بندهای استاندارد بین المللی ISO/IEC 9797-1 : 2011 در مورد این استاندارد معتبر و الزامی است.

1- Message Auhentication code algorithm
2- N-bit block cipher
3- Output transformation
4- plaintex