INSO

16196-2

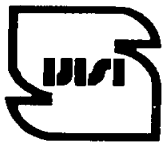
1st. Edition

Apr.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ملی ایران
۲-۱۶۱۹۶

چاپ اول

اردیبهشت ۱۳۹۲

فناوری اطلاعات – فنون امنیتی – طرح‌های امضای رقمی(دیجیتال) با بازیابی پیام
قسمت ۲: سازوکارهای مبتنی بر تجزیه اعداد صحیح

Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery Part 2: Integer Factorization Based Mechanisms

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 صدورگواهی 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 - طرح‌های امضای رقمی (دیجیتال)

با بازیابی پیام - قسمت ۲: سازوکارهای مبتنی بر تجزیه اعداد صحیح»

رئیس :	**سمت و/ یا نمایندگی**
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
دبیر :	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
امیریان، احسان (کارشناس ارشد مهندسی کامپیوتر - نرم‌افزار)	مدیرعامل شرکت هوشمندی تجاری تالی
بختیاری، شیرین (کارشناسی مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس سازمان فناوری اطلاعات
خوشنویسان، نازنین (لیسانس مهندسی نرم‌افزار)	نماینده دانشگاه شهید بهشتی
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات

فیاضی، مهدی (لیسانس مهندسی برق مخابرات)	کارشناس مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
مزینی، ناصر (دکتری کامپیوتر)	استادیار دانشگاه علم و صنعت ایران
معروف، سینا (لیسانس مهندسی کامپیوتر)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
موجبی، محمود (فوق لیسانس مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (لیسانس مهندسی فناوری اطلاعات)	نماینده دانشگاه شهید بهشتی

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی - طرح‌های امضای رقمی (دیجیتال) با بازیابی پیام - قسمت ۲: سازوکارهای مبتنی بر تجزیه اعداد صحیح» که پیش‌نویس آن درکمیسیون های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در اجلاس دویست و پنجاه و سومین کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۱۱/۳ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان 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 زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر 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.
منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 9796-2: 2010, 3rd Ed.: Information technology - Security techniques - Digital Integer factorization based mechanisms - Part 2: Signature schemes giving message recovery

مقدمه

از سازوکارهای امضای رقمی[1](دیجیتال) می‌توان برای فراهم کردن خدماتی از قبیل احراز هویت هستار[2]، احراز هویت منبع داده[3]، عدم انکار[4] و یکپارچگی داده‌ها[5] استفاده کرد. یک سازوکار امضای دیجیتال الزامات زیر را برآورده می‌کند.

- با مشخص بودن کلید درستی‌سنجی[6] و در دسترس نبودن کلید امضاء[7] نمی‌توان یک امضای معتبر را به‌صورت محاسباتی برای پیام‌ها تولید کرد.
- با مشخص بودن امضاهای تولیدشده توسط یک امضاءکننده نمی‌توان به‌صورت محاسباتی یک امضای معتبر را بر روی یک پیام جدید ایجاد یا کلید امضاء را بازیابی کرد.
- نباید محاسباتی وجود داشته باشد که حتی برای یک امضاءکننده، بتوان دو پیام متفاوت با امضای یکسان را یافت.

یادآوری ۱- امکان‌پذیری محاسباتی به نیازهای امنیتی و محیطی مشخص شده وابسته است.

اکثر سازوکارهای امضای دیجیتال مبتنی بر فنون رمزنگاشتی[8] غیرمتقارن بوده و شامل سه عمل پایه زیر هستند:

- فرایندی برای تولید کلیدهای جفتی که هر جفت شامل یک کلید امضای خصوصی و یک کلید درستی‌سنجی عمومی متناظر آن است.
- فرایندی که از کلید امضاء استفاده می‌کند و فرایند امضاء نامیده می‌شود.
- فرایندی که از کلید درستی‌سنجی استفاده می‌کند و فرایند درستی‌سنجی نامیده می‌شود.

دو نوع سازوکار امضای دیجیتال وجود دارد.

- اگر برای یک کلید امضای مشخص دو امضای تولیدشده یکسان باشند، سازوکار غیرتصادفی (یا قطعی) نامیده می‌شود؛ طبق استاندارد ملی ایران به شماره ۱-۱۱۴۹۴: سال ۱۳۸۷.
- اگر برای یک پیام و کلید امضای مشخص، هر بار استفاده از فرایند امضاء یک امضای متفاوت تولید کند، این سازوکار تصادفی نامیده می‌شود.

اولین و سومین مورد از سه سازوکار مشخص‌شده در این استاندارد قطعی (غیرتصادفی) هستند درحالی‌که دومین مورد مشخص‌شده تصادفی است.

سازوکارهای امضای دیجیتال را می‌توان به دو رده‌ی زیر تقسیم کرد:

---

1 - Digital signature
1- Entity authentication
2- Data origin authentication
3- Non-repudiation
4- Integrity of data
5- Verification key
6- Signature key
7- Cryptographic

- زمانی که کل پیام باید به همراه امضاء ذخیره و/یا ارسال شود، این سازوکار «سازوکار امضاء با پیوست» نامیده می‌شود (طبق استاندارد ملی ایران به شماره ۱-۱۱۴۹۴: سال ۱۳۸۷).
- زمانی که کل پیام یا قسمتی از آن را می‌توان از امضاء بازیابی کرد، این سازوکار «سازوکار امضاء با بازیابی پیام» نامیده می‌شود[طبق استاندارد ISO/IEC 9796 (تمامی قسمت‌ها)].

یادآوری ۲- هر سازوکار امضای با بازیابی پیام، مانند سازوکار مشخص شده در استاندارد ISO/IEC 9796 (تمامی قسمت‌ها)، را می‌توان تغییر داد تا یک امضای دیجیتال با پیوست بدهد. این عمل را می‌توان با اعمال سازوکار امضاء به یک کد درهم که به‌عنوان تابعی از پیام به‌دست آمده است انجام داد. در صورت استفاده از این روش، تمام قسمت‌های تولید و درستی‌سنجی امضاها باید طبق این روش عمل کنند. هم‌چنین تمام قسمت‌ها باید این توانایی را داشته باشند که به‌صورت مشخص تابع درهم‌ساز مورد استفاده جهت تولید کد درهم از پیام را تعیین کنند.

سازوکارهای مشخص شده در استاندارد ISO/IEC 9796 (همه قسمت‌ها) بازیابی کامل یا جزیی را با هدف کاهش سربارهای ذخیره‌سازی و انتقال ممکن می‌کنند. اگر پیام به اندازه کافی کوتاه باشد، آن‌گاه کل پیام را می‌توان درون امضاء قرار داد و در فرایند درستی‌سنجی آن را از امضاء بازیابی کرد. در غیر این‌صورت، می‌توان قسمتی از پیام را در امضاء قرار داد و باقی‌مانده آن را ذخیره کرده و/یا به همراه امضاء ارسال نمود.
سازوکارهای مشخص‌شده در این استاندارد از یک تابع درهم‌ساز برای درهم‌سازی کل پیام استفاده می‌کنند. (احتمالاً در بیش از یک قسمت) استاندارد ISO/IEC 10118 توابع درهم‌سازی برای امضاهای دیجیتال را مشخص می‌کند.

فناوری اطلاعات – فنون امنیتی – طرح‌های امضای رقمی (دیجیتال) با بازیابی پیام
قسمت ۲: سازوکارهای مبتنی بر تجزیه اعداد صحیح

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین سه طرح امضای دیجیتال با بازیابی پیام است که دو طرح از آن قطعی (غیرتصادفی) و دیگری تصادفی است. امنیت هر سه طرح مبتنی بر دشواری تجزیه به عامل‌های اعداد بزرگ است. هر سه طرح هم بازیابی کامل و هم بازیابی جزیی را فراهم می‌کنند.
این استاندارد روش تولید کلید برای سه طرح امضاء را مشخص می‌کند. لیکن، فنون مربوط به مدیریت کلید و تولید اعداد تصادفی (موردنیاز طرح امضای تصادفی) خارج از بحث این استاندارد هستند.
اولین سازوکار مشخص شده در این استاندارد فقط برای پیاده‌سازی‌های موجود قابل استفاده است و به دلایل همسازی با سازوکارهای قبلی[1] نگاه داشته شده‌اند.

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 جزیی از این استاندارد ملی ایران محسوب می‌شود.
در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر (و همه اصلاحیه‌ها) مورد نظر است.
استفاده از مرجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 10118 (all parts), Information technology - Security techniques – Hash-functions

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌روند:

۱-۳

ظرفیت

عدد صحیح مثبتی که تعداد بیت‌های در دسترس درون امضاء را برای بخش قابل بازیابی پیام نشان می‌دهد.

1- Backward compatibility

۲-۳

دامنه گواهی

مجموعه‌ای از هستارهای استفاده‌کننده از گواهی‌های کلیدهای عمومی ایجاد شده توسط یک صادرکننده گواهی (CA)[1] یا مجموعه‌ای از صادرکنندگان که تحت یک خط مشی امنیتی واحد عمل می‌کنند.

۳-۳

پارامترهای دامنه گواهی

پارامترهای رمزنگاشتی ویژه یک دامنه گواهی که توسط همه اعضای یک دامنه گواهی شناخته و پذیرفته شده‌اند.

۴-۳

تابع درهم‌ساز مقاوم در برابر برخورد[2]

تابع درهم‌سازی که ویژگی زیر را داشته باشد:

- از نظر محاسباتی امکان نگاشت دو ورودی متمایز به یک خروجی یکسان وجود نداشته باشد.

به ISO/IEC 10118-1 رجوع کنید.

۵-۳

کد درهم[3]

رشته‌ای از بیت‌ها که خروجی یک تابع درهم‌ساز است.

به ISO/IEC 10118-1 رجوع کنید.

۶-۳

تابع درهم‌ساز

تابعی که رشته‌هایی از بیت‌ها را به رشته‌هایی از بیت‌های با طول ثابت می‌نگارد به‌صورتی که دو ویژگی زیر برآورده شوند:

- در مورد یک خروجی معین، از لحاظ محاسباتی یافتن یک ورودی که به این خروجی نگاشته شود، امکان‌پذیر نیست؛

1- Certification Authority
3- Collision-resistant hash-function
3- Hash code

- در مورد یک ورودی معین، از لحاظ محاسباتی یافتن یک ورودی دومی که به خروجی یکسانی نگاشته شود، امکان‌پذیر نیست.
- به ISO/IEC 9797-2 رجوع کنید.

۷-۳

تابع تولید ماسک[1]

تابعی که رشته‌هایی از بیت‌ها را به رشته‌هایی از بیت‌ها با طول مشخص تصادفی می‌نگارد و دارای ویژگی زیر است:

- این امکان محاسباتی وجود نداشته باشد که تنها با معلوم بودن قسمتی از یک خروجی و نه ورودی بتوان قسمت دیگر خروجی را پیش‌بینی کرد.

۸-۳

پیام

رشته‌ای از بیت‌ها با هر طولی

طبق استاندارد ملی ایران شماره ۱-۱۱۴۹۴: سال ۱۳۸۷.

۹-۳

نماینده پیام

رشته بیتی که به‌عنوان تابعی از پیام به‌دست آمده است و با کلید امضای خصوصی ترکیب می‌شود تا امضاء به‌دست آید.

۱۰-۳

نیبل[2]

بلوکی از چهار بیت متوالی (نصف یک هشت‌تایی[3])

۱۱-۳

قسمت غیرقابل بازیابی

قسمتی از پیام که ذخیره‌شده یا به همراه امضاء ارسال شده است؛ این قسمت زمانی که بازیابی پیام کامل باشد، خالی است.

---

1 - Mask
1- Nibble
2- Octet

۱۲-۳

هشت‌تایی

رشته هشت بیتی

۱۳-۳

کلید خصوصی[1]

کلید مربوط به جفت کلید نامتقارن یک هستار که رمز آن را حفظ کرده و تنها باید توسط آن هستار استفاده شود.

به ISO/IEC 9798-1 رجوع کنید.

۱۴-۳

کلید امضای خصوصی

کلید خصوصی که تبدیل امضای خصوصی را تعریف می‌کند.

به ISO/IEC 9798-1 رجوع کنید.

۱۵-۳

کلید عمومی

کلید مربوط به جفت کلید نامتقارن یک هستار که می‌تواند عمومی شود.

به ISO/IEC 9798-1 رجوع کنید.

۱۶-۳

سامانه کلید عمومی

طرح رمزنگاشتی «امضای دیجیتال» شامل سه تابع است:

- *تولید کلید*: روشی برای تولید یک جفت کلید که شامل یک کلید امضای خصوصی و یک کلید درستی‌سنجی خصوصی است؛
- *تولید امضاء*: روشی برای تولید یک امضاء Σ از یک نمایشگر پیام F و یک کلید امضای خصوصی؛
- *گشایش امضاء*[2]: روشی برای به‌دست آوردن نمایشگر پیام بازیابی‌شده F^* از امضاء Σ و کلید درستی‌سنجی عمومی.

1- Private key
2- Signature opening

یادآوری – خروجی این تابع همچنین حاوی یک نشانه است که موفقیت یا عدم موفقیت رویه گشایش امضاء را نشان می‌دهد.

۱۷-۳

کلید درستی‌سنجی عمومی

کلید عمومی که تبدیل درستی‌سنجی عمومی را مشخص می‌کند.

به ISO/IEC 9798-1 رجوع کنید.

۱۸-۳

قسمت قابل بازیابی

قسمتی از پیام انتقال یافته در امضاء

۱۹-۳

سالت[1]

داده تصادفی تولیدشده توسط هستار امضاءکننده به هنگام ایجاد نمایش‌گر پیام در طرح امضای ۲

۲۰-۳

امضاء

رشته‌ای از بیت‌های حاصل‌شده از فرایند امضاء

طبق استاندارد ملی ایران شماره ۱-۱۱۴۹۴: سال ۱۳۸۷.

۲۱-۳

پشت‌بند[2]

رشته‌ای از بیت‌ها با طول یک یا دو هشت‌تایی که هنگام ایجاد نمایشگر پیام به انتهای قسمت قابل بازیابی پیام متصل می‌شود.

۴ نمادها و کوته‌نوشت‌ها

در این استاندارد، نمادها و کوته‌نوشت‌های زیر به‌کار می‌روند:

یادآوری – در بیشتر موارد، از حروف بزرگ برای نمایش رشته‌های بیت و رشته‌های هشت‌تایی استفاده می‌شود درحالی که حروف کوچک برای نمایش توابع به‌کار می‌روند.

1 - Salt
2 - Trailer

C رشته هشت‌تایی که طول بیت قسمت قابل بازیابی پیام را کدبندی می‌کند (و در ایجاد نمایشگر پیام در طرح‌های امضای ۲ و۳ به کار می‌رود).

c ظرفیت طرح امضاء یا به عبارتی بیشترین تعداد بیت‌های در دسترس برای قسمت قابل بازیابی پیام

c^* طول پیام قابل بازیابی یا به عبارتی طول قسمت قابل بازیابی پیام به واحد بیت ($c \geq c^*$)

رشته‌های بیت ساخته شده در هنگام ایجاد نمایشگر پیام در طرح‌های امضای ۲ و۳

رشته‌های بیت ساخته شده در هنگام بازیابی پیام در طرح‌های امضای ۲ و۳

F نمایشگر پیام (یک رشته بیت)

F^* نمایشگر پیام بازیابی شده (به عنوان خروجی در مرحله گشایش امضاء)

G تابع تولید ماسک

H کد درهم محاسبه شده به عنوان تابعی از پیام M (یک رشته بیت)

H^* کد درهم بازیابی شده به دست آمده در مرحله بازیابی پیام

H تابع درهم‌ساز مقاوم در برابر برخورد

K طول بیت پیمانه‌های کلید امضای خصوصی و کلید درستی‌سنجی عمومی (به پیوست الف مراجعه شود)

طول بیت کدهای درهم تولید شده توسط تابع درهم‌ساز h

طول بیت سالت S

M پیامی که امضاء می‌شود (یک رشته بیت)

M^* پیامی که از یک امضاء به عنوان نتیجه فرایند درستی‌سنجی بازیابی می‌شود

قسمت قابل بازیابی پیام M؛ یعنی $M = M_1 \,||\, M_2$

قسمت قابل بازیابی بازیابی شده پیام (تولید شده به هنگام بازیابی پیام)

قسمت غیرقابل بازیابی پیام M؛ یعنی $M = M_1 \,||\, M_2$

قسمت غیرقابل بازیابی پیام به عنوان ورودی فرایند درستی‌سنجی

N رشته بیت ساخته شده به هنگام ایجاد نمایشگر پیام در طرح‌های ۲ و ۳

N^* رشته بیت تولید شده به هنگام بازیابی پیام در طرح‌های ۲ و ۳

P رشته‌ای از بیت‌های صفر ساخته شده به هنگام ایجاد نمایشگر پیام در طرح‌های ۲ و ۳

S سالت (یک رشته بیت)

S^* سالت بازیابی شده (یک رشته بیت)

T تعداد هشت‌تایی‌ها در فیلد پشت‌بند (t مساوی ۱ یا ۲)

T فیلد پشت‌بند (یک رشته با 8t بیت که به هنگام ایجاد نمایشگر پیام استفاده می‌شود)

عدد صحیحی در بازه ۰ تا ۷ که در تعیین تخصیص پیام استفاده می‌شود

عدد صحیحی در بازه ۰ تا ۷ که در تعیین طرح‌های امضای ۲ و۳ استفاده می‌شود

امضاء (یک رشته بیت که شامل k-1 یا k بیت است)

|A| طول بیت رشته بیت A یا به عبارتی تعداد بیت‌های A

A || B سلسله‌بندی رشته‌های بیت A و B (به همان ترتیب)

برای یک عدد حقیقی a، کوچکترین عدد صحیحی که از a کوچکتر نباشد

a mod n برای اعداد صحیح a و n، (a mod n) باقی مانده (غیرمنفی) به‌دست آمده از تقسیم n بر a را مشخص می‌کند. به طور مشابه، اگر b = a mod n باشد، آن‌گاه b یک عدد صحیح یکتا است که موارد زیر را برآورده می‌کند:

الف) $0 \leq b < n$ و

ب) $(b - a)$ یک مضرب صحیح از n است.

عملگر بیتی *یای انحصاری*[1] که برای ترکیب دو رشته دودویی با طول یکسان به کار می‌رود

۵ تبدیل بین رشته‌های بیت و اعداد صحیح

برای نمایش عدد صحیح غیرمنفی x با یک رشته بیتی به طول l (l باید به‌گونه‌ای باشد که $2^l > x$)، عدد صحیح باید به فرم دودویی یکتای زیر نوشته شود:

$$x = 2^{l-1}x_{l-1} + 2^{l-2}x_{l-2} + \cdots + 2x_1 + x_0$$

به‌طوری که $0 < x_i < 2$ (توجه داشته باشید که یک یا چند رقم ابتدایی صفر خواهند بود اگر $x < 2^{l-1}$). رشته بیتی باید به‌صورت زیر باشد:

$$x_{l-1}x_{l-2} \dots x_0.$$

برای نمایش یک رشته بیت $x_{l-1}x_{l-2} \dots x_0$ (به طول l) به‌شکل عدد صحیح x، فرایند وارون فوق باید استفاده شود؛ به‌عبارت دیگر، x عدد صحیحی است که باید به‌صورت زیر تعریف شود:

$$x = 2^{l-1}x_{l-1} + 2^{l-2}x_{l-2} + \cdots + 2x_1 + x_0$$

1 – Bit-wise exclusive-or

۶ الزامات

به کاربران این استاندارد توصیه می‌شود که در صورت امکان از سازوکار دوم استفاده کنند. (طرح امضای دیجیتال ۲) اما در محیط‌هایی که تولید متغیرهای تصادفی توسط امضاءکننده غیرعملی پنداشته می‌شود، استفاده از طرح امضای دیجیتال ۳ توصیه می‌شود.

کاربرانی که می‌خواهند از مکانیزم امضای دیجیتالی مطابق با این استاندارد استفاده کنند، باید از برقرار بودن ویژگی‌های زیر اطمینان حاصل کنند:

الف - پیام M که قرار است امضاء شود باید یک رشته دودویی با هر طولی و احتمالاً خالی باشد.

ب - تابع امضاء از یک کلید امضای خصوصی استفاده می‌کند در حالی که تابع درستی‌سنجی کلید درستی-سنجی عمومی متناظر را به‌کار می‌برد.

- هر هستار امضاءکننده باید از کلید امضای خصوصی متناظر با کلید درستی‌سنجی عمومی خود به‌طور مخفیانه استفاده کند.

- هر هستار درستی‌سنج بهتر است کلید درستی‌سنجی عمومی هستار امضاءکننده را بداند.

پ - استفاده از طرح‌های امضای مشخص شده در این استاندارد، نیازمند انتخاب یک تابع درهم‌ساز مقاوم در برابر برخورد است. توابع درهم‌ساز در استاندارد ISO/IEC 10118 به فرم استاندارد درآورده شده‌اند. باید انقیاد[1] بین سازوکار امضاء و تابع درهم‌ساز مورداستفاده وجود داشته باشد. بدون چنین انقیادی، این امکان وجود دارد که مهاجم از یک تابع درهم‌ساز ضعیف (و نه تابع درهم‌ساز واقعی) استفاده و به این وسیله امضایی را جعل کند.

یادآوری ۱- راه‌های متفاوتی برای به‌دست آوردن این انقیاد وجود دارد. در ادامه گزینه‌های زیر به ترتیب افزایش خطرپذیری[2] فهرست شده‌اند.

۱- نیاز به یک تابع درهم‌ساز ویژه به هنگام استفاده از یک سازوکار امضای ویژه. فرایند درستی‌سنجی باید به‌طور منحصربه‌فرد از این تابع درهم‌ساز ویژه استفاده کند. استاندارد ISO/IEC 14888-3 مثالی از این گزینه را ارائه می‌دهد که در آن سازوکار DSA نیازمند استفاده از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 است (تابع درهم‌ساز شناخته شده با نام SHA-1).

۲- پذیرفتن مجموعه‌ای از توابع درهم‌ساز و اشاره صریح به تابع درهم‌ساز مورد استفاده در پارامترهای دامنه گواهی. در دامنه گواهی، فرایند درستی‌سنجی باید به‌طور منحصربه‌فرد از تابع درهم‌ساز اشاره شده در این گواهی استفاده کند. در خارج از دامنه گواهی، خطری از ناحیه صادرکننده گواهی که از سیاست کاربر پیروی نمی‌کند، وجود دارد. برای مثال، اگر یک CA خارجی یک گواهی ایجاد کند که به توابع درهم‌ساز دیگر مجوز دهد، آن‌گاه مشکلات جعل امضاء به‌روز می‌کند. در چنین حالتی، یک درستی‌سنج گمراه‌شده[3] ممکن است با یک CA که یک گواهی دیگر را ایجاد کرده است، دچار مشکل شود.

1- Binding
2-Risk
3- Misled

۳- پذیرفتن مجموعه‌ای از توابع درهم‌ساز و اشاره به تابع درهم‌ساز مورد استفاده توسط روشی دیگر؛ مثلاً، نشانه‌ای در پیام یا یک پیمان دوسویه[۱]. فرایند درستی‌سنجی باید به‌طور منحصربه‌فرد از تابع درهم‌ساز اشاره شده در روش دیگر استفاده کند. اما، ممکن است مهاجم با استفاده از یک تابع درهم‌ساز دیگر امضایی را جعل کند.

یادآوری ۲- «روش دیگر» که در بند سوم به آن اشاره شد می‌تواند به فرم یک نشانگر تابع درهم‌ساز باشد که در نمایشگر پیام F قرار دارد. (به زیربندهای ۸-۲-۲ و ۹-۲-۳مراجعه شود.) اگر نشانگر تابع درهم‌ساز به این صورت در نمایشگر پیام F قرار داشته باشد، آن‌گاه یک حمله‌کننده نمی‌تواند از یک امضای موجود با M_1 یکسان و M_2 متفاوت استفاده مجدد کند، حتی هنگامی که بتوان درستی‌سنج را متقاعد کرد که امضاهای ایجاد شده از طریق یک تابع درهم‌ساز را که به اندازه کافی ضعیف هستند، بپذیرد. اما همان‌طور که به تفصیل در [16] بحث شده است (به پیوست ت مراجعه شود.)، در این مورد آخر و تابع درهم‌ساز ضعیف، یک حمله‌کننده هنوز می‌تواند یک امضای جدید با یک M_1 «تصادفی» بیابد.

یادآوری ۳- می‌توان با ضروری کردن وجود یک ساختار مشخص در M_1، از حمله اشاره شده در یادآوری ۲ که امضاء جدیدی را با یک M_1 «تصادفی» ارائه می‌دهد، جلوگیری کرد. برای مثال، یک فرد مجاز است که محدودیتی را بر روی طول M_1 قرار دهد به‌طوری که از ظرفیت طرح امضاء به اندازه کافی کمتر باشد. (به پیوست ت مراجعه شود.) برای طرح‌های امضای ۲ و ۳، محدودیت طولی بر روی M_1 می‌تواند از استفاده مجدد حمله‌کننده از امضاهای موجود جلوگیری کند حتی اگر هیچ نشانگر تابع درهم‌سازی درون نمایشگر پیام قرار نداشته باشد؛ البته به شرطی که تابع تولید ماسک g بر اساس تابع درهم‌ساز باشد. این حالت تحت این فرض منطقی برقرار است که تابع درهم‌ساز ضعیف موردبحث یک تابع درهم‌ساز «همه منظوره[۲]» است و تابعی نیست که تنها برای هدف خاص جعل امضاء طراحی شده باشد.

کاربر سازوکار امضای دیجیتال بهتر است یک ارزیابی خطر انجام دهد و در این ارزیابی هزینه‌ها و امتیازات روش‌های مختلف دیگر را برای دستیابی به انقیاد مورد نیاز در نظر بگیرد. این ارزیابی بهتر است ارزیابی هزینه مربوط به امکان تولید امضای جعلی را شامل شود.

ت- درستی‌سنج امضاء باید همیشه وسیله‌ای ایمن و مستقل برای تشخیص این‌که کدام یک از سه طرح امضای مشخص شده در این استاندارد برای تولید امضاء به‌کار رفته‌اند، در اختیار داشته باشد. به‌علاوه، اگر طرح‌های امضاء ۲ و۳ به‌کار رفته باشند، درستی‌سنج باید وسیله‌ای برای تشخیص این‌که کدام یک از دو تابع تولید امضاء مشخص‌شده در پیوست ب مورد استفاده قرار گرفته‌اند را نیز در اختیار داشته باشد. مثلاً، می‌توان با مشخص کردن سازوکار و تابع تولید امضاء در «پارامترهای دامنه» مورد توافق یا قرار دادن یک نشانگر معلوم برای طرح امضاء و تابع تولید امضاء در گواهی کلید عمومی امضاءکننده، به چنین حالتی دست یافت. همچنین این امکان وجود دارد که تابع تولید امضاء در یک الگوریتم نشانگر که به داده‌های امضاء شده مربوط است، مشخص شود.

ث- هر یک از طرح‌های امضای دیجیتال مشخص شده در این استاندارد دارای گزینه‌های خاصی هستند؛ گستره گزینه‌های ممکن هر طرح باید از طریق وسیله‌ای مستقل و ایمن توسط امضاءکننده برای درستی‌سنج شناخته شود. این گزینه‌ها در زیر آورده شده‌اند.

4- Bilateral agreement
2- General purpose

- برای هر سه طرح امضای دیجیتال، درستی‌سنج باید بداند کدامیک از گزینه‌های ۱ و۲ از فیلد پشت‌بند به‌کار می‌رود.
- برای طرح‌های امضای دیجیتال ۲ و ۳، درستی‌سنج باید L_S که طول سالت S است را بداند.

به‌عنوان مثال، برای دستیابی به چنین حالتی می‌توان انتخاب گزینه‌ها را در «پارامترهای دامنه» مشخص کرد یا اطلاعات گزینه‌ها را در گواهی کلید عمومی امضاءکننده قرار داد.

۷ مدلی برای فرایندهای امضاء و درستی‌سنجی

۷-۱ کلیات

مدلی که در اینجا برای طرح امضاء با بازیابی پیام ارائه شده است، برای هر سه طرح امضای دیجیتال در این استاندارد صدق می‌کند. وقتی که این مدل به یک پیام M اعمال شود، این نوع طرح امضاء می‌تواند پیام را به‌صورت کامل یا جزیی بازیابی کند.

- اگر M به اندازه کافی کوتاه باشد، آن‌گاه می‌توان پیام را به‌صورت کامل بازیابی کرد زیرا این امکان برای M وجود خواهد داشت که به‌طور کامل در امضاء قرار داده شود.
- اگر M بیش از حد طولانی باشد، آن‌گاه بازیابی پیام جزیی خواهد بود. در این صورت، M باید به دو قسمت قابل بازیابی و غیرقابل بازیابی تقسیم شود. قسمت قابل بازیابی رشته‌ای از بیت‌ها با طول محدود است که در امضاء قرار داده می‌شود و قسمت غیرقابل بازیابی رشته‌ای از هشت‌تایی‌ها با هر طولی است که ذخیره شده و/یا به همراه امضاء ارسال می‌شود.

این مدل به سه قسمت تقسیم می‌شود: تعیین رویه‌ی برای امضاءکردن یک پیام، تعیین رویه‌ی برای درستی-سنجی یک امضاء و جزییات جنبه‌های اضافی امضاء کردن و درستی‌سنجی. برای این‌که بتوان یک طرح امضاء را کامل کرد لازم است موارد اشاره شده در قسمت آخر مدل تعریف شوند. بندهای ۸، ۹ و ۱۰ این جنبه‌های اضافی را برای سه طرح تعریف شده در این استاندارد مشخص می‌کنند.

۷-۲ امضاء کردن یک پیام

۷-۲-۱ نمای کلی

برای امضاء کردن پیام معین M، نیاز به انجام سه گام داریم: تخصیص پیام، تولید رشته قابل بازیابی و تولید امضاء.

- *تخصیص پیام* شامل فرایندی است که در آن پیام به دو قسمت تقسیم می‌شود: یک قسمت قابل بازیابی M_1 و قسمت غیرقابل بازیابی M_2 (که ممکن است خالی باشد.) طول قسمت قابل بازیابی توسط ظرفیت c طرح امضاء محدود می‌شود که مقدار این ظرفیت با انتخاب طرح امضاء و کلید آن تعیین می‌شود. قسمت قابل بازیابی حین فرایند درستی‌سنجی از امضاء بازیابی می‌شود در حالی که قسمت غیرقابل بازیابی باید با استفاده از شیوه‌های دیگر در اختیار درستی‌سنج قرار گیرد. (مثلاً، می‌توان آن را ارسال

کرده یا با امضاء ذخیره کرد.) از این رو، اگر پیام به اندازه کافی کوتاه باشد، می‌توان کل پیام را به قسمت قابل بازیابی تخصیص داد و قسمت غیرقابل بازیابی خالی خواهد بود.

- *تولید نمایشگر پیام* دو قسمت پیام را به‌عنوان ورودی گرفته و یک رشته قالب‌بندی‌شده را که نمایشگر پیام نامیده می‌شود، به‌عنوان خروجی قرار می‌دهد. این خروجی، ورودی گام تولید امضاء خواهد بود.
- *تولید امضاء* نمایشگر پیام و کلید امضای خصوصی را به‌عنوان ورودی می‌گیرد و امضاء Σ را به‌عنوان خروجی می‌دهد. این فرایند با استفاده از سامانه کلید عمومی انجام می‌شود.

۷-۲-۲ تخصیص پیام

انتخاب طرح امضاء و کلید آن، ظرفیت c امضاء را تعیین می‌کند که در آن c باید رابطه $c \geq 7$ را برآورده کند. پیام M که قرار است امضاء شود باید به‌صورت زیر به دو قسمت M_1 و M_2 تقسیم شود.

طول پیام قابل بازیابی c^* باید به‌گونه‌ای انتخاب شود که $c^* \leq c$ ، $c^* \leq |M|$ و $c^* \equiv |M| \pmod 8$. برای طرح امضای ۱، c^* برابر با کمینه $c - \Delta$ و |M| قرار داده می‌شود به‌طوری‌که $\Delta = (c - |M|) \bmod 8$.

- اگر $c^* = |M|$، آن‌گاه باید کل پیام قابل بازیابی باشد؛ به‌عبارت دیگر، $M_1 = M$ و M_2 باید خالی باشد.
- اگر $c^* > |M|$، آن‌گاه M_1 باید برابر c^* بیت سمت چپ M بوده و M_2 باید برابر باقی‌مانده M باشد؛ به‌عبارت دیگر، M_2 شامل $|M| - c^*$ بیت خواهد بود.

در هر دو صورت داریم: $M = M_1 || M_2$.

یادآوری ۱- در اهداف عملی، کاربر مجاز است پیام M را به‌گونه‌ای ساختاربندی کند که مطمئن شود داده‌هایی را که می خواهد به‌وضوح ذخیره یا ارسال کند (مثلاً اطلاعات نشانی) به قسمت غیرقابل بازیابی پیام یعنی M_2 تخصیص داده شود. به هر حال، ساختار و تفسیر پیام M خارج از بحث این استاندارد است.

یادآوری ۲- روش تخصیص پیام تضمین می‌کند که طول M_2 همیشه تعداد صحیحی از هشت‌تایی‌ها است. علاوه بر این، انتخاب c^* به‌عنوان کمینه $c - \Delta$ و |M| به‌طوری‌که ($\Delta = (c - |M|) \bmod 8$)، تضمین می‌کند که M_1 تا جایی که امکان‌پذیر است، تابع این شرط باشد. همچنین، اگر طول M تعداد صحیحی از هشت‌تایی‌ها باشد، به‌عبارت دیگر، اگر |M| مضرب صحیحی از ۸ باشد آن‌گاه M_1 و M_2 هردو شامل تعداد صحیحی از هشت‌تایی‌ها خواهند بود.

۷-۲-۳ تولید نمایشگر پیام

این گام قسمت‌های قابل بازیابی و غیر قابل بازیابی پیام، M_1 و M_2، را به‌عنوان ورودی دریافت می‌کند و نمایشگر پیام F را خروجی می‌دهد. روش‌های اجرای این گام در بندهای ۸، ۹ و ۱۰ این استاندارد آمده است. این روش‌ها نیازمند استفاده از تابع درهم‌ساز h هستند. در مورد سازوکارهای ۲ و ۳ یک تابع تولید ماسک g که از h نیز استفاده می‌کند مورد نیاز است. تابع درهم‌ساز h باید از بین توابع استاندارد شده در استاندارد ISO/IEC 10118 انتخاب شود؛ تابع تولید ماسک g باید برابر تابع مشخص شده در پیوست پ این استاندارد قرار داده شود.

۷-۲-۴ تولید امضاء

این گام نمایشگر پیام F و کلید امضای خصوصی را به‌عنوان ورودی گرفته و امضاء Σ را خروجی می‌دهد. برای انجام این گام باید از سامانه کلید عمومی مشخص شده در پیوست ب این استاندارد استفاده شود.

۷-۳ درستی‌سنجی یک امضاء

۷-۳-۱ نمای کلی

یک پیام امضاء شده در حالت بازیابی کامل فقط شامل امضاء Σ است و در حالت بازیابی جزیی شامل قسمت غیرقابل بازیابی M_2^* به همراه امضاء Σ است. یک امضاء باید پذیرفته شود اگر و تنها اگر فرایند درستی‌سنجی موفقیت‌آمیز باشد.

با معلوم بودن امضاء Σ و قسمت پیام غیرقابل بازیابی M_2^*، انجام سه گام گشایش امضا، بازیابی پیام و هم‌گذاری پیام[1] برای درستی‌سنجی Σ و بازیابی M^* مورد نیاز خواهد بود.

- *گشایش امضاء*، امضاء Σ و کلید درستی‌سنجی عمومی را به‌عنوان ورودی می‌گیرد و نمایشگر پیام بازیابی شده F^* را خروجی می‌دهد. در غیر این‌صورت، نشانه‌ای را به‌عنوان عدم موفقیت درستی‌سنجی باز می‌گرداند. این فرایند با استفاده از سامانه کلید عمومی انجام می‌گیرد.
- *بازیابی پیام*، نمایشگر پیام بازیابی شده F^* و قسمت غیرقابل بازیابی پیام M_2^* را به‌عنوان ورودی می‌گیرد و قسمت قابل بازیابی (بازیابی شده) پیام M_1^* را خروجی می‌دهد یا این‌که نشانه‌ای را به‌عنوان عدم موفقیت درستی‌سنجی باز می‌گرداند.
- *هم‌گذاری پیام* شامل فرایندی است که در آن پیام بازیابی‌شده M^* از قسمت‌های قابل بازیابی (بازیابی‌شده) M_1^* و غیرقابل بازیابی M_2^* (که ممکن است خالی باشد.) دوباره‌سازی می‌شود.

۷-۳-۲ گشایش امضاء[2]

این گام، امضاء Σ و کلید درستی‌سنجی عمومی را به‌عنوان ورودی می‌گیرد و نمایشگر پیام بازیابی شده F^* را خروجی می‌دهد یا نشانه‌ای را به‌عنوان عدم موفقیت درستی‌سنجی باز می‌گرداند. این فرایند با استفاده از سامانه کلید عمومی که در پیوست ب این استاندارد مشخص شده است، انجام می‌گیرد.

۷-۳-۳ بازیابی پیام

این گام نمایشگر پیام بازیابی شده F^* و قسمت غیرقابل بازیابی پیام M_2^* را به‌عنوان ورودی می‌گیرد و قسمت قابل بازیابی پیام M_1^* را خروجی می‌دهد یا نشانه‌ای را به‌عنوان عدم موفقیت درستی‌سنجی باز می‌گرداند. این فرایند باید با استفاده از یکی از روش‌های مشخص‌شده در بندهای ۸، ۹ و ۱۰ این استاندارد انجام گیرد. این روش‌ها نیازمند استفاده از یک تابع درهم‌ساز و در مورد دومین و سومین سازوکار، یک تابع تولید ماسک هستند.

1- Message assembly
2- Signature opening

تابع درهم‌ساز مورد استفاده باید از میان توابع استاندارد شده استاندارد ISO/IEC 10118 انتخاب می‌شود. تابع تولید ماسک g باید برابر تابع مشخص شده در پیوست پ این استاندارد قرار داده شود.

۷-۳-۴ هم‌گذاری پیام

این گام شامل فرایندی است که در آن پیام بازیابی‌شده M^* از قسمت‌های قابل بازیابی M_1^* و غیرقابل بازیابی M_2^* (که ممکن است خالی باشد.) دوباره‌سازی می‌شود. به‌عبارت دیگر، M^* به‌صورت $M^* = M_1^* \,||\, M_2^*$ ساخته می‌شود.

۷-۴ تعیین یک طرح امضاء

این زیربند توضیح می‌دهد که به چه انتخاب‌هایی نیاز داریم تا فرایندهای امضاء و درستی‌سنجی مشخص شده در این استاندارد را به‌صورت یکتا تعیین کنیم.

الف- مراحل تخصیص و هم‌گذاری پیام به‌صورت یکتا در این قسمت از استاندارد ISO/IEC 9796 تعریف می‌شوند.

ب- یکی از سه گزینه مشخص شده در بندهای ۸، ۹ و ۱۰ این استاندارد باید برای مراحل تولید نمایشگر پیام و بازیابی پیام انتخاب شود. در صورت انتخاب هر کدام از این گزینه‌ها، یک تابع درهم‌ساز نیز باید از بین توابع استاندارد شده استاندارد ISO/IEC 10118 انتخاب شود و این شرط که خروجی تابع درهم‌ساز باید حداقل ۱۶۰ بیت داشته باشد را رعایت کند. در دو مورد از سه گزینه، یک تابع تولید ماسک نیز مورد نیاز است و این تابع در پیوست پ این استاندارد تعریف شده است.

پ- مراحل تولید امضاء و گشایش امضاء تا گام انتخاب کلید امضای خصوصی مورد استفاده در فرایند تولید امضاء به‌صورت یکتا در پیوست ب این استاندارد تعریف شده‌اند. در مورد طرح‌های امضای ۲ و ۳ با توان فرد، مراحل تولید امضاء و گشایش امضاء تا گام انتخاب بین امضای پایه و جایگزین و توابع درستی‌سنجی تعریف شده‌اند. روش مورد استفاده برای تولید جفت کلیدهای امضای خصوصی و جفت کلیدهای درستی‌سنجی عمومی در پیوست ب این استاندارد تعریف شده‌اند.

۸ طرح امضای دیجیتال ۱

۸-۱ کلیات

بند ۸ به تعریف فرآیندهای تولید نمایشگر پیام و بازیابی پیام برای یک طرح امضای دیجیتال قطعی با بازیابی پیام می‌پردازد.

به‌علت وجود امکان حمله (به [5] و [6] مراجعه شود.)، این طرح فقط باید در محیطی مورد استفاده قرار گیرد که در آن محدودیت‌های عملیاتی تضمین می‌کنند که یک مهاجم نمی‌تواند از تعداد زیادی از پیام‌های انتخاب شده امضایی به‌دست آورد.

یادآوری- طرح امضای دیجیتال ۱ بهتر است فقط در محیطی استفاده شود که در آن سازگاری با سامانه‌های پیاده‌کننده اولین ویرایش این استاندارد مورد نیاز است. (به [5] و [6] مراجعه شود.) اما طرح امضای دیجیتال ۱ فقط با سامانه‌هایی سازگار است که اولین ویرایش این استاندارد که از کدهای هش حداقل ۱۶۰ بیتی استفاده می‌کنند را پیاده‌سازی کنند.

۸-۲ پارامترها

۸-۲-۱ طول پیمانه

فرض می‌شود که کلید امضای خصوصی مورد استفاده طول پیمانه‌ای با k بیت دارد(به پیوست ب مراجعه شود). این فرض هم c، ظرفیت امضا، و هم طول F، نمایشگر پیام، را تعیین می‌کند.

۸-۲-۲ گزینه‌های دسته پشت‌بند

در این طرح امضای دیجیتال، دسته پشت‌بند (که به‌عنوان قسمتی از ساخت نمایشگر پیام استفاده می‌شود) ممکن است طولی برابر یک یا دو هشت‌تایی داشته باشد. این پشت‌بند باید شامل t هشت‌تایی(t مساوی با ۱ یا ۲) باشد به‌طوری‌که سمت راست‌ترین نیبل(۴ بیت) همیشه برابر با مبنای شانزده C باشد. دو گزینه زیر مجاز هستند.

- گزینه ۱ ($t = 1$): پشت‌بند باید شامل یک هشت‌تایی باشد؛ این هشت‌تایی باید برابر با مبنای شانزده BC باشد.
- گزینه ۲ ($t = 2$): پشت‌بند باید شامل دو هشت‌تایی متوالی باشد؛ سمت راست‌ترین هشت‌تایی باید برابر با مبنای شانزده CC باشد و سمت چپ‌ترین هشت‌تایی باید شناسه تابع درهم‌ساز باشد. شناسه تابع درهم‌ساز به تابع درهم‌ساز مورد استفاده اشاره می‌کند.

بازه 00 تا 7F به استاندارد ISO/IEC JTC1 اختصاص داده شده است؛ استاندارد ISO/IEC 10118 یک شناسه یکتا در این بازه برای هر تابع درهم‌ساز استاندارد شده تعیین می‌کند. بازه 08 تا FF برای استفاده مالکیتی[1] در نظر گرفته شده است.

یادآوری – برخلاف آنچه در گذشته تلقی می‌شد، استفاده از گزینه ۲، نیاز درستی‌سنج به یک ابزار مستقل و ایمن برای تشخیص تابع درهم‌ساز مورد استفاده در درستی‌سنجی امضاء را از بین نمی‌برد. نادرست بودن این موضوع در [16] نشان داده شده است. (به پیوست ت نیز مراجعه شود.)

۸-۲-۳ ظرفیت

ظرفیت c امضاء برای این طرح به‌صورت زیر داده شده است:

$$c = k - L_h - 8t - 4.$$

همان‌طور که در ۷-۲-۲ تعریف شد، طول پیام قابل بازیابی c^* باید موارد زیر را برآورده کند:

الف- $c^* = |M_1|$ در حالت بازیابی پیام کامل ؛

1- Proprietary use

ب- $c - 7 \leq c^* \leq c$ در حالت بازیابی جزیی.

۸-۳ تولید نمایشگر پیام

در این طرح، تولید نمایشگر پیام شامل دو گام اصلی است:

- درهم‌سازی پیام؛
- قالب‌بندی.

۸-۳-۱ درهم‌سازی پیام

پیام M (به‌طوری‌که $M = \mathrm{M}_1 || \mathrm{M}_2$) باید ورودی تابع درهم‌ساز h باشد تا کد درهم H به‌دست آید؛ به‌عبارت دیگر، $\mathrm{H} = \mathrm{f}(M)$. توجه داشته باشید که H شامل L_h بیت است.

۸-۳-۲ قالب‌بندی

یک رشته k بیتی باید به‌صورت زیر ساخته شود (از چپ به راست عمل می‌کند.):

- دو بیت برابر 01 قرار داده می‌شود.
- در حالت بازیابی کامل، یک بیت برابر با 0 قرار داده می‌شود (یعنی وقتی که $M = M_1$) و در حالت بازیابی جزیی برابر 1 قرار داده می‌شود. (یعنی وقتی که $|M_2| > 0$)
- همه $\mathrm{k} - \mathrm{L}_h - |M_1| - 8\mathrm{t} - 4$ بیت‌های لایه‌گذاری[1] برابر با 0 قرار داده می‌شوند.
- یک بیت برابر با 1 قرار داده می‌شود. (آخرین بیت لایه‌گذاری)
- $|M_1|$ بیت از M_1،
- L_h بیت از H، کد درهم،
- 8t بیت از فیلد پشت‌بند T.

یادآوری ۱- در جایی که از بازیابی جزیی استفاده می‌شود، M_2 تا حد ممکن کوتاه نگه داشته می‌شود زیرا باید شرط عدد صحیحی از هشت‌تایی‌ها بودن را برآورده کند. در این حالت، تعداد بیت‌های لایه‌گذاری برابر صفر کمتر از هشت خواهد بود.

نمایشگر پیام F با پردازش از چپ به راست رشته بالا در دسته‌هایی با چهار بیت متوالی یا نیبل به‌دست می‌آید. این پردازش شامل مراحل زیر است:

۱- سمت چپ‌ترین نیبل باید بدون تغییر باقی بماند.

۲- اگر سمت راست‌ترین بیت سمت چپ‌ترین نیبل برابر 0 باشد آن‌گاه:

الف- همه نیبل‌های بعدی که برابر با 0000 هستند، در صورت وجود، باید با مبنای شانزده B جایگزین شوند. این نیبل‌ها قسمتی از فیلد لایه‌گذاری هستند.

ب- اولین نیبل بعدی که برابر با 0000 نباشد باید با مبنای شانزده B (یعنی 1011) *بای انحصاری* شود. این نیبل، نیبل حاوی آخرین بیت لایه‌گذاری است.

1- Padding bits

۳- تمام بیت‌های بعدی باید بدون تغییر باقی بمانند.

یادآوری ۲- این به معنای آن است که اگر سمت راست‌ترین بیت سمت چپ‌ترین نیبل برابر با ۱ باشد (و بنابراین هیچ بیت لایه‌گذاری ۰ وجود ندشته باشد)، آن‌گاه هیچ تغییری در رشته بیت داده نمی‌شود.

۴- اولین بیت رشته حاصل (که همیشه برابر با 0 خواهد بود) باید حذف شود که منجر به یک F به‌عنوان k-1 بیت خواهد شد.

۴-۸ بازیابی پیام

همان‌طور که در بند ۶ مشخص شد، درستی‌سنج باید قبل از پردازش یک امضاء بداند که کدام تابع درهم‌ساز در حال استفاده است. بنابراین، درستی‌سنج از L_h نیز آگاه خواهد بود.

اگر سمت راست‌ترین هشت‌تایی نمایشگر پیام بازیابی‌شده F^* که یک رشته با k-1 بیت است برابر با :

- مبنای شانزده BC باشد، آن‌گاه پشت‌بند حاوی آن هشت‌تایی است؛
- مبنای شانزده CC باشد، آن‌گاه حاوی سمت راست‌ترین دو هشت‌تایی F^* است در حالی که سمت چپ-ترین هشت‌تایی شناسه تابع درهم‌ساز مورد استفاده است. توصیه می‌شود توسط درستی‌سنج بررسی شود که آیا تابع درهم‌ساز مورد استفاده صحیح است یا خیر. اگر تابع درهم‌ساز متفاوت بود، درستی-سنجی امضاء ناموفق بوده است.

اگر پشت‌بند یا شناسه تابع درهم‌ساز (در صورت وجود) را نتوان تفسیر کرد امضاء Σ نباید مورد پذیرش قرار گیرد. در غیر این‌صورت فرایند درستی‌سنجی باید ادامه یابد.

اگر سمت چپ‌ترین بیت نمایشگر پیام بازیابی‌شده F^* برابر با 0 باشد، امضاء Σ نباید مورد پذیرش قرار گیرد..

یک 0 باید به سمت چپ رشته افزوده شود (که منجر به یک رشته k بیتی می‌شود). این رشته از چپ به راست در دسته‌هایی با چهار بیت متوالی یا نیبل به‌صورت زیر باید پردازش شود.

۱- سمت چپ‌ترین نیبل باید بدون تغییر باقی بماند.

۲- اگر سمت راست‌ترین بیت سمت چپ‌ترین نیبل برابر 0 باشد آن‌گاه:

الف- همه نیبل‌های بعدی که برابر با B هستند، (در صورت وجود) قسمتی از فیلد لایه‌گذاری هستند،

ب- اولین نیبل بعدی که برابر با B نباشد، باید با مبنای شانزده B، *XOR* شود تا مقدار اولیه این نیبل بازیابی شود.

۳- تمام بیت‌های بعدی باید بدون تغییر باقی بمانند.

اکنون می‌توان مکان آخرین (سمت راست‌ترین) بیت لایه‌گذاری را مشخص کرده و بنابراین تعداد مجموع بیت‌های لایه‌گذاری را محاسبه کرد. سومین بیت اولین نیبل را نیز می‌توان پردازش کرد تا مشخص شود امضاء، کدام بازیابی جزیی یا کلی را فراهم می‌کند. در حالت بازیابی جزیی، اگر نه یا بیشتر بیت لایه‌گذاری وجود داشته باشد، امضاء نباید پذیرفته شود. (به‌عبارت دیگر، هشت یا بیشتر از هشت بیت لایه‌گذاری صفر) در غیر این‌صورت فرایند درستی‌سنجی باید ادامه یابد.

تمام بیت‌ها تا پایان فیلد لایه‌گذاری باید از سمت چپ نسخه تغییر یافته F^* حذف شوند و پشت‌بند با طول یک یا دو هشت‌تایی نیز از سمت راست حذف شود. رشته دودویی باقی‌مانده باید به دو قسمت تقسیم شود.

- کد درهم بازیابی‌شده H^* باید حاوی L_h بیت سمت راست باشد.
- قسمت بازیابی‌شده پیام M_1^* باید حاوی بیت‌های باقی‌مانده سمت چپ باشد.

قسمت بازیابی‌شده پیام M_1^* باید به قسمت غیرقابل بازیابی پیام M_2^* الحاق و به فرایند درستی‌سنجی و تابع درهم‌ساز داده شود. اگر نتیجه با H^* یکسان باشد یعنی $H^* = h(M_1^* || M_2^*)$، آن‌گاه امضاء باید پذیرفته شده و M_1^* باید برگردانده شود. در غیر این‌صورت امضاء نباید پذیرفته شود.

۹ طرح امضای دیجیتال ۲

۹-۱ کلیات

بند ۹ تولید نمایشگر پیام و فرایندهای بازیابی پیام را برای یک طرح امضای دیجیتال تصادفی با بازیابی پیام توضیح می‌دهد.

یادآوری – این طرح امضاء با طرح IFSSR مشخص شده در [10] ,IEEE P1363a سازگار است. این طرح تقریباً مبتنی بر طرحی به‌نام [10] ,PSS-R است. روش تولید نمایشگر پیام به همین نحو از شیوه EMSR3 در [10] ,IEEE P1363a گرفته شده است.

۹-۲ پارامترها

۹-۲-۱ طول پیمانه

فرض می‌شود که کلید امضای خصوصی مورد استفاده پیمانه‌ای با طول k بیت دارد. (به پیوست ب مراجعه شود.) این فرض هم c، ظرفیت امضاء، و هم طول F، نمایشگر پیام، را تعیین می‌کند.

۹-۲-۲ طول سالت

یک طول برای سالت L_s باید انتخاب شود. L_s باید یک عدد صحیح مثبت باشد ($L_s > 0$)؛ L_h یک مقدار متداول است.

۹-۲-۳ گزینه‌های فیلد پشت‌بند

در این طرح امضای دیجیتال، فیلد پشت‌بند (که به‌عنوان قسمتی از ساخت نمایشگر پیام استفاده می‌شود) ممکن است طولی برابر یک یا دو هشت‌تایی داشته باشد. پشت‌بند باید شامل t هشت‌تایی(t مساوی با ۱ یا ۲) باشد به‌طوری‌که سمت راست‌ترین نیبل همیشه برابر با مبنای شانزده C باشد. دو گزینه زیر مجاز هستند:

- گزینه ۱ ($t = 1$): پشت‌بند باید حاوی یک هشت‌تایی باشد؛ این هشت‌تایی باید برابر با مبنای شانزده BC باشد.

- گزینه ۲ ($t = 2$): پشت‌بند باید حاوی دو هشت‌تایی متوالی باشد؛ هشت‌تایی سمت راست باید برابر با مبنای شانزده CC باشد و هشت‌تایی سمت چپ باید برابر شناسه تابع درهم‌ساز باشد. شناسه تابع درهم‌ساز به تابع درهم‌ساز مورد استفاده اشاره می‌کند.
- بازه 00 تا 7F به استاندارد ISO/IEC JTC1 اختصاص داده شده است؛ استاندارد ISO/IEC 10118 یک شناسه یکتا را در این بازه برای هر تابع درهم‌ساز استاندارد شده، تعیین می‌کند. بازه 80 تا FF برای استفاده مالکیتی در نظر گرفته شده است.

۹-۲-۴ ظرفیت

ظرفیت c امضاء برای این طرح به‌صورت زیر داده شده است:

$$c = k - L_h - L_s - 8t - 2.$$

۹-۳ تولید نمایشگر پیام

در این طرح، تولید نمایشگر پیام شامل دو گام اصلی است:

- درهم‌سازی پیام؛
- قالب‌بندی.

۹-۳-۱ درهم‌سازی پیام

کد درهم H باید با استفاده از مراحل زیر یا توالی معادل آن محاسبه شود:

طول بیت M_1 یعنی $|M_1|$ را با استفاده از آنچه در بند ۵ بیان شد به یک رشته بیت C با طول ۶۴ بیت تبدیل کنید.

رشته بیت تصادفی جدید S را تولید کنید. رشته بیت S دارای طول L_s بیت باشد.

کد درهم H را به‌صورت $H = h(C||M_1||h(M_2)||S)$ محاسبه کنید. توجه داشته باشید که H دارای L_h بیت است.

۹-۳-۲ قالب‌بندی

نمایشگر پیام F باید طبق مراحل زیر یا توالی معادل آن مراحل محاسبه شود:

۱- P را برابر با رشته بیتی قرار دهید که حاوی $k + \delta - L_h - L_s - |M_1| - 8t - 2$ بیت 0 است که در آن $\delta = (k - 1)\ mod\ 8$ است.

۲- D را برابر با رشته بیتی قرار دهید که به‌صورت $D = ||1||M_1||S$ تعریف می‌شود که در آن ۱ یک تک بیت است. طول D برابر $k + \delta - L_h - 8t - 1$ بیت است.

یادآوری – اگر طول کد درهم عدد صحیحی از هشت‌تایی‌ها باشد، آن‌گاه طول رشته بیت D نیز عدد صحیحی از هشت‌تایی‌ها خواهد بود.

۳- تابع تولید ماسک g را به کد درهم H اعمال کنید تا رشته بیت N با طول $k+\delta-L_h-8t-1$ بیت تولید شود.

۴- طول $D\oplus N$ برابر $k+\delta-L_h-8t-1$ است. D' را برابر رشته‌ای با طول $k-L_h-8t-1$ بیت قرار دهید که از حذف δ بیت از سمت چپ $D\oplus N$ به‌دست می‌آید.

۵- F را برابر $D'||H||T$ قرار دهید که در آن T فیلد پشت‌بند با 8t بیت است. F رشته‌ای با k-1 بیت است.

۴-۹ بازیابی پیام

اگر سمت راست‌ترین هشت‌تایی نمایشگر پیام بازیابی شده F^* که یک رشته با k-1 بیت است برابر با:

- مبنای شانزده BC باشد، آن‌گاه پشت‌بند حاوی آن هشت‌تایی است؛
- مبنای شانزده CC باشد، آن‌گاه پشت‌بند حاوی سمت راست‌ترین دو هشت‌تایی F^* است که در آن سمت چپ‌ترین هشت‌تایی برابر شناسه تابع درهم‌ساز مورد استفاده است. درستی‌سنج باید بررسی کند که آیا تابع درهم‌ساز مورد استفاده صحیح است یا خیر. اگر تابع درهم‌ساز متفاوت بود، درستی‌سنجی امضاء ناموفق بوده است.

اگر پشت‌بند یا شناسه تابع درهم‌ساز را (در صوت وجود) نتوان تفسیر کرد، امضاء Σ نباید پذیرفته شود. در غیر این‌صورت، فرآیند درستی‌سنجی باید ادامه یابد.

سپس قسمت قابل بازیابی پیام M_1 باید در مراحل زیر یا توالی معادل آن با استفاده از نمایشگر پیام بازیابی شده F^* و قسمت غیرقابل بازیابی M_2 بازیابی شود.

۱- δ بیت 0 به انتهای سمت چپ F^* اضافه کنید.

۲- D'^* را برابر با سمت چپ‌ترین $k+\delta-L_h-8t-1$ بیت رشته حاصل و H^* را برابر L_h بیت بعدی قرار دهید.

۳- تابع تولید ماسک g را به رشته H^* اعمال کنید تا رشته بیت N با طول $k+\delta-L_h-8t-1$ بیت تولید شود.

۴- D^* را برابر با $D^*=D'^*\oplus N^*$ قرار دهید.

۵- سمت چپ‌ترین δ بیت D^* را برابر با 0 قرار دهید.

۶- با شروع از سمت چپ D^*، اولین بیت ۱ را جست و جو کنید. این بیت و تمامی صفرهای سمت چپ آن را حذف کنید. سپس S را برابر با سمت راست‌ترین L_s بیت D^* و M_1^* را برابر با بقیه بیت‌های D^* قرار دهید. اگر اولین بیت ۱ وجود نداشت، نشانه‌ای مبنی بر ناموفق بودن درستی‌سنجی بازگردانید و عملیات را متوقف کنید.

۷- طول بیت M_1^* را با استفاده از آنچه در بند ۵ بیان شد به یک رشته بیت C با طول ۶۴ بیت تبدیل کنید.

۸- اگر $H^*=h(C||M_1^*||h(M_2^*)||S^*)$ باشد، قسمت پیام بازیابی شده M_1^* را خروجی دهید. در غیر این‌صورت، نشانه‌ای به‌عنوان عدم موفقیت درستی‌سنجی بازگردانید.

۱۰ طرح امضای دیجیتال ۳

بند ۱۰ تولید نمایشگر پیام و فرآیندهای بازیابی پیام را برای یک طرح امضای دیجیتال قطعی با بازیابی پیام توضیح می‌دهد.

این طرح با طرح تعریف‌شده در بند ۹ یکسان است به‌جز این‌که S یک مقدار ثابت است که می‌تواند طول صفر داشته باشد؛ به‌عبارتی، $L_s \geq 0$ (برخلاف شرط $L_s > 0$ که در بند ۹ اعمال می‌شود). بنابراین این طرح قطعی و غیرتصادفی است.

طول ثابت S می‌تواند توسط امضاءکننده انتخاب شود. از سوی دیگر، این امکان وجود دارد که به‌عنوان قسمتی از دامنه پارامترها تعیین شود.

یادآوری ۱– سطح امنیت این طرح مانند سطحی است که از به‌کار بردن « درهم‌سازی تمام دامنه» به‌دست می‌آید [1] و [4] .

یادآوری ۲– طرح امضای دیجیتال ۳ برتر از طرح امضای دیجیتال ۱ به حساب می‌آید – (به بند ۱ مراجعه شود.) این برتری به دلایل زیر است:

- طرح‌هایی که با طرح امضای دیجیتال ۳ شباهت زیادی دارند دارای اثبات ریاضی برای امنیت هستند (به [4] مراجعه شود)، اما این فنون اثبات ریاضی، در مورد طرح امضای دیجیتال ۱ صادق نیست.
- هر دو طرح دارای بازده قابل مقایسه‌ای هستند.

پیوست الف

(الزامی)

پیمانه ASN.1

الف-۱ کلیات

```
MessageRecoverySignatureMechanisms {
  iso(1) standard(0) signature-schemes(9796) part2(2) asn1-module(1)
    message-recovery-signature-mechanisms(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

  HashFunctions
    FROM DedicatedHashFunctions {
      iso(1) standard(0) hash-functions(10118) part(3)
        asn1-module(1) dedicated-hash-functions(0) } ;

SignatureWithMessageRecovery ::= SEQUENCE {
  algorithm  ALGORITHM.&id({MessageRecovery}),
  parameters ALGORITHM.&Type({MessageRecovery}{@algorithm}) OPTIONAL
}

MessageRecovery ALGORITHM ::= {
  dswmr-mechanism1A     |
  dswmr-mechanism2A     |
  dswmr-mechanism3A     |
  dswmr-mechanism1N     |
  dswmr-mechanism2N     |
  dswmr-mechanism3N     |
  dswmr-mechanism1A-sha1 |
  dswmr-mechanism2A-sha1 |
  dswmr-mechanism3A-sha1 |
  dswmr-mechanism1N-sha1 |
  dswmr-mechanism2N-sha1 |
  dswmr-mechanism3N-sha1,

  ...  -- Expect additional signature scheme objects --
}

dswmr-mechanism1A ALGORITHM ::= {
  OID mechanism1A PARMS HashFunctions
}

dswmr-mechanism2A ALGORITHM ::= {
```

```
  OID mechanism2A PARMS HashFunctions
}

dswmr-mechanism3A ALGORITHM ::= {
  OID mechanism3A PARMS HashFunctions
}

dswmr-mechanism1N ALGORITHM ::= {
  OID mechanism1N PARMS HashFunctions
}

dswmr-mechanism2N ALGORITHM ::= {
  OID mechanism2N PARMS HashFunctions
}

dswmr-mechanism3N ALGORITHM ::= {
  OID mechanism3N PARMS HashFunctions
}

dswmr-mechanism1A-sha1 ALGORITHM ::= { OID  mechanism1A-sha1 }

dswmr-mechanism2A-sha1 ALGORITHM ::= { OID  mechanism2A-sha1 }

dswmr-mechanism3A-sha1 ALGORITHM ::= { OID  mechanism3A-sha1 }

dswmr-mechanism1N-sha1 ALGORITHM ::= { OID  mechanism1N-sha1 }

dswmr-mechanism2N-sha1 ALGORITHM ::= { OID  mechanism2N-sha1 }

dswmr-mechanism3N-sha1 ALGORITHM ::= { OID  mechanism3N-sha1 }

-- Cryptographic algorithm identification --

ALGORITHM ::= CLASS {
  &id    OBJECT IDENTIFIER  UNIQUE,
  &Type  OPTIONAL
}
 WITH SYNTAX { OID &id [PARMS &Type] }

-- Message recovery signature mechanisms --

OID ::= OBJECT IDENTIFIER  -- Alias

signatureMechanismA OID ::= {
  iso(1) standard(0) signature-schemes(9796) part2(2) mechanism(0)
alternate(0) }
```

```
mechanism1A OID ::= { signatureMechanismA mechanism1(0) }

mechanism2A OID ::= { signatureMechanismA mechanism2(1) }

mechanism3A OID ::= { signatureMechanismA mechanism3(2) }

signatureMechanismN OID ::= {
  iso(1) standard(0) signature-schemes(9796) part2(2) mechanism(0) normal(1) }

mechanism1N OID ::= { signatureMechanismN mechanism1(0) }

mechanism2N OID ::= { signatureMechanismN mechanism2(1) }

mechanism3N OID ::= { signatureMechanismN mechanism3(2) }

-- Combined signature scheme and hash-function mechanisms –-

mechanismA-Hash OID ::= {
  iso(1) standard(0) signature-schemes(9796) part2(2)
    mechanismHash(2) alternate(0) }

mechanism1A-sha1 OID ::= { mechanismA-Hash mechanism1-SHA1(0) }
mechanism2A-sha1 OID ::= { mechanismA-Hash mechanism2-SHA1(1) }

mechanism3A-sha1 OID ::= { mechanismA-Hash mechanism3-SHA1(2) }

mechanismN-Hash OID ::= {
  iso(1) standard(0) signature-schemes(9796) part2(2)
    mechanismHash(2) normal(1) }

mechanism1N-sha1 OID ::= { mechanismN-Hash mechanism1-SHA1(0) }

mechanism2N-sha1 OID ::= { mechanismN-Hash mechanism2-SHA1(1) }

mechanism3N-sha1 OID ::= { mechanismN-Hash mechanism3-SHA1(2) }

END  -- MessageRecoverySignatureMechanisms –
```

الف-۲ استفاده از شناسه‌های شیء[1] متوالی

هر طرح امضاء از یک تابع درهم‌ساز و یک توالی حاوی یک شناسه الگوریتم درهم‌ساز و پارامترهای مربوطه آن استفاده می‌کند. بنابراین، این امکان وجود دارد که یکی از شناسه‌های اختصاصی الگوریتم تابع درهم‌ساز مشخص‌شده در استاندارد ISO/IEC 10118-3 و پارامترهای مربوطه آن به دنبال شناسه شی طرح امضاء بیایند.

با استفاده از نمادگذاری مقدار[2] ASN.1 XML، یک مقدار از نوع SignatureWithMessageRecovery که از سازوکار پردازش امضای معمولی ۱ تعریف شده در این استاندارد و تابع درهم‌ساز SHA-1 تعریف‌شده در استاندارد ISO/IEC 10118-3 استفاده می‌کند، به‌صورت زیر ارائه خواهد شد:

```
<SignatureWithMessageRecovery>
  <algorithm> 1.0.9796.2.0.1.0 </algorithm>
  <parameters>
    <HashFunctions>
      <algorithm> 1.3.14.3.2.26 </algorithm>
      <parameters/>
    </HashFunctions>
  </parameters>
</SignatureWithMessageRecovery>
```

یک مقدار از نوع SignatureWithMessageRecovery که از شناسه شی ترکیبی برای سازوکار پردازش امضای معمولی ۱ و تابع درهم‌ساز SHA-1 تعریف‌شده در استاندارد ISO/IEC 10118-3 استفاده می‌کند، دارای شکل ساده‌تر زیر است:

```
<SignatureWithMessageRecovery>
  <algorithm> 1.0.9796.2.2.1.0 </algorithm>
</SignatureWithMessageRecovery>
```

1- Object identifiers
2- Value notation

پیوست ب

(الزامی)

سامانه کلید عمومی برای امضای دیجیتال

در این پیوست، یک سامانه کلید عمومی تعریف می‌شود. این سامانه کلید عمومی دارای سه قسمت اصلی است:

- *تولید کلید*: روشی برای تولید یک جفت کلید که شامل یک کلید امضای خصوصی و یک کلید درستی‌سنجی خصوصی است؛
- *تولید امضاء*: روشی برای تولید یک امضاء Σ از یک نمایشگر پیام F و یک کلید امضای خصوصی؛ و
- *گشایش امضاء*: روشی برای به‌دست آوردن نمایشگر پیام بازیابی‌شده F^* از امضاء Σ و کلید درستی‌سنجی عمومی. خروجی این تابع همچنین حاوی نشانه‌ای است که موفقیت یا عدم موفقیت فرآیند گشایش امضاء را مشخص می‌کند.

ب-۱ اصطلاحات و تعاریف

در این پیوست، اصطلاحات و تعاریف زیر به‌کار می‌روند:

ب-۱-۱

پیمانه

عدد صحیحی برابر با حاصل‌ضرب دو عدد اول است که قسمتی از کلیدهای عمومی و خصوصی را تشکیل می‌دهد.

ب-۱-۲

کلید امضای خصوصی

توان امضای خصوصی و پیمانه

ب-۱-۳

کلید درستی‌سنجی عمومی

توان درستی‌سنجی عمومی و پیمانه

ب-۲ نمادها و اصطلاحات کوتاه‌نوشت‌ها

در این پیوست، علاوه بر نمادهای تعریف‌شده در بند ۴، نمادها و کوته‌نوشت‌های زیر نیز به‌کار می‌روند.

F	عدد صحیحی که F نمایش دودویی آن است
f^*	یک عدد صحیح که به هنگام گشایش امضاء محاسبه می‌شود
J	یک عدد صحیح که به هنگام تولید امضاء محاسبه می‌شود
J^*	یک عدد صحیح که به هنگام گشایش امضاء محاسبه می‌شود
n	پیمانه (قسمتی از کلید درستی‌سنجی عمومی و کلید امضای خصوصی)
p, q	عامل‌های ضرب اول پیمانه
S	توان امضاء
V	توان درستی‌سنجی
l	کوچک‌ترین مضرب مشترک اعداد صحیح a و b
n	کمینه دو مقدار a و b
	نماد ژاکوبی[1] a نسبت به n

یادآوری ۱- p را برابر یک عدد اول فرد و a را برابر یک عدد صحیح مثبت قرار دهید. فرمول زیر نماد لژاندر[2] a نسبت به p را تعریف می‌کند.

$$(a|p) = a^{(p-1)/2} \bmod p$$

نماد لژاندر مضارب p نسبت به p برابر 0 است. زمانی که a مضرب p نباشد، نماد لژاندر a نسبت به p بسته به این‌که a مربع به پیمانه p باشد یا نباشد برابر ۱+ یا ۱- است.

یادآوری ۲- n را برابر یک عدد صحیح مثبت فرد و a را برابر یک عدد صحیح مثبت قرار دهید. نماد ژاکوبی a نسبت به n برابر با حاصل‌ضرب نمادهای لژاندر a نسبت به عوامل ضرب اول n است (که نمادهای لژاندر را برای عوامل ضرب اول تکراری تکرار

1 - Jaxobi
2 - Legendre

می‌کند). بنابراین اگر $n = p\ q$، آن‌گاه $(a|n) = (a|p)(a|q)$. نماد ژاکوبی a نسبت به n را می‌توان بدون دانستن عوامل ضرب اول n محاسبه کرد.

ب-۳ تولید کلید

یادآوری – در این سند هیچ روشی برای اعتبارسنجی کلید عمومی مشخص نشده است؛ به‌عبارت دیگر، هیچ تضمینی به طرف‌ها (یعنی طرف تولیدکننده جفت کلید، طرف استفاده‌کننده از کلید عمومی یا یک طرف سوم خنثی) داده نمی‌شود که یک کلید عمومی مشخص، مطابق با تعریف ریاضی کلید عمومی باشد. کلیدهای نامعتبر می‌توانند به‌علت یک خطای سهوی در محاسبه تولید کلید یا اقدام عمدی مهاجم ظاهر شوند. بهتر است فرض شود که استفاده از یک کلید نامعتبر تمام تضمین‌های امنیتی را باطل می‌کند. این تضمین‌ها شامل عدم توانایی مهاجم در جعل امضاء یا کشف کلید خصوصی مربوطه است. کاربرانی که خواهان اطمینان از اعتبار ریاضی کلید عمومی قبل از به‌کار بردن آن هستند، بهتر است از روش‌های دیگری مانند روش‌هایی که در استاندارد ISO/IEC 9796-3 وجود دارد، استفاده کنند. به‌عنوان یک اصل کلی در هر سامانه رمز، استفاده از یک کلید که به‌صورت نادرست تولید شده ولی یک کلید عمومی معتبر است (برای مثال، کلیدی که از یک منبع که به اندازه کافی تصادفی نیست تولید شده است.) یا یک کلید خصوصی که به‌صورت نادرست محافظت می‌شود، ممکن است تمام تضمین‌های امنیتی را باطل کند. اعتبارسنجی پیاده‌سازی می‌تواند این خطرات و احتمال استفاده از کلیدهای نامعتبر را کاهش دهد. به هرحال، استفاده از اعتبارسنجی تضمین خاصی را فراهم نمی‌کند که یک کلید عمومی مشخص در واقع معتبر است یا خیر.

ب-۳-۱ توان درستی‌سنجی عمومی

هر هستار امضاءکننده باید یک عدد صحیح مثبت v را به‌عنوان توان درستی‌سنجی عمومی خود انتخاب کند. توان درستی‌سنجی ممکن است در بعضی از کاربردهای خاص استانداردسازی شود.

یادآوری – مقادیر ۲، ۳، ۱۷ و ۶۵۵۳۷ ممکن است که در عمل مفید باشند.

ب-۳-۲ عوامل ضرب اول مخفی و پیمانه عمومی

هر هستار امضاءکننده باید به‌صورت مخفی و تصادفی دو عدد اول بزرگ متمایز p و q را با شرایط زیر انتخاب کند:

- اگر v فرد باشد، آن‌گاه v باید مقسوم علیه مشترک[1] p-1 و q-1 باشد.
- اگر v زوج باشد، آن‌گاه v باید مقسوم علیه مشترک (p-1)/2 و (q-1)/2 باشد. به‌علاوه، p و q نباید به 8 هم‌پیمانه باشند.

پیمانه عمومی n برابر با حاصل‌ضرب p و q قرار داده می‌شود؛ یعنی $n = p\ q$. اندازه پیمانه n مقدار k به بیت را به‌صورت زیر تعیین می‌کند

$$2^{k-1} < n \leq 2^k - 1$$

یادآوری ۱– برای جلوگیری از تجزیه عامل‌های پیمانه، می‌توان شروط اضافی دیگری را در انتخاب اعداد اول در نظر گرفت.

1- Coprime

یادآوری ۲- بعضی از شکل‌های پیمانه، کاهش پیمانه‌ای را ساده می‌کند و به جدول ذخیره‌سازی کمتری نیاز دارد. مثال‌هایی از این شکل‌ها عبارتند از:

$n = 2^{64x} - r$ با طول: $k = 64x$ بیت،

$n = 2^{64x} + r$ با طول: $k = 64x + 1$ بیت،

که در آن: $2x \leq y \leq 1$ و $r < 2^{64x-8y} < 2r$.

برای پیمانه‌هایی به شکل $2^{64x} - r$ با ارزش‌ترین $8y$ بیت برابر 1 هستند که در آن $8y$ حداکثر یک چهارم طول پیمانه است. برای پیمانه‌هایی به شکل $2^{64x} + r$ با ارزش‌ترین بیت برابر 1 است و $8y$ بیت 0 به دنبال آن می‌آید که در آن $8y$ حداکثر یک چهارم طول پیمانه است.

ب-۳-۳ توان امضای خصوصی

توان امضای خصوصی باید هر عدد صحیح مثبت s باشد به‌طوری‌که $sv - 1$ مضربی باشد از:

- $lcm(p-1, q-1)$ اگر v فرد باشد؛
- $lcm(p-1, q-1)/2$ اگر v زوج باشد.

یادآوری - به‌طور کلی s کوچک‌ترین مقدار ممکن است.

ب-۴ تابع تولید امضاء

نمایشگر پیام F رشته‌ای با طول $k - 1$ بیت است که سمت راست‌ترین چهار بیت آن برابر 1100 (مبنای شانزده C) است. این رشته نمایش دودویی یک عدد صحیح مثبت است که با f مشخص می‌شود.

در این صورت J به شکل زیر تعریف می‌شود:

- اگر v فرد باشد، آن‌گاه $J = f$،
- اگر v زوج و $(f|n) = +1$، آن‌گاه $J = f$ و
- اگر v زوج و $(f|n) = -1$، آن‌گاه $J = f/2$.

یادآوری - اگر v زوج باشد، آن‌گاه عملیات بالا تضمین می‌کند که نماد ژاکوبی J نسبت به n همیشه ۱+ است.

امضاء Σ یک رشته بیت با طول k-1 بیت است که با استفاده از آنچه در بند ۵ بیان شد با عدد صحیح $\min\{J^s \bmod n, n - (J^s \bmod n)\}$ متناظر است.

ب-۵ تابع گشایش امضاء

امضاء Σ رشته‌ای با طول $k - 1$ بیت است؛ این رشته نمایش دودویی یک عدد صحیح مثبت کمتر از n است. این عدد صحیح باید به توان v رسیده و به پیمانه n نوشته شود تا J^* به‌دست آید؛ به‌عبارت دیگر:

$$J^* = \sum^v \bmod n$$

آن‌گاه عدد صحیح f^* باید به‌صورت زیر محاسبه شود:

- اگر v فرد باشد و
- اگر $J^* \bmod 16 = 12$، آن‌گاه $f^* = J^*$،

- اگر $J^* \bmod 16 = n - 12 \bmod 16$، آن‌گاه $f^* = n - J^*$.
- اگر v زوج باشد و
- اگر $J^* \bmod 8 = 1$، آن‌گاه $f^* = n - J^*$.
- اگر $J^* \bmod 8 = 4$، آن‌گاه $f^* = J^*$،
- اگر $J^* \bmod 8 = 6$، آن‌گاه $f^* = 2J^*$،
- اگر $J^* \bmod 8 = 7$، آن‌گاه $f^* = 2(n - J^*)$،

امضاء Σ در همه موارد دیگر باید رد شود؛ همچنین اگر $f^* \bmod 16 \neq 12$ و اگر $f^* \leq 2^{k-1} - 1$ را برآورده نکند، امضاء نباید پذیرفته شود.

نمایشگر پیام بازیابی شده F^* یک رشته با k-1 بیت است که با استفاده از آنچه در بند ۵ بیان شد با عدد صحیح f^* متناظر است.

ب-۶ تابع تولید امضای جایگزین

وقتی که v فرد باشد، این تابع را می‌توان به‌عنوان جایگزین تابع بند ب-۴ استفاده کرد. این تابع باید به همراه تابع گشایش امضاء بند ب-۷ استفاده شود.

نمایشگر پیام F رشته‌ای با طول $k - 1$ بیت است که سمت راست‌ترین چهار بیت آن برابر 1100 (مبنای شانزده C) است. این رشته نمایش دودویی یک عدد صحیح مثبت است که با f مشخص می‌شود.

در این حالت عدد صحیح J به‌صورت $J = f$ تعریف می‌شود.

امضاء Σ یک رشته با k-1 بیت است که با استفاده از آنچه در بند ۵ بیان شد با عدد صحیح $J^s \bmod n$ متناظر است.

یادآوری – این تفاوت بین این تابع و تابع بیان‌شده در بند ب-۴ وجود دارد که امضاء Σ همیشه برابر $J^s \bmod n$ است و برای انتخاب کمینه $\{J^s \bmod n, n - (J^s \bmod n)\}$ هیچ گام «قدر مطلق»ی انجام نمی‌شود.

ب-۷ تابع گشایش امضای جایگزین

وقتی که v فرد باشد، این تابع را می‌توان به‌عنوان جایگزین تابع بند ب-۵ استفاده کرد. این تابع باید به همراه تابع تولید امضاء بند ب-۶ استفاده شود.

امضاء Σ رشته‌ای با طول $k - 1$ بیت است؛ این رشته نمایش دودویی یک عدد صحیح مثبت کمتر از n است. این عدد صحیح باید به توان v رسیده و به پیمانه n نوشته شود تا J^* به‌دست آید؛ به‌عبارت دیگر:

آن‌گاه عدد صحیح f^* به‌صورت $f^* = J^*$ محاسبه خواهد شد.

امضاء Σ نباید پذیرفته شود اگر $f^* \bmod 16 \neq 12$ و اگر $J^* \leq 2^{k-1} - 1$ برقرار نشوند.

نمایشگر پیام بازیابی شده F^* یک رشته با k-1 بیت است که با استفاده از آنچه در بند ۵ بیان شد با عدد صحیح f^* متناظر است.

یادآوری – تفاوتی بین این تابع و تابع بیان‌شده در بند ب-۵ وجود دارد که عدد صحیح f^* همیشه با J^* برابر است و نیازی به «شفاف‌سازی» بین J^* و $n - J^*$ وجود ندارد.

پیوست پ
(الزامی)
تابع تولید ماسک

در این پیوست، به تعریف یک تابع ماسک مبتنی بر تابع درهم‌ساز می‌پردازیم.

یادآوری – این تابع به گسترش تابع تعریف‌شده با عنوان MGF1 در IEEE Std 1363-2000 [9] پرداخته و این امکان را برای ورودی و خروجی فراهم می‌کند که به‌صورت رشته‌های بیتی باشند. این مورد مانند پیشنهادات داده شده توسط بلار[1] و راگاوی[2] در [2] و [3] است.

یک تابع تولید ماسک رشته بیتی Z و طول مطلوب خروجی را به‌عنوان ورودی گرفته و رشته بیتی N با همان طول را به‌عنوان خروجی می‌دهد.

پ-۱ نمادها و کوته‌نوشت‌ها

در این پیوست، افزون بر نمادهای تعریف شده در بند ۴، نمادها و کوته‌نوشت‌های زیر نیز به‌کار می‌روند:

L_N	طول (به بیت) خروجی تابع تولید ماسک g
L_Z	طول (به بیت) رشته هشت‌تایی Z
N	خروجی تابع تولید ماسک g (یک رشته بیتی)
Z	یک ورودی رشته‌ای بیتی به تابع تولید ماسک g

پ-۲ الزامات

استفاده از این تابع نیازمند انتخاب یک تابع درهم‌ساز است. این تابع درهم‌ساز که در این‌جا از h برای نمایش آن استفاده می‌کنیم، باید برابر با h تابع درهم‌ساز پاراگراف (ث) بند ۶ انتخاب شود. طول خروجی تابع h به واحد بیت را با L_n نمایش می‌دهیم.

پ-۳ مشخصات

پ-۳-۱ پارامترها

یک ورودی برای تابع g، یک خروجی با طول مورد نظر به واحد بیت که با عدد صحیح L_N نشان داده می‌شود را می‌دهد.

پ-۳-۲ تولید ماسک

رشته بیتی N باید با طی مراحل زیر یا توالی معادل آن محاسبه شود.

1- Bellare
2- Rogaway

۱- اگر L_Z از محدودیت طول ($۲^{۶۴}$-۳۳) برای توابع درهم‌ساز تخصیص داده شده ۱ و ۳ با توجه به استاندارد ISO/IEC 10118-3 فراتر رفته یا $L_N > L_h \times 2^{32}$ شود، خروجی «error» ظاهر شده و توقف روی می‌دهد.

۲- N را یک رشته خالی قرار دهید.

۳- i=0 قرار دهید.

۳-۱- i را با استفاده از معادله بیان شده در بند ۵ به رشته بیتی C به طول ۳۲ بیت تبدیل کنید.

۳-۲- N :=N || h(Z || C) قرار دهید.

۳-۳- $i := i + 1$ قرار دهید.

۳-۴- اگر $i < \lceil L_N/L_h \rceil$ به گام ۳-۱ بروید.

۴- سمت چپ‌ترین L_N بیت N را به خروجی بدهید.

پیوست ت

(اطلاعاتی)

درباره شناساه‌های تابع درهم‌ساز و انتخاب طول قابل بازیابی پیام

همان‌طورکه پیشتر در بند ۶ (الزامات) نیز به آن اشاره شد، کاربران طرح‌های امضاء که در این استاندارد تعیین شده‌اند، باید یک تابع درهم‌ساز مقاوم در برابر برخورد h را انتخاب کنند. برای انجام ایمن فرآیند درستی‌سنجی، لازم است تا درستی‌سنج روشی روشن برای تعیین تابع درهم‌سازی که برای تولید امضاء استفاده شده است، داشته باشد. اگر یک طرف ثالث خراب‌کار بتواند درستی‌سنج را قانع کند که از یک تابع درهم‌ساز ضعیف[1] برای تولید امضاء استفاده شده‌است (به‌عنوان مثال یک تابع درهم‌ساز فاقد ویژگی یکطرفه[2])، آنگاه این طرف ثالث می‌تواند درستی‌سنج را قانع کند که یک امضای معتبر برای یک پیام غلط[3] به‌کار رفته است.

سه طرح امضای دیجیتال تعیین‌شده در این استاندارد به یک شناسه تابع درهم‌ساز اجازه می‌دهد تا در تماینده پیام F جای گیرد. (به زیربند ۸-۲-۲ مراجعه شود.) اگر شناسه تابع درهم‌ساز درون F در نظر گرفته شود، مهاجم نمی‌تواند به‌طور متقلبانه مجدداً از امضای موجود با M_1 یکسان و M_2 متفاوت استفاده کند، حتی اگر درستی‌سنج قانع شود که امضاهای تولیدشده توسط تابعی آن‌چنان ضعیف را بپذیرد که پیش تصاویر[4] آن‌را می‌توان یافت. گمان می‌رود که این ایده مشکل مطرح‌شده در بند پیشین را حل کند.

به هر روی، همان‌طورکه پیشتر در [16] به‌تفصیل بحث شده است، حتی اگر شناسه تابع درهم‌ساز نیز درون نمایشگر پیام گنجانده شود، اگر درستی‌سنج بتواند قانع شود که یک تابع درهم‌ساز *ضعیف* به‌کار رفته، همچنان حملات دیگر امکان‌پذیر هستند. منظور از ضعیف در این‌جا تابع درهم‌ساز فاقد ویژگی یک‌طرفه است؛ یعنی با معلوم بودن کد درهم، یافتن رشته ورودی که توسط تابع درهم‌ساز به این کد درهم نگاشت‌شده به‌طور محاسباتی امکان‌پذیر است. (به یاد داشته باشید که این دقیقاً همان نوع ضعفی است که در ابتدا ما را به گنجاندن شناسه تابع درهم‌ساز درون نمایشگر پیام تحریک کرد.)

حملات توصیف‌شده در [16] به روشی که در ادامه می‌آید، عمل می‌کنند. مهاجم، « امضاهایی»را به‌صورت تصادفی تولید می‌کند و برای هرکدام از این امضاها تابع درستی‌سنجی عمومی مربوط به هستاری را که به‌دنبال جعل امضایش است، اعمال می‌کند و *نماینده*[5] پیام بازیابی‌شده را به‌دست می‌آورد (این گام *گشایش امضاء* است). گام بعدی حمله متناسب با قالب نمایشگر پیام تغییر می‌کند؛ اما اساساً در این گام مهاجم قالب نمایشگر پیام بازیابی شده را برای صحیح بودن و بنابراین مطابقت با یک امضای اصل[6] بررسی می‌کند. بررسی این‌که آیا

1- Weak
2- One-way property
3- False
4- Pre-image
5- Representative
6- Genuine signature

شناسه تابع درهم‌ساز در این رشته همان شناسه مطابق با تابع درهم‌ساز ضعیف است نیز در این گام صورت می-گیرد. احتمال وقوع این رویداد می‌تواند به بزرگی 2^{-16} باشد. (بنابراین مهاجم نیازی به آزمودن *امضاهای تصادفی* بسیار زیاد برای یافتن امضایی با ویژگی‌های مطلوب ندارد.)

با معلوم بودن یک *امضاء*، مهاجم اکنون کد درهم جای گرفته درون نمایشگر پیام بازیابی‌شده را برمی‌دارد و با توجه به ضعیف بودن تابع درهم‌ساز، قسمت غیرقابل بازیابی پیام را درمی‌یابد. این قسمت در ترکیب با قسمت قابل بازیابی جای گرفته درون تماینده پیام به کد درهم مطلوب منجر می‌شود. به‌عبارت دیگر، مهاجم می‌تواند یک امضای جدید را با یک M_1 تصادفی جعل کند. بنابراین گنجاندن شناسه تابع درهم‌ساز در یک نماینده پیام، منجر به اجتناب از نیاز به درستی‌سنج، به‌عنوان یک وسیله مستقل ایمن برای شناخت تابع درهم‌ساز مورد نیاز برای درستی‌سنجی، امضاء نیست.

این بحث همچنین به انتخاب طول قابل بازیابی c^* برای طرح‌های ۲ و ۳ امضاء نیز مربوط می‌گردد. همانطور که پیشتر در زیربند ۷-۲-۲ بحث شد، c^* باید به‌گونه‌ای انتخاب شود که $c^* \leq c$. c ظرفیت طرح امضاء است. مطلوب است که مقدار c به c^* نزدیک باشد تا طول قسمت قابل بازیابی پیام بیشینه و طول قسمت غیر قابل بازیابی آن کمینه شود. پیشنهاد می‌شود که c^* اندکی کمتر از c انتخاب شود (به‌عنوان مثال، c-16 ، c-24 یا c-80، مطابق با سطح دشواری مطلوب) تا حملات توصیف‌شده از نوع ذکر شده در بالا نیز دشوارتر شوند.

پیوست ث
(اطلاعاتی)
مثال‌ها

این پیوست شامل مجموعاً ۱۲ مثال از تولید امضاء و درستی‌سنجی آن برای سه طرح تعریف‌شده در این استاندارد به همراه دو مثال از تولید کلید است.

بند ث-۱ شامل مثال‌هایی با توان عمومی برابر با ۳ است.

- ث-۱-۱ شامل مثالی از تولید کلید است.
- ث-۱-۲ شامل سه مثال از تولید امضاء و درستی‌سنجی آن است به‌گونه‌ای که همه‌ی آن‌ها شامل بازیابی کلی پیام می‌شوند. برای هر کدام از طرح‌های تعریف‌شده در این استاندارد نیز مثالی وجود دارد.
- ث-۱-۳ شامل سه مثال از تولید و درستی‌سنجی امضاء است به‌گونه‌ای که همه آن‌ها شامل بازیابی جزیی پیام هستند. برای هر کدام از طرح‌های تعریف‌شده در این استاندارد نیز مثالی وجود دارد.

بند ث-۲ شامل مثال‌هایی با توان عمومی برابر با ۲ است.

- ث-۲-۱ شامل مثالی از تولید کلید است.
- ث-۲-۲ شامل سه مثال از تولید امضاء و درستی‌سنجی آن است به‌گونه‌ای که همه‌ی آن‌ها شامل بازیابی کامل پیام می‌شوند. برای هر کدام از طرح‌های تعریف‌شده در این استاندارد نیز مثالی وجود دارد.
- ث-۲-۳ شامل سه مثال از تولید امضاء و درستی‌سنجی آن است به‌گونه‌ای که همه آن‌ها شامل بازیابی جزیی هستند. برای هر کدام از طرح‌های تعریف‌شده در این استاندارد نیز مثالی وجود دارد.

ث-۱ مثال‌های با توان عمومی ۳

بند ث-۱ شامل مثال‌هایی است که در آن‌ها توان عمومی برابر با ۳ است.

ث-۱-۱ مثالی از فرایند تولید کلید

کلید نمونه دارای یک پیمانه $k = ۱۰۲۴$ بیتی با توان عمومی $v = ۳$ است.

p FB96145 995C82F 527CAA B3FB42 6D00A0 8B2BDE 2E7B8F7 0C9E78
B7FABF E86E9F6 ACE3435 9D043A 93F3E47 D93FA88 D357790 77A949

q FF0EAFC 7058516 A8CD8E 36E752 2F32B86 068016B A89F2E 418882E
6F570122 F92D2E9 EFFF732 1818F25 BF095D6 208F93C CEF4767 568AB2

پیمانه عمومی n حاصلضرب عوامل ضرب اول پنهان[1] p و q است و طولی برابر با ۱۰۲۴ بیت دارد.

n FAA8ED EEF1CE D29814B EEAA15 C060BB EB1A51 AB0398 ADDFD3
CB9BE2 087B1D 1F78A39 62B5F20 7A73008 30913CD EE60183 E249DD
9CA4EB E0420E5 13D7305 4A73A92 BEFBFF C89858D 5E5B389 FEC5252

1- Secret prime factor

0493316 625F296 5AB8FA AA14C4 C0DD24 DEFCEB 2429110 0149A77

توان امضای خصوصی s برابر با وارون ضربی v به پیمانه lcm است (p-1,q-1).

s	0A71B48	DF4A13	5E1BAB	9F47163	92AEB2	A9CBC3	B1CAD1	3C93FE2
	33267EC	805A769	F6A506	F9723F6	1A6F75	ECB0B7	1F44010	9418693
	316AAC	F39B37	6105DF	AEA60B	C17306F	179F2ED	704D5A6	BCB141
	C9380F5	500823C	67E8ED	7F8A510	59E9541	498C91F	1ABE8C	6220E72

ث-۱-۲ مثال‌هایی با بازیابی کلی

سه مثال از از تولید امضاء و درستی‌سنجی آن و یک مثال برای هر کدام از سه طرح در این‌جا آورده شده است.

ث-۱-۲-۱ مثال طرح امضای ۱

این مثال از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به SHA-1 نیز شناخته می‌شود.)

ث-۱-۲-۱-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۶۴ نویسه کدگذاری شده اسکی تشکیل شده است.

abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopqopqrpqrs

پیام M در مبنای ۱۶ به‌صورت رشته هشت‌تایی زیر با طول ۶۴ یعنی ۵۱۲ بیت خواهد بود.

M	6162636	62636465	63646566	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727

۱۶۰بیت کد درهم با اعمال SHA-1 به ۵۱۲ بیت M محاسبه می‌شود.

H = 79EA0C76 F0056373 FFD6A5AA D389DD90 8B0C0E94

یک شناسه در فیلد پشت‌بند تابع درهم‌سازی را که در حال استفاده است نشان می‌دهد. استاندارد ISO/IEC 10118-3 شناسه تابع درهم‌ساز اختصاص یافته ۳ را برابر با مقدار ۳۳ قرار می‌دهد. بنابراین فیلد پشت‌بند T متشکل از ۱۶ بیت زیر خواهد بود.

T = 33CC

این پیام به اندازه کافی برای بازیابی کامل کوتاه است. ۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن دو بیت سرآیند با مقدار ۰۱، بیت بیشتر داده[1] برابر با 0 ، ۳۲۲ (۴-۱۶-۱۶۰-۵۱۲-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت مرزی[2] برابر ۱، ۵۱۲ بیت M_1 (M)، ۱۶۰بیت H و ۱۶ بیت فیلد پشت‌بند T تشکیل شده است. رشته قابل بازیابی S_r از جایگزینی ۸۲ نیبل لایه‌گذاری 0 با B به‌دست می‌آید. نیبل مرزی که برابر با ۱ است نیز با نیبلی برابر با A جای‌گذاری می‌شود.

2- More data
1- Border

S	4BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	
	BBBBB							
	BBBBB	BBBBB	BBBA61	6364626	6465636	6566646	6667656	676866
	6869676	696A686	6A6B696	6B6C6A	6C6D6B	6D6E6C	6E6F6D6	6F706E
	70716F7	7172707	727379E	0C76F00	6373FFD	A5AAD3	DD908B	0E9433

عدد صحیح قابل بازیابی f_r عدد صحیح مثبت بدون علامت نمایش داده شده توسط S_r است. f_r با توان s به پیمانه‌ی n افزایش داده شده است.

t	D636922	6E1FE0	7DF603	E5EE602	B4EF2E	3E8C3C	BA00057	40860A3
	FCA66D	33795AC	9119151	FE852CA	C80F315	8614205	ED32277	9F30793
	421D615	39792C4	1319F23	CFFD18	12D17A	442E5B	B17DCF	654BEF
	5F500A1	365CD5	BD2794	C938F7C	BA7759	472E892	7424A74	868B63

چون نتیجه فوق بزرگتر از n/2 است، امضاء به‌صورت $\sum = n - t$ است.

∑	24725B1	80D1ED	54A210F	08BBB52	0B718C	AC8E15	F1039362	6D59C8
	CEF574	D501C3	8E5F8E8	6430C55	B263CF	AA7D1C	012DF0C	431963E
	5A8789	A6C8E2	00BD3E	7A76905	AC2A85	8469FD1	ACDD68	997935C
	A543274	2C02539	9D91661	E0DBCD	0665CA	97CE621	B00469B	7ABE43

از آن‌جا که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

ث-۱-۲-۱-۲ فرآیند درستی‌سنجی

امضاء ∑ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	AEED31	3336127	16DC58	32EE599	04A4FF	2F5E962	EF47DD	F224177
	0FE0265	4CBF62	63BE423	FF518FA	160D9D	CB2AD8	87F8B2D	7AE176
	343B83	76D7A5	A96BC6	DF073E	528E93	5B29EC7	EFEBCB	8F54B6
	9421C1F	F0ECB8	E84580B	9D9DD4	5D6924	395217A	469885F	F2B573

از آن‌جا که f_s با (۱۲- n) به پیمانه ۱۶ هم‌نهشت است، می‌توان آن‌را با مکملش نسبت به n جایگزین کرد. به‌عبارت دیگر، عدد صحیح بازیابی‌شده $f_r' = n - f_s$ خواهد بود.

f	4BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB
	BBBBB	BBBBB	BBBA61	6364626	6465636	6566646	6667656	6768666
	6869676	696A686	6A6B696	6B6C6A	6C6D6B	6D6E6C	6E6F6D6	6F706E6
	70716F7	7172707	727379E	0C76F00	6373FFD	A5AAD3	DD908B	0E9433C

f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود.

- هشت‌تایی سمت چپ S_r' برابر با 4B است که شامل سرآیند برابر با ۰۱، بیت بیشتر- داده برابر با 0 (بازیابی کامل)، یک بیت لایه‌گذاری برابر با 0 و یک نیبل لایه‌گذاری برابر با B است. در ادامه، ۸۱ نیبل

دیگر با مقدار B قرار دارند. نیبل مرزی نیز مقداری برابر با A دارد. ۴۲ هشت‌تایی سمت راست S_r' حذف شده‌اند.

- سمت راست‌ترین هشت‌تایی S_r' برابر با CC است. بنابراین، پشت‌بند از دو هشت‌تایی تشکیل شده و مقداری برابر با 33CC دارد. این دو هشت‌تایی نیز از سمت راست S_r' حذف می‌شوند.

شناسه تابع درهم‌ساز برابر با 33 است. بنابراین، تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۳ است. بقیه رشته ۶۷۲ بیتی به دو قسمت تقسیم می‌شود.

- M_1^* شامل ۵۱۲ بیت سمت چپ است.
- H' شامل ۱۶۰ بیت سمت راست است.

M_1 6162636 62636465 6364656 6465666 6566676 6667686 6768696 68696A6
696A6B 6A6B6C6 6B6C6D 6C6D6E 6D6E6F 6E6F70 6F70717 7071727

H' 79EA0C76 F0056373 FFD6A5AA D389DD90 8B0C0E94

بدلیل کامل بودن بازیابی پیام، پیام بازیابی‌شده M^* تنها متشکل از M_1^* است. و H'' به‌عنوان کد درهم دیگر نیز با اعمال SHA-1 به M^* به‌دست می‌آید.

H'' 79EA0C76 F0056373 FFD6A5AA D389DD90 8B0C0E94

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۱-۲-۲ مثال طرح امضای ۲

این مثال از تابع درهم‌ساز اختصاصی ۱ از استاندارد ISO/IEC 10118-3 استفاده می‌کند (و به‌صورت RIPEMD-160 نیز شناخته می‌شود.)

ث-۱-۲-۲-۱ فرآیند امضاء

پیام M در مبنای ۱۶ به‌صورت رشته هشت‌تایی زیر با طول ۴۸ یعنی ۳۸۴ بیت خواهد بود.

M FEDCBA 765432 FEDCBA 7654321 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432

۱۶۰ بیت سالت S تولید می‌شوند.

S = 436BCA99 54EC376C 96B79C95 D4B82686 F3494AD3

۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی با طول ۷۶۸ (۱۶۰+۱۶۰+۳۸۴+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C طول پیام بازیابی‌شده، ۳۸۴ بیت قسمت غیر قابل بازیابی پیام M_1 (M)، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت S تشکیل شده است. $H=h(C \parallel M_1 \parallel h(M_2) \parallel S)$.

H = 50BE9461 4DA4AF5F 8E78C269 E0DFA03E 027CE74F

یک شناسه در فیلد پشت‌بند تابع درهم‌سازی که در حال استفاده است را نشان می‌دهد؛ استاندارد ISO/IEC 10118-3 مقدار شناسه را برای تابع درهم‌ساز اختصاصی ۱ به‌صورت مقدار ۳۱ قرار می‌دهد. بنابراین، فیلد پشت‌بند T متشکل می‌شود از ۱۶ بیتی که در ادامه می‌آید.

T = 31CC

این پیام به اندازه کافی برای بازیابی کامل کوتاه است. ۱۰۲۴ بیت رشته میانی[1] S_i از کنار هم قرار دادن ۳۰۳ (۱-۱۶-۱۶۰-۱۶۰-۳۸۴-۱۰۲۴) بیت لایه‌گذاری برابر با 0 ، بیت حاشیه برابر ۱، ۳۸۴ بیت M_1 (M)، ۱۶۰بیت L، ۱۶۰ بیت H و ۱۶ بیت فیلد پشت‌بند T تشکیل شده است.

S	0000000	0000000	00000000	0000000	0000000	0000000	0000000	0000000
	0000000	0001FE	BA98765	3210FE	BA9876	3210FE	BA98765	3210FED
	BA9876	3210FE	BA98765	3210FE	BA9876	3210436	CA9954	376C96
	9C95D4	2686F34	4AD350	94614D	AF5F8E	C269E0	A03E027	E74F31

رشته بازیابی‌شده S_r از اعمال تابع تولید ماسکMGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود، چرا که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است.

S	7BB5D9	4572EE	BECAE6	6939DC	A6F1986	8B33966	B09581D	7DC6906
	CFE499	108754	BC3AF3F	A6F562	6C91DA	BFF8CE	29AC5B	6C1B52
	49B7669	549E678	ABDAD6	A565394	7373C4C	4ECADF	08A5C00	0511B9F
	D78039	7F4BD7	420A50B	94614D	AF5F8E7	C269E0	A03E027	E74F31

عدد صحیح بازیابی‌شده f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. f_r به توان s به پیمانه n افزایش می‌یابد. نتیجه توسط عدد صحیح مثبت بدون علامت موقت t نمایش داده می‌شود.

t	A4958B	DA6AB0	E7F544B	1313DB9	BB7336	3678459	31386D3	9F0A477
	37B853D	6BBBA8	ECAC7C	B19FFA	98B40E	0B638D	7DDAAE	FF198E
	AB1002	76C1FF	03041201	FF8E6A	4AFDF0	06E10E	F3F6909	34864A
	D983AA	BD725F	A288DE	27810D3	807956	78F3CF	EA45A8	ADA422

رشته دودویی نمایش‌دهنده عدد صحیح t یک عدد صحیح بدون علامت است. این رشته امضایی است که توسط دیگر تابع تولید امضاء یعنی $\sum' = t$ تولید می‌شود. (به بند الف-۶ مراجعه شود.)

از آن‌جایی که نتیجه فوق بزرگتر از n/2 است، آن‌را با مکملش نسبت به n جایگذاری می‌کنیم. رشته دودویی نمایش‌دهنده آن عدد صحیح که به‌صورت یک عدد صحیح مثبت بدون علامت است، امضای $\sum = n - t$ است.

$\sum$ =	5613618	14871D	EAA2C	DB9639	04ED85	B4A20C	79CB2B	0ED58B
	93E38E	9CBF75	32CC26	B115F7	E1BEF2	252DAF	708569	E3304E1
	F194E8	69800E	10D31E	4AE53E	73FE0E	C1B74A	6A64A8	CA3ED
	2B0F86	A4ECC	B8301B	8293B7	4063CD	66091B	39E368	53A585

از آن‌جا که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

1- Intermediate string

ث-۱-۲-۲-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از$n/2$ است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	7EF3140	A97EE03	13CD2E	857038E	196F22D	5FE6BB	FA6E170	301942D
	FBB748	F7F3C90	633DAF	BBC08F	0DE125	70986E6	C4B3BD	762E8A
	52ED84	8BA3A6	67FC5A	A50E6F	4B883A	79CD79	55B5788	F9B36B
	2D12F76	E31351D	18AEA9	15B3774	117D95F	1C930A	83EB0E8	19FA75

از آن‌جایی که f_s با (۱۲۸- n) به پیمانه ۱۶ هم‌نهشت است می‌توان آن‌را با مکمل آن نسبت به n جایگزین کرد. به‌عبارت دیگر، عدد صحیح بازیابی‌شده $f_r' = n - f_s$ خواهد بود.

f_r	7BB5D9	4572EE	BECAE6	6939DC	A6F1986	8B33966	B09581D	7DC6906
	CFE499	108754	BC3AF3F	A6F562	6C91DA	BFF8CE	29AC5B	6C1B52
	49B7669	549E678	ABDAD6	A565394	7373C4C	4ECADF	08A5C00	0511B9F
	D78039F	7F4BD7	420A50B	94614D	AF5F8E7	C269E0	A03E027	E74F31

f_r' به‌صورت یک عدد صحیح مثبت بدون علامت توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' اعمال شده و S_i' رشته میانی بازیابی‌شده را نتیجه می‌دهد.

S_i	8000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0001FE	BA98765	3210FE	BA9876	3210FE	BA98765	3210FE
	BA9876	3210FE	BA98765	3210FE	BA9876	3210436	CA9954	376C96
	9C95D4	2686F34	4AD350	94614D	AF5F8E	C269E0	A03E027	E74F31

S_i' نشان‌دهنده رشته میانی بازیابی‌شده است که به‌شرح زیر به‌دست می‌آید:

- چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود چرا که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است. ۳۷ هشت‌تایی سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و هشت‌تایی حاشیه نیز مقدار ۰۱ را به خود می‌گیرد. این ۳۸ هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با CC است. بنابراین پشت‌بند از دو هشت‌تایی تشکیل شده و مقداری برابر با 31CC دارد. این دو هشت‌تایی نیز از سمت راست S_i' حذف می‌شوند.

شناسه تابع درهم‌ساز برابر با ۳۱ است. بنابراین تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۱ است.

رشته ۷۰۴ بیتی باقیمانده به ۳ قسمت تقسیم می‌شود.

- M_1^* متشکل از ۳۸۴ بیت سمت چپ است.
- S^* متشکل از ۱۶۰ بیت سمت راست است.
- H' متشکل از ۱۶۰ بیت سمت راست است.

M_1	FEDCBA	765432	FEDCBA	7654321	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432				
S^* =	436BCA9	54EC376	96B79C9	D4B8268	F3494AD			

H′ 50BE9461 4DA4AF5F 8E78C269 E0DFA03E 027CE74F

بدلیل کامل بودن بازیابی پیام، پیام بازیابی‌شده M^* تنها متشکل از M_1^* است. H''، کد درهم دیگر، نیز با اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی به‌دست می‌آید. طول این رشته ۷۶۸ (۱۶۰+۱۶۰+۳۸۴+۶۴) بوده و از کنار هم قرار دادن ۶۴ بیت از C'، طول پیام بازیابی‌شده، ۳۸۴ بیت پیام بازیابی‌شده M^*، ۱۶۰ بیت کد درهم قسمت غیرقابل بازیابی پیام $h(M_2)$ (که خالی است) و ۱۶۰ بیت سالت بازیابی‌شده S^* تشکیل شده است.
$H''= h(C' \| M_1^* \| h(M_2^*) \| S^*)$.

H″ 50BE9461 4DA4AF5F 8E78C269 E0DFA03E 027CE74F

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۱-۲-۳ مثال طرح امضای ۳

این مثال از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌عنوان SHA-1 نیز شناخته می‌شود.)

ث-۱-۲-۳-۱ فرآیند امضاء

پیامی که باید امضاء شود تهی است یعنی یک رشته دودویی با طول صفر.
از آن‌جا که این طرح امضاء از نوع قطعی است، یک مقدار سالت S با طول صفر انتخاب می‌شود.
۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۳ به رشته دودویی با طول ۲۲۴ (۱۶۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C طول پیام بازیابی‌شده و ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ (که خالی است) به‌دست می‌آید. ($H=h(C \| h(M_2))$)

H = A35D1688 A60AC69F D53E4442 8BFD380E 94DB9176

تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. بنابراین فیلد پشت‌بند T تنها متشکل است از یک هشت‌تایی است.

T = BC

این پیام به اندازه کافی برای بازیابی کامل کوتاه است. ۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۸۵۵ (۱۰۲۴-۱۶۰-۸) بیت لایه‌گذاری برابر با 0 ، بیت حاشیه برابر ۱، ۱۶۰ بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده است.

S 00000000 0000000 00000000 0000000 0000000 0000000 0000000 00000000
00000000 0000000 00000000 0000000 0000000 0000000 0000000 0000000
00000000 0000000 00000000 0000000 0000000 0000000 0000000 0000000
00000000 0000000 00000000 0000000 0000000 0000000 000001A 5D1688A
0AC69FD 3E44428 FD380E9 B9176B

رشته قابل بازیابی S_r از اعمال تابع تولید MGF1 ماسک به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. چپ‌ترین بیت S_r نیز از آن‌جا که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است برابر 0 قرار داده می‌شود.

S	7CCB54	2079C84	343B0AB	6307273	36359229	BD3DFD	A9FE80	AD1EF3
	44758A	3B7C70	FACB6F	12690E	6DF5897	585A78C	723F0C	50535C8
	8F0868F	CA94F3	FB079FB	9126286	5EECA3	ACA1259	033A0D	136A7A
	D60508	6CF68B	DA0AE6	5D1688	0AC69F	3E44428	FD380E	DB9176

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. f_r به توان s به پیمانه n افزایش می‌یابد. نتیجه توسط عدد صحیح مثبت بدون علامت موقت t نمایش داده می‌شود.

t	F9DD9F	FAB4AF	ED3B05	C5848B2	756AC5	B2890F	BC268D	C5E91E
	8E3B058	2EF6585	EF5323C	4E2C308	C6140C	F535796	5B3BF0	621082E
	77F4A42	3567355E	AA151F	652BAF	58A4B3	7A0646	FD4177C	D79F5D
	EEC562	A2D0F5	C409AE	D5B9F8	493AF2	8F91D8	CE32C4	35C1311

رشته دودویی نمایش‌دهنده عدد صحیح t یک عدد صحیح بدون علامت است. این رشته امضایی است که توسط دیگر تابع تولید امضاء یعنی $t = \sum'$ تولید می‌شود. (به بند الف.۶ رجوع شود.)
از آن‌جا که نتیجه فوق بزرگتر از n/2 است، امضاء به‌صورت $\sum = n - t$ است.

∑	00CB4D	F43D1E3	E55D0F	29258A2	4AF5F6	3891429	EEDD0B	E7F6B4
	3D60DC	D984C57	30257FC	1489C17	B45EF3	3B5BC3	93242771	80395A
	24B0470	AADAD8	69C2109	E547F92	66574C2	4E92127	6119C0D	2725C7
	15CDCE	BF8E338	96AF4C	D45ACC	77A2317	4F6B131	55F64C3	CB8876

از آن‌جا که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

ث-۱-۲-۳-۲ فرآیند درستی‌سنجی

امضاء ∑ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	7DDD99	CE7805E	9E5D0A	8BA2EE	8A2B29	2DDC53	0105188	00C0E01
	872657A	CCFEAD	24AD33	504CE32	0C7D77	D836C41	7C210B	91F68096
	0D9C82	15AD1A	18CF909	B94D80	600F5B	1BF7334	5B212B	EB5AAA
	2E8E295	F5689DF	80AE140	4CFE3C	B61684	A0B8A8	26F1027	25B830B

از آن‌جا که f_s با (۱۲- n) به پیمانه ۱۶ هم‌نهشت است عدد صحیح بازیابی‌شده $f_r' = n - f_s$ خواهد بود.

f_r	7CCB54	2079C84	343B0AB	6307273	36359229	BD3DFD	A9FE80	AD1EF3
	44758A	3B7C70	FACB6F	12690E	6DF5897	585A78C	723F0C	50535C8
	8F0868F	CA94F3	FB079FB	9126286	5EECA3	ACA1259	033A0D	136A7A
	D60508	6CF68B	DA0AE6	5D1688	0AC69F	3E44428	FD380E	DB9176

f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. رشته بازیابی‌شده S_r از اعمال تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴=) بیت سمت چپ S_r' به‌دست می‌آید.

S_i	00000000	0000000	0000000	00000000	0000000	0000000	0000000	0000000
	00000000	0000000	0000000	00000000	0000000	0000000	0000000	0000000
	00000000	0000000	0000000	00000000	0000000	0000000	0000000	0000000
	00000000	0000000	0000000	00000000	0000000	0000000	000001A	5D1688A
	0AC69FD	3E44428	FD380E9	DB9176B				

S_i' نشان‌دهنده رشته میانی بازیابی شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۱۰۶ هشت‌تایی سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و هشت‌تایی مرزی نیز مقدار ۰۱ را به خود می‌گیرد. این ۱۰۷ هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با BC است. این هشت‌تایی نیز از سمت راست S_i' حذف می‌شود.

از آن‌جا که پشت‌بند مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۳ است.

از آن‌جا که هیچ اطلاعات دیگری باقی نمانده است، رشته ۱۶۰ بیتی باقیمانده، کد درهم H' فرض می‌شود.

H' A35D1688 A60AC69F D53E4442 8BFD380E 94DB9176

پیام بازیابی‌شده M خالی فرض می‌شود و بنابراین بازیابی کامل است. H'' دیگر کد درهم نیز به‌وسیله اعمال تابع SHA-1 به رشته دودویی با طول ۲۲۴ (۱۶۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C' طول پیام بازیابی‌شده و ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ (که خالی است) به‌دست می‌آید. $H=h(C' \| h(M_2))$.

H'' A35D1688 A60AC69F D53E4442 8BFD380E 94DB9176

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۱-۳ مثال‌هایی با بازیابی جزیی

سه مثال از تولید امضاء و درستی‌سنجی آن و یک مثال برای هر کدام از سه طرح در این‌جا آورده شده است.

ث-۱-۳-۱ مثال طرح امضای ۱

این مثال از تابع درهم‌ساز اختصاصی ۱ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت RIPEMD-160 نیز شناخته می‌شود.)

ث-۱-۳-۱-۱ فرآیند امضاء

این مثال امضای یک پیام متشکل از ۱۳۲ هشت‌تایی یعنی ۱۰۵۶ بیت را نشان می‌دهد.

M FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 7654321

FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 7654321
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 7654321
FEDCBA

۱۶۰ بیت کد درهم از اعمال تابع درهم‌ساز اختصاصی ۱ به هر۱۰۵۶ بیت M محاسبه می‌شود.

H = F0EA911A F528FA38 777D4B9A 58B6FDA4 2D7E1999

تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. بنابراین فیلد پشت‌بند T از ۸ بیت زیر تشکیل شده-است

T = BC

در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طورکلی قابل بازیابی باشد. بنابراین آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۸۴۸ بیت سمت چپ.
- M_2 متشکل است از ۲۰۸ بیت باقیمانده یعنی ۲۶ هشت‌تایی.

M FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 7654321
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 7654321
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDC

M۲ BA98 76543210 FEDCBA98 76543210 FEDCBA98 76543210 FEDCBA98

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن دو بیت سرآیند با مقدار ۰۱، بیت بیشتر داده برابر با ۱ ، چهار (۴-۸-۱۶۰-۸۴۸-۱۰۲۴) بیت لایه‌گذاری برابر با 0 ، بیت حاشیه برابر ۱، ۸۴۸ بیت M_1 (M)، ۱۶۰بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده است. رشته قابل بازیابی S_r از جایگزینی نیبل مرزی که برابر با ۱ است با نیبلی برابر با A منتج می‌شود.

S_r 6AFED 9876543 10FEDC 9876543 10FEDC 9876543 10FEDC 9876543
10FEDC 9876543 10FEDC 9876543 10FEDC 9876543 10FEDC 9876543
10FEDC 9876543 10FEDC 9876543 10FEDC 9876543 10FEDC 9876543
10FEDC 9876543 10FEDC EA911A 28FA38 7D4B9A B6FDA4 7E1999

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. f_r به توان s به پیمانه n افزایش می‌یابد. نتیجه توسط عدد صحیح مثبت بدون علامت موقت t نمایش داده می‌شود.

t C9DE5B 67CFD8 506749A2 F2E5035 9C2C5E 3DD4683 AEF714 A01283F
95C35F 53A8755 AEADBB 2B9876E 14EA5C EA11BC F33E516 7B4B73
38EB6D AA3DF3 1434E846 E2E7414 E24C71 D2A0FB 77E3737 1444360
962A9C D9CC2E 4FE30BE A3E20B 0CCF47 70E64A9 9FFAA5 98BC10

چون نتیجه فوق بزرگتر از n/2 است،. امضاء به‌صورت $\sum = n - t$ است.

∑	30CA91	8721F57	8230CB1	FBC511	24345CA	AD45E9	FC0C848	0DCD4F
	35D8822	B4D2A8	70CAE7	371D7B	6588A45	467F801	FB21C6	66FE69
	63B97D	36041B2	FFA2480	678C67	DCAF8D	F5F75CF	E677C52	EA80EF
	6E68953	8892FB4	0AD5EE	0632B9	B40DDD	6E16A09	842E6B9	688D96

پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۲۶ هشت‌تایی از پیام غیر قابل بازیابی M_2تنها ۲۲ هشت‌تایی از پیام M بیشتر است.

ث-۱-۳-۱-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	8FAA10	567B7A0	C19937F	5633C11	AF61DE	52A3FD	9A04BC	15697F0
	BA9D05	7004C9A	0E79C6	CA3F9D	697423C	981AE8	DD613B	49D388
	8BA60E	47CBBA	02D8539	B1FD54	ADFD22	302204A	4D5C5B	664ED0
	F39454A	C9E8D5	49BA1D	BF83A9	97E2EB	61B150E	6D2B6C	83300D

از آن‌جایی که f_s با (۱۲- n) به پیمانه ۱۶ هم‌نهشت است می‌توان آن را با مکمل آن نسبت به n جایگزین کرد. به‌عبارت دیگر، عدد صحیح بازیابی‌شده $f_r^{'} = n - f_s$ خواهد بود.

f	6AFEDC	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	9876543
	10FEDCB	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	9876543
	10FEDCB	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	664ED0
	10FEDCB	987654	10FEDC	EA911A	28FA387	7D4B9A	B6FDA4	7E1999

$f_r^{'}$ یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی شده $S_r^{'}$ نمایش داده می‌شود.

- هشت‌تایی سمت چپ $S_r^{'}$ برابر با 6A است. این هشت‌تایی شامل سرآیند برابر با 01، بیت بیشتر- داده برابر با ۱ (بازیابی جزیی)، یک بیت لایه‌گذاری برابر با 0 و یک نیبل مرزی برابر با A است. این هشت‌تایی از سمت چپ $S_r^{'}$ حذف می‌شود.
- هشت‌تایی سمت راست $S_r^{'}$ برابر با BC است. این هشت‌تایی نیز از سمت راست $S_r^{'}$ حذف می‌شود.

از آن‌جا که پشت‌بند مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۱ است.

رشته ۱۰۰۸ بیتی باقی‌مانده نیز به دو قسمت تقسیم می‌شود:

- M_1^{*} متشکل است از ۸۴۸ بیت سمت چپ
- $H^{'}$ متشکل است از ۱۶۰ بیت سمت راست

M_1	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	7654321
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	7654321
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDC					

H′ = F0EA911A F528FA38 777D4B9A 58B6FDA4 2D7E1999

از آن‌جا که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^* قسمت بازیابی‌شده و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

M_1	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	7654321
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	7654321
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA							

دیگر کد درهم H'' از اعمال تابع درهم‌ساز اختصاصی ۱ به M^* به‌دست می‌آید.

H″ F0EA911A F528FA38 777D4B9A 58B6FDA4 2D7E1999

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۱-۳-۲ مثال طرح امضاء ۲

این مثال از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت SHA-1 نیز شناخته می‌شود.)

ث-۱-۳-۲-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۱۱۲ نویسه کدگذاری شده ASCII تشکیل شده است.

Abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopqopqrpqrsqrstrstustuvtuvw
uvwxvwxywxyzxyzayzabzabcabcdbcde

در مبنای شانزده، پیام M رشته هشت‌تایی زیر با طول ۱۱۲ هشت‌تایی است؛ یعنی ۸۹۶ بیت.

M	6162636	62636465	63646566	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	73747576	7475767	7576777	7677787	7778797	78797A
	797A616	7A61626	61626364	6263646				

۱۶۰ بیت سالت S تولید می‌شوند.

S = 4C95C1B8 7A1DE8AC C193C14C F3147FE9 C6636078

در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طورکلی قابل بازیابی باشد. بنابراین، آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۶۸۸ بیت سمت چپ
- M_2 متشکل است از ۲۰۸ بیت یا همان ۲۶ هشت‌تایی باقی‌مانده

M	6162636	62636465	63646566	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727

7172737 72737475 73747576 7475767 7576777 7677

M_2 7879 7778797A 78797A61 797A6162 7A616263 61626364 62636465

۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۳ به رشته دودویی با طول ۱۰۷۲ (=۱۶۰+۱۶۰+۶۸۸+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C، طول پیام قابل بازیابی، ۶۸۸ بیت قسمت قابل بازیابی پیام M_1، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت S تشکیل شده است. $H=h(C \parallel M_1 \parallel h(M_2) \parallel S)$

H = 16671F61 4F2954A8 6E51CB81 102A3D47 E2C11EBD

تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. بنابراین فیلد پشت‌بندT تنها شامل هشت‌تایی زیر است.

T = BC

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۷ (۱-۸-۱۶۰-۱۶۰-۶۸۸-۱۰۲۴) بیت‌های لایه‌گذاری برابر با 0، بیت حاشیه برابر ۱، ۶۸۸ بیت M_1، ۱۶۰بیت L، ۱۶۰ بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده‌است.

S	0161626	6462636	65636465	6664656	6765666	6866676	6967686	6A68696
	6B696A	6C6A6B	6D6B6C	6E6C6D	6F6D6E	706E6F	716F707	72707172
	7371727	7472737	75737475	7674757	7775767	7876774	95C1B8	1DE8AC
	93C14C	147FE9C	63607816	671F614	2954A86	51CB81	2A3D47	C11EBD

رشته قابل بازیابی S_r از اعمال تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. از آن‌جایی که δ =۱ ((۱۰۲۴-۱) به پیمانه ۸)است، چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود.

S	390871A	2B83F41	63782F5	BB700D	63C071	98C7D1	9B8616A	B72DF9D
	B899BF	C3839D	903CEF	A9C1849	6412999	6FE8D3	FDA1D0	2251EAA
	34017F7	C66DD6	D3F001	23CA2D	43383F3	9724B84	2529C5F	73205FB
	D1FCC8	D18C68	B9E356	671F614	2954A8	51CB81	2A3D47E	C11EBD

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. f_r به توان s به پیمانه n افزایش می‌یابد. نتیجه توسط عدد صحیح مثبت بدون علامت موقت t نمایش داده می‌شود.

t	92ACA1	2842617	1E4A13	C051048	8C3CC91	1CB6F5	CF95090	5FDEA5
	3C189F6	E6BA3F	4268B4	2363B3B	12D023A	1C96541	C1F9E6	58F6B3
	8DEB1B	41792AA	341DB1	88366A5	1E18DB	E4A2E3	77A2B4	1DFB34
	CCAD18	C4AFFA	5570855	AEB685	2E1F124	F70F529	ED02F5	BFD572

رشته دودویی نمایش‌دهنده عدد صحیح t یک عدد صحیح بدون علامت است. این رشته امضایی است که توسط دیگر تابع تولید امضاء یعنی $t = \sum'$ تولید می‌شود. (به بند ب-۶ رجوع شود.)

از آن‌جا که نتیجه فوق بزرگتر از n/2 است، امضاء به‌صورت $\sum = n - t$ است.

$\sum$	67FC4B	C6AF6C	B44E01A	2E5910C	3423F21	CE635C	DB6E8F	4E012E1
	8F8342A	21C0DE	DD0FEE	3F523E5	67A2DC	13FAE8	2C66322	8953293
	0EB9CF	9EC8E3	DFB97E	C23D3E	A0E3237	E3F5754	E6B8839	E0C9F0

37E6195 9DAF2E 0548754 FB5E3F 92BE122 E7ED98 37261BF 417434

پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۲۶ هشت‌تایی از پیام غیر قابل بازیابی M_2، تنها ۴۲ هشت‌تایی از پیام M بیشتر است.

ث-۱-۳-۲-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	C1A07B	C36DDA	6F1FE55	333A077	5CA049	5252809	0F7D823	F6B1D95
	13022263	44F7800	8F3BB42	B8F46D	166066F	C0A868	F0BE47	BFF7F26
	68A36B	19D4384	3FE72F0	26A97B	7BC3C0	3173A09	3931729	8BA4C5
	32966893	90D2C0E	A0D5A4	42F563	97887C0	8D316A	F9EBC9	402AE9

از آن‌جایی که f_s با (n -۱۲) به پیمانه ۱۶ هم‌نهشت است، عدد صحیح بازیابی‌شده $f_r^{'} = n - f_s$ خواهد بود.

f_r	390871A	2B83F41	63782F5	BB700D	63C071	98C7D1	9B8616A	B72DF9
	B899BF	C3839D	903CEF	A9C1849	6412999	6FE8D3	FDA1D0	2251EA
	34017F7	C66DD6	D3F001	23CA2D	43383F3	9724B84	2529C5F	73205FB
	D1FCC8	D18C687	B9E356	671F614	2954A8	51CB81	2A3D47E	C11EBDBC

$f_r^{'}$ یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده $S_r^{'}$ نمایش داده می‌شود. رشته بازیابی‌شده S_r از اعمال تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ $S_r^{'}$ به‌دست می‌آید.

S_i	0161626	6462636	6563646	6664656	6765666	6866676	6967686	6A68696
	6B696A	6C6A6B	6D6B6C	6E6C6D	6F6D6E	706E6F	716F707	72707172
	7371727	7472737	7573747	7674757	7775767	7876774	95C1B8	1DE8AC
	93C14C	147FE9C	6360781	671F614	2954A8	51CB81	2A3D47	C11EBD

$S_i^{'}$ نشان‌دهنده رشته میانی بازیابی‌شده است که به شرح زیر به‌دست می‌آید:

- از آن‌جایی که δ =۱ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت $S_i^{'}$ برابر 0 قرار داده می‌شود. ۷ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت مرزی نیز مقدار ۱ را به خود می‌گیرد. این هشت‌تایی از سمت چپ $S_i^{'}$ حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی $S_i^{'}$ برابر با BC است. این هشت‌تایی نیز از سمت راست $S_i^{'}$ حذف می‌شود.

از آن‌جا که فیلد پشت‌بند T مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۳ است.

رشته ۱۰۰۸ بیتی باقی‌مانده به ۳ قسمت تقسیم می‌شود.

- M_1^* متشکل از ۶۸۸ بیت سمت چپ است.
- S^* متشکل از ۱۶۰ بیت سمت راست است.
- $H^{'}$ متشکل از ۱۶۰ بیت سمت راست است.

M_1 6162636 62636465 6364656 6465666 6566676 6667686 676869 68696A
696A6B6 6A6B6C6 6B6C6D 6C6D6E 6D6E6F 6E6F70 6F7071 707172
7172737 72737475 7374757 7475767 7576777 7677

S^* 4C95C1 7A1DE8 C193C14 F3147FE C663607

H' 16671F61 4F2954A8 6E51CB81 102A3D47 E2C11EBD

از آن‌جایی که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^* قسمت بازیابی‌شده و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

M 6162636 62636465 63646566 6465666 6566676 6667686 6768696 68696A6
696A6B6 6A6B6C6 6B6C6D 6C6D6E 6D6E6F 6E6F70 6F70717 7071727
7172737 72737475 73747576 7475767 7576777 7677787 7778797 78797A
797A616 7A61626 61626364 6263646

H''، کد درهم دیگر، با اعمال SHA-1 به رشته دودویی با طول ۱۰۷۲ (۱۶۰+۱۶۰+۶۸۸+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C' طول پیام بازیابی‌شده، ۶۸۸ بیت قسمت M_1^* پیام بازیابی‌شده، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت بازیابی S^* تشکیل شده است. $H''=h(C' \| M_1^* \| h(M_2^*) \| S^*)$.

H'' 16671F61 4F2954A8 6E51CB81 102A3D47 E2C11EBD

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۱-۳-۳ مثال طرح امضاء ۳

این مثال از تابع درهم‌ساز اختصاصی۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت SHA-1 نیز شناخته می‌شود.)

ث-۱-۳-۳-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۱۳۲ هشت‌تایی یا همان ۱۰۵۶ بیت تشکیل شده است.

M FEDCB 7654321 FEDCB 7654321 FEDCB 7654321 FEDCB 7654321
FEDCB 7654321 FEDCB 7654321 FEDCB 7654321 FEDCB 7654321
FEDCB 7654321 FEDCB 7654321 FEDCB 7654321 FEDCB 7654321
FEDCB 7654321 FEDCB 7654321 FEDCB 7654321 FEDCB 7654321
FEDCB

از آن‌جایی که این طرح امضاء از نوع قطعی است، یک مقدار سالت S با طول صفر انتخاب می‌شود.
در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طور کلی قابل بازیابی باشد. بنابراین آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۸۴۰ بیت سمت چپ
- M_2 متشکل است از ۲۱۶ بیت یا همان ۲۷ هشت‌تایی باقی‌مانده

M FEDCBA98 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA98 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA98 765432 FE

M_2 DCBA9 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA98

۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۳ به رشته دودویی با طول ۱۰۶۴ (۶۴+۸۴۰+۱۶۰) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C، طول پیام قابل بازیابی، ۸۴۰ بیت قسمت قابل بازیابی پیام M_1 و ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$. $H=h(C \| M_1 \| h(M_2) \| S)$

H E30A9CB8 F10DC3C8 1897D9E8 D394555A AC6DEC79

یک شناسه در فیلد پشت‌بند T تابع درهم‌سازی که در حال استفاده است را نشان می‌دهد. استاندارد ISO/IEC 10118-3 شناسه تابع درهم‌ساز اختصاص یافته ۳ را برابر با مقدار ۳۳ قرار می‌دهد. بنابراین فیلد پشت‌بند T متشکل از ۱۶ بیت زیر خواهد بود.

T = 33CC

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۷ (۱-۱۶-۱۶۰-۸۴۰-۱۰۲۴) بیت لایه‌گذاری برابر با 0 ، بیت مرزی برابر ۱، ۸۴۰ بیت M_1، قسمت قابل بازیابی پیام، ۱۶۰بیت کد درهم قسمت h(M2)، قسمت غیرقابل بازیابی پیام و ۱۶ بیت فیلد پشت‌بند T تشکیل شده است.

S 01FEDC 987654 10FEDC 10FEDC 10FEDC 9876543 10FEDC 9876543
01FEDC 987654 10FEDC 10FEDC 10FEDC 9876543 10FEDC 9876543
01FEDC 987654 10FEDC 10FEDC 10FEDC 9876543 10FEDC 9876543
01FEDC 987654 10FEE30 9CB8F10 C3C8189 D9E8D3 555AAC EC7933

رشته قابل بازیابی S_r از اعمال تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. نیز از آن‌جایی که δ =۱ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_r برابر 0 قرار داده می‌شود.

S	1E1F9F6	4356F60	0062DE	FC99458	8259AE	7F4ACA	0655D64	0435C851
	ED9D17	837A12	1886C24	DED123	470510B	459AD41	9931003	C824907
	0DC63B	422008F	4D68E9	0DFDD5	8FAD50	DD7A43	BB38E64	EEDF14
	2549A7F	B1869D	C4E5E3	9CB8F10	C3C818	D9E8D3	555AAC	EC7933C

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. f_r به توان s به پیمانه n افزایش می‌یابد. نتیجه درصورت کوچکتر بودن از n/2 حفظ می‌شود. رشته دودویی نمایش‌دهنده این عدد صحیح به‌عنوان یک عدد صحیح مثبت بدون علامت، امضاء $\sum$ است.

30147E	074705D	F33EF7	D0EE10	D5535A	9A7727	D8D4DC	42C693B
1FB544	AE2323	185BED	C8AA5F	9D3AAE	1FC3EC	DF297A	56D6BC
5196A6	806E3F	F8A841	2984EF9	33940013	4A6D17	2FCF094	783AEB
6F11397	66863E7	28F4542	E2AE8A	7355633F	380F937	308C149	1419448

در این مثال امضای تولیدشده توسط دیگر تابع تولید امضاء نیز رشته دودویی $\sum$ است، یعنی $\sum'=\sum$.
پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۲۷ هشت‌تایی از پیام غیر قابل بازیابی M_2 تنها ۲۳ هشت‌تایی از پیام M بیشتر است.

ث-۱-۳-۳-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح به توان ۳ به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	1E1F9F6	4356F60	0062DE	FC99458	8259AE	7F4ACA	0655D64	0435C851
	ED9D17	837A12	1886C24	DED123	470510B	459AD41	99310030	C824907
	0DC63B	422008F	4D68E9	0DFDD5	8FAD50	DD7A43	BB38E64	EEDF14
	2549A7F	B1869D	C4E5E3	9CB8F10	C3C818	D9E8D39	555AAC	EC7933C

از آن‌جا که f_s با ۱۲ به پیمانه ۱۶ هم‌نهشت است، عدد صحیح بازیابی‌شده $f_r' = f_s$ خواهد بود.
f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. رشته بازیابی‌شده S_i' از اعمال تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' به‌دست می‌آید.

S	81FEDC	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	9876543
	10FEDC	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	9876543
	10FEDC	987654	10FEDC	9876543	10FEDC	9876543	10FEDC	9876543
	10FEDC	987654	10FEDC	9CB8F1	C3C8189	D9E8D3	555AAC	EC7933

S_i' نشان‌دهنده رشته میانی بازیابی‌شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۷ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت مرزی نیز مقدار ۱ را به خود می‌گیرد. این هشت‌تایی از سمت چپ S_i' حذف می‌شوند.

- سمت راست‌ترین هشت‌تایی S_i' برابر با CC است. بنابراین پشت‌بند از دو هشت‌تایی تشکیل شده و برابر با 33CC است. این دو هشت‌تایی نیز از سمت راست S_i' حذف می‌شود.

از آن‌جا که پشت‌بند مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۳ است.

نشانگر تابع درهم‌ساز برابر با ۳۳ است. بنابراین تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۳ است.

باقی رشته ۱۰۰۰ بیتی به دو قسمت تقسیم می‌شود.

- M_1^* شامل ۸۴۰ بیت سمت چپ می‌شود.
- H' شامل ۱۶۰ بیت سمت راست می‌شود.

M_1 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FE

H' E30A9CB8 F10DC3C8 1897D9E8 D394555A AC6DEC79

از آن‌جا که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^* قسمت بازیابی‌شده و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

M FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA

H''، کد درهم دیگر، با اعمال SHA-1 به رشته دودویی با طول ۱۰۶۴ (۱۶۰+۸۴۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C' طول پیام بازیابی‌شده، ۸۴۰ بیت قسمت M_1^* پیام بازیابی‌شده، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2^*)$ تشکیل شده‌است. $H''=h(C' \| M_1^* \| h(M_2^*))$.

H' E30A9CB8 F10DC3C8 1897D9E8 D394555A AC6DEC79

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲ مثال‌هایی با توان عمومی ۲

بند ث-۲ شامل مثال‌هایی با کلید عمومی ۲ است.

ث-۲-۱ مثال‌هایی از فرآیند تولید کلید

این کلید نمونه پیمانه‌ای با k =۱۰۲۴ بیت و توان عمومی ۲ دارد. از آن‌جا که توان درستی‌سنجی عمومی v زوج است، یکی از ضرایب اصلی پنهان هم‌نهشت با ۳ به پیمانه ۸ و دیگری با ۷ به پیمانه ۸ سازگار است.

p F69AD6 F97E4CC B4A76F 1F43871 C71100C F9256C3 BE98CC BEC063
A2282D CFCAF0 0E7492C 1FB19C 0F73EEF 1A08B0 6756E7D 5670D6

q C41DB9 D877706 2BEA883 1E49AF B5B6CB 2847958 472150 96C65E8
C211458 FDE60F E12CA9 A370A3 74D33B5 8EB791 0FD528 3D8F61

پیمانه عمومی n حاصلضرب ضرایب اصلی پنهان p و q است. طول آن برابر با ۱۰۲۴ بیت است.

n BCEB2E 2E1C8E 99BC96 F8F91D 084EA6E C75BD1 D0CDBE 21DA29F
9E73112 9DB0D1 B192018 A8126B 2D13AB 9958763 DA8F79F 62C7379
6109D2C 4AA2E0 B383A7 BF17FF 145760A 8B58BE 00C52BA BD05A9
BE5BA5 E6721F 066D37 9BF072 7BABB2 F6B2963 043DB47 6F9D217

توان امضای خصوصی s برابر با معکوس حاصلضربی v به پیمانه lcm است ۲/ (p-1,q-1).

n 029FB5F 55F9491 7777F3D 7FE703 A3ABC2 70FDB8 6A02DB 2794CEC
05C1992 85BEE67 57CCB1 8972089 1D120D0 FB04C8 D141FE2 5A42C45
F0883D5 73742EB 98435B5 B393B4 F053C59 A8950D CA990A 888C6D
085CEB 6B02AE BCC2D5 B4C9F9 3FE1657 2F4E084 9AD9224 D8622D

ث-۲-۲ مثال‌هایی با بازیابی کامل

سه مثال از از تولید امضاء و درستی‌سنجی آن و یک مثال برای هر کدام از سه طرح در این‌جا آورده شده است.

ث-۲-۲-۱ مثال طرح امضاء ۱

این مثال از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت SHA-1 نیز شناخته می‌شود.)

ث-۲-۲-۱-۱ فرآیند امضاء

پیام M در مبنای ۱۶ به‌صورت رشته هشت‌تایی زیر با طول ۴۸ یعنی ۳۸۴ بیت خواهد بود.

M FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432

۱۶۰بیت کد درهم با اعمال تابع درهم‌ساز اختصاصی ۳ به ۳۸۴ بیت M محاسبه می‌شوند.

H = 85DCC7FC 51371637 5A059D02 5439FCD9 25C828AC

تابع درهم‌ساز در حال استفاده به‌طور ضمنی معلوم است. بنابراین فیلد پشت‌بند T متشکل از ۸ بیت زیر خواهد بود.

T = BC

این پیام به اندازه کافی برای بازیابی کامل کوتاه است. ۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن دو بیت سرآیند با مقدار ۰۱، بیت بیشتر داده برابر با 0 ، ۴۶۸ (۴-۸-۱۶۰-۳۸۴-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت حاشیه برابر ۱، ۳۸۴ بیت M_1 (M)، ۱۶۰بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده است. رشته قابل بازیابی

S_r از جایگزینی ۱۱۶ نیبل لایه‌گذاری ۰ با B به‌دست می‌آید. نیبل مرزی که برابر با ۱ است نیز با نیبلی برابر با A جای‌گذاری می‌شود.

S	4BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB
	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	DCBA98
	543210F	DCBA98	543210F	DCBA98	543210F	DCBA98	543210F	DCBA98
	543210F	DCBA98	5432108	DCC7FC	3716375	059D025	39FCD9	C828AC

عدد صحیح قابل بازیابی f_r عدد صحیح مثبت بدون علامت نمایش داده شده توسط S_r است. از آن‌جا که ژاکوبی f_r نسبت به n برابر ۱ است، نتیجه حفظ می‌شود. l_r با توان s به پیمانه‌ی n افزایش داده شده است رشته دودویی نمایش‌دهنده آن عدد صحیح که به‌صورت یک عدد صحیح مثبت بدون علامت است امضاء $\sum$ است.

$\sum$	0C0C62D	523F2D	972679D	348D9A	38E93AE	D19E97	875DCC	6B2637D
	CE7D4C	5967529	B96D27	D9B41F	56E65EE	328FDB	AE6F4E	A0CFC1
	F8AB5A	CC7C9B	487EC2	90CBC2	1AFDC5	9C3478	3C46D5	A0E08D
	D965A9	FCAFE3	2D64B1	0706AF	43288156	DA3FF9	CB040D	0863F26

از آن‌جا که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

ث-۲-۲-۱-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. مجذور این عدد صحیح به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	712F72F	7260D2	DE00DA	3D3D61	4C92EB	0BA015D	1512031	661E6E3
	E2B7556	E1F515	F5D645	EC56AF	7157EF	DD9CBA	1ED3BE	860C9F
	0CD7C1	6DE847	5F51964	E25D675	C0254F	AE9E25C	AC931A	E04B11
	6A29940	09B7874	B23B272	BF28767	44957B1	F11593D	CA40DB	A77474

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جا که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۰۰۱ هستند، $f_r' = n - f_s$ خواهد بود.

f_r'	4BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB
	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	BBBBB	DCBA98
	543210F	DCBA98	543210F	DCBA98	543210F	DCBA98	543210F	DCBA9
	543210F	DCBA98	5432108	DCC7FC	3716375	059D025	39FCD9	C828AC

f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود.

- هشت‌تایی سمت چپ S_r' برابر با 4B است. این هشت‌تایی شامل سرآیند برابر با ۰۱، بیت بیشتر- داده برابر با 0 (بازیابی کامل)، یک بیت لایه‌گذاری برابر با 0 و یک نیبل لایه‌گذاری برابر با B است. در ادامه ۱۱۵ نیبل دیگر با مقدار B قرار دارند. نیبل مرزی نیز مقداری برابر با A دارد. ۵۹ هشت‌تایی سمت راست Sr′ حذف شده‌اند.
- سمت راست‌ترین هشت‌تایی S_r' برابر با BC است. این هشت‌تایی نیز از سمت راست S_r' حذف می‌شوند.

از آن‌جا که پشت‌بند مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۳ است.

باقی رشته ۵۴۴ بیتی به دو قسمت تقسیم می‌شود.

- M_1^* شامل ۳۸۴ بیت سمت چپ می‌شود.
- H' شامل ۱۶۰ بیت سمت راست می‌شود.

M_1 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432

H' 85DCC7FC 51371637 5A059D02 5439FCD9 25C828AC

به‌دلیل کامل بودن بازیابی پیام، پیام بازیابی‌شده M^* تنها متشکل از M_1^* است. H''، کد درهم دیگر، نیز با اعمال SHA-1 به M^* به‌دست می‌آید.

H'' 85DCC7FC 51371637 5A059D02 5439FCD9 25C828AC

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲-۲-۲ مثال طرح امضای ۲

این مثال از تابع درهم‌ساز اختصاصی ۱ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت RIPEMD-160 نیز شناخته می‌شود.)

ث-۲-۲-۲-۱ فرآیند امضاء

پیام مورد نظر برای امضاء خالی است، یعنی یک رشته دودویی با طول صفر.

۱۶۰ بیت سالت S تولید می‌شوند.

S = 61DF870C 4890FE85 D6E3DD87 C3DCE372 3F91DB49

۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به یک رشته دودویی با طول ۳۸۴ (=۱۶۰+۱۶۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C طول پیام قابل بازیابی، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت S تشکیل شده است. $H=h(C \parallel h(M_2) \parallel S)$.

H = 632E21FD 52D2B95C 5F7023DA 63DE9509 C01F6C7B

تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. بنابراین فیلد پشت‌بند T تنها متشکل است از هشت بیت.

T = BC

پیـام خالی است و بنابـراین بازیـابی پیـام کامل است. ۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۶۹۵ (۱-۸-۱۶۰-۱۶۰-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت مرزی برابر ۱، ۱۶۰بیت S، ۱۶۰ بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده است.

S	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000161	DF870C4	90FE85D6	E3DD87C	DCE3723	91DB496	2E21FD5
	D2B95C5	7023DA6	DE9509C	1F6C7BB			

رشته بازیابی‌شده S_r از اعمال تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. از آن‌جایی که δ (۱۰۲۴-۱) = ۱ به پیمانه ۸) است، چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود.

S_r	73FEAF	EB12914	43FE63	22BB4A	188A8F3	BD8D8A	4AD6C3	EE92035
	C7F237	36B1212	E947F6	C68FE3	247D27D	F298CA9	02EB21	A64C26
	44471EF	C0DFE1	4606F0	8E63E87	DACA99	FA62973	567473B	D38FAE
	AB2286	934A9C	D3263E	2E21FD	D2B95C	7023DA6	DE9509	1F6C7B

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نمایش داده می‌شود. از آن‌جایی که ژاکوبی f_r نسبت به n برابر ۱- می‌شود، $J=f_r/2$ عدد صحیح نمایشگر آن است.

J	39FF578	F58948	21FF31A	115DA5	0C45479	5EC6C5	256B61A	F74901A
	E3F91B	1B5890	F4A3FB	6347F1B	123E93E	F94C654	817590F	5326136
	22238F7	606FF0	A303785	4731F43	6D654C	FD314B	AB3A39	69C7D73
	D591430	49A54E	E9931F3	9710FE	695CAE	B811ED	EF4A84E	0FB63D

J به توان s به پیمانه n افزایش می‌یابد و نتیجه به‌صورت زیر خواهد بود.

J	B6935A	DCABB3	D7A712	CA86B2	AF7937D	4F52362	93B07B	895A467
	50553EC	92570E7	975CDB	D3EC94	CA626E9	4E7FD5	16ED9C	9E619D
	DC05A5	4089E59	50C9E86	4DD10E	DD70915	843D755	057C99F	7133025
	E56474B	6A7A484	DC1F41	1603BB	DBA44A	1A6F821	4013757	67C97D

چون نتیجه فوق بزرگتر از n/2 است، امضاء به‌صورت $\sum = n - t$ است.

Σ	0657D3	5170DB7	C21583A	2E726A	58D56F0	78099B6	3D1D42	987FE37
	4E1DD2	0B59C31	1A3525F	D425D6	62B13D	4AD8A0	C3A1DD	C46599
	85042D2	0A18FA	62B9BE	7146F17	36E6CF	071B48E	FB4891A	4BD2A7
	D8F7304	7BF7D77	2A4DF6	85ECB7	A007678	DC4314	C42A3F0	07D3A46

از آن‌جا که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

ث-۲-۲-۲-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. مجذور این عدد صحیح به پیمانه n رسیده و عدد صحیح f_s را نتیجه می‌دهد.

f	39FF578	F58948	21FF31A	115DA5	0C45479	5EC6C5	256B61A	F74901A
	E3F91B	1B5890	F4A3FB	6347F1B	123E93E	F94C654	817590F	5326136
	22238F7	606FF0	A303785	4731F43	6D654C	FD314B	AB3A39	69C7D73
	D591430	49A54E	E9931F3	9710FE	695CAE	B811ED	EF4A84E	0FB63D

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جایی که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۱۱۰ هستند، $f_r' = 2f_s$ خواهد بود.

f_r	73FEAF	EB12914	43FE635	22BB4A	188A8F3	BD8D8A	4AD6C3	EE92035
	C7F237	36B1212	E947F67	C68FE36	247D27D	F298CA9	02EB21	A64C26
	44471EF	C0DFE1	4606F0B	8E63E87	DACA99	FA62973	567473B	D38FAE
	AB2286	934A9C	D3263E6	2E21FD	D2B95C5	7023DA6	DE9509	1F6C7B

f_r' به‌صورت یک عدد صحیح مثبت بدون علامت توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' اعمال شده و S_i' رشته میانی بازیابی‌شده را نتیجه می‌دهد.

S_i	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000161	DF870C4	90FE85D	E3DD87C	DCE3723	91DB496	2E21FD5
	D2B95C5	7023DA6	DE9509C	1F6C7BB			

S_i' نشان‌دهنده رشته میانی بازیابی شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۶۹۵ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت مرزی نیز مقدار ۱ را به خود می‌گیرد. این ۸۷ هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با BC است. این هشت‌تایی نیز از سمت راست S_i' حذف می‌شوند.

از آن‌جا که پشت‌بند مقداری برابر با BC دارد، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است. این تابع در این مثال تابع درهم‌ساز اختصاصی ۱ است.

رشته ۳۲۰ بیتی باقیمانده به ۲ قسمت تقسیم می‌شود:

- S^* متشکل از ۱۶۰ بیت سمت راست است.
- H' متشکل از ۱۶۰ بیت سمت راست است.

S^*	61DF870C	4890FE85	D6E3DD87	C3DCE372	3F91DB49
H'	632E21FD	52D2B95C	5F7023DA	63DE9509	C01F6C7B

پیام بازیابی‌شده M^* خالی فرض شده و بنابراین بازیابی پیام کامل است. H''، کد درهم دیگر، نیز با اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی به‌دست می‌آید. طول این رشته ۳۸۴ (۱۶۰+۱۶۰+۶۴) بوده و از کنار هم

قرار دادن ۶۴ بیت از C'، طول پیام قابل بازیابی،۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت S^* تشکیل شده است $H=h(C' \| h(M_2) \| S^*)$.

H'' 632E21FD 52D2B95C 5F7023DA 63DE9509 C01F6C7B

از آن‌جا که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲-۲-۳ مثال طرح امضای ۳

این مثال از تابع درهم‌ساز اختصاصی ۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت SHA-1 نیز شناخته می‌شود.)

ث-۲-۲-۳-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۶۴ نویسه کدگذاری شده ASCII تشکیل شده است.

abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopqopqrpqrs

در مبنای شانزده، پیام M رشته هشت‌تایی زیر با طول ۶۴ هشت‌تایی، یعنی ۵۱۲ بیت است.

M_1 6162636 62636465 6364656 6465666 6566676 6667686 6768696 68696A6
696A6B 6A6B6C6 6B6C6D 6C6D6E 6D6E6F 6E6F70 6F70717 7071727

از آن‌جا که این طرح امضاء از نوع قطعی است، یک مقدار سالت S با طول صفر انتخاب می‌شود.

۱۶۰ بیت کد درهم H به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۳ به رشته دودویی با طول ۷۳۶ (=۱۶۰+۵۱۲+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C طول پیام قابل بازیابی، ۵۱۲ بیت قسمت قابل بازیابی پیام M_1 و ۱۶۰ بیت $h(M_2)$ کد درهم قسمت غیر قابل بازیابی پیام که خالی است تشکیل می‌شود. $H=h(C \| M_1 \| h(M_2))$

H D74009C4 638462E6 9D5923E7 433AEC02 8B9A90E6

یک شناسه در فیلد پشت‌بند T تابع درهم‌سازی که در حال استفاده است را نشان می‌دهد. استاندارد ISO/IEC 10118-3 شناسه تابع درهم‌ساز اختصاص یافته ۳ را برابر با مقدار ۳۳ قرار می‌دهد. بنابراین فیلد پشت‌بند T متشکل از ۱۶ بیت زیر خواهد بود.

T = 33CC

این پیام به اندازه کافی برای بازیابی کامل کوتاه است. ۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۳۵۵ (۱-۱۶-۱۶۰-۵۱۲-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت حاشیه برابر ۱، ۵۱۲ بیت M_1 (M)، ۱۶۰بیت S، ۱۶۰بیت H و ۱۶ بیت فیلد پشت‌بند T تشکیل شده است.

S 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00016162 63646263 64656364 65666465
66676566 67686667 68696768 696A6869 6A6B696 6B6C6A6 6C6D6B6
6D6E6C6 6E6F6D6 6F706E6F 70716F70 71727071 7273D740 09C46384
62E69D59 23E7433 EC028B9 90E633C

رشته قابل بازیابی S_r از اعمال تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴)بیت سمت چپ S_i به‌دست می‌آید. از آن‌جایی که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود.

S	296B062	4010E1	230D456	A5F88F	550AAF	31C805	81E811E	E53E5F7
	AE64FC2	2A486B	3E87972	90C54B	7A862F2	A21919	3ECF067	40A8C8
	41DE8D	F1942C	90D1367	8FFC0D	FB906E7	39C1EC	64C0E06	F0A7443
	6170E411	DF91F7	D1FFD7	09C4638	62E69D5	23E7433	EC028B	90E633C

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. از آن‌جایی که ژاکوبی f_r نسبت به n برابر ۱- می‌شود، $J=f_r/2$ عدد صحیح نمایشگر آن است.

J	14B5831	200870F6	1186A2B	52FC478	AA8557	18E402E	40F408F	F29F2FB
	D7327E	1524358	9F43CB9	C862A5	3D43179	D10C8C	1F67833	2054646
	20EF46	F8CA167	C8689B3	47FE06C	7DC837	9CE0F60	3260703	F853A2
	B0B872	EFC8FB	E8FFEB	04E231C	31734EA	91F3A19	760145C	487319E

J به توان s به پیمانه n افزایش می‌یابد. چون نتیجه کمتر از n/2 است، امضاء $\sum_{=} J^s$ می‌شود.

4F9FE3	21E8EA	786363C	D14D0A	401174B	B94AFB	3E24D01	4CB8CD
075E4D	F4E0809	7DFC3C	3A65457	3178F28	DFF7E1	A9D29B	B18AE2
C483A9	2EF1FB	7BBFA1	269BFA	245C27	E6DF35	CADEE6	74A9737
2145408	91530D	F8AED1	CB95149	28E552	1A61128	2C099D7	442A462

از آن‌جایی که M_2 خالی است، پیام امضاء شده تنها شامل ۱۲۸ هشت‌تایی امضاء است.

ث-۲-۲-۲-۲ فرآیند درستی‌سنجی

امضاء ∑ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. مجذور این عدد صحیح به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	14B5831	200870F6	1186A2B	52FC478	AA8557	18E402E	40F408F	F29F2FB
	D7327E	1524358	9F43CB9	C862A5	3D43179	D10C8C	1F67833	2054646
	20EF46	F8CA167	C8689B3	47FE06C	7DC837	9CE0F60	3260703	F853A2
	B0B872	EFC8FB	E8FFEB	04E231C	31734EA	91F3A19	760145C	487319E

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جا که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۱۱۰ هستند، $f_r'= 2f_s$ خواهد بود.

f_r	296B062	4010E1	230D456	A5F88F	550AAF	31C805	81E811E	E53E5F7
	AE64FC2	2A486B	3E87972	90C54B	7A862F2	A21919	3ECF067	40A8C8
	41DE8D	F1942C	90D1367	8FFC0D	FB906E7	39C1EC	64C0E06	F0A7443
	6170E411	DF91F7	D1FFD7	09C4638	62E69D5	23E7433	EC028B	90E633C

f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. رشته بازیابی‌شده S_i' از اعمال تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' به‌دست می‌آید.

S_i	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00016162	63646263	64656364	65666465
	66676566	67686667	68696768	696A6869	6A6B696	6B6C6A6	6C6D6B6
	6D6E6C6	6E6F6D6	6F706E6F	70716F70	71727071	7273D740	09C46384
	62E69D59	23E7433	EC028B9	90E633C			

S_i' نشان‌دهنده رشته میانی بازیابی شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که δ =۱ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۳۳۵ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت حاشیه نیز مقدار ۱ را به خود می‌گیرد. این ۴۲ هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با CC است. بنابراین پشت‌بند متشکل از دو هشت‌تایی است و مقداری برابر 33CC دارد. این دو هشت‌تایی نیز از سمت راست S_i' حذف می‌شود.

از آن‌جایی که شناسه تابع مقداری برابر با ۳۳ دارد، تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۳ است.

باقی رشته ۶۷۲ بیتی به دو قسمت تقسیم می‌شود.

- M_1^* شامل ۵۱۲ بیت سمت چپ می‌شود.
- H' شامل ۱۶۰ بیت سمت راست می‌شود.

=	6162636	62636465	6364656	6465666	6566676	6667686	6768696	68696A6
	696A6B	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727

H' D74009C4 638462E6 9D5923E7 433AEC02 8B9A90E6

چون بازیابی پیام کامل است، پیام بازیابی‌شده M^* تنها از M_1^* تشکیل شده است. H''، کد درهم دیگر، نیز با اعمال SHA-1 به رشته دودویی به‌دست می‌آید. طول این رشته ۷۳۶ (۶۴+۵۱۲+۱۶۰) بوده و از کنار هم قرار دادن ۶۴ بیت از C' طول پیام بازیابی‌شده، ۵۱۲ بیت M_1^* قسمت پیام دریافتی، ۱۶۰ بیت کد درهم (خالی) قسمت غیر قابل بازیابی پیام ($H''=h(C' \| M_1^* \| h(M_2^*))$.

H'' D74009C4 638462E6 9D5923E7 433AEC02 8B9A90E6

از آن‌جایی که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲-۳ مثال‌هایی با بازیابی جزیی

در این‌جا سه مثال از از تولید امضاء و درستی‌سنجی آن و یک مثال برای هر کدام از سه طرح آورده شده است.

ث-۲-۳-۱ مثال طرح امضای ۱

این مثال از تابع درهم‌ساز اختصاصی۳ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت SHA-1 نیز شناخته می‌شود.)

ث-۲-۳-۱-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۱۱۲ نویسه کدگذاری شده ASCII تشکیل شده است.

abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq
opqrpqrsqrstrstustuvtuvwuvwxvwxywxyzxyzayzabzabcabcdbcde

در مبنای شانزده، پیام M رشته هشت‌تایی زیر با طول ۱۱۲ هشت‌تایی، یعنی ۸۹۶ بیت است.

```
M  6162636  62636465  63646566  6465666  6566676  6667686  6768696  68696A6
   696A6B6  6A6B6C6  6B6C6D  6C6D6E  6D6E6F  6E6F70  6F70717  7071727
   7172737  72737475  73747576  7475767  7576777  7677787  7778797  78797A
   797A616  7A61626  61626364  6263646
```

۱۶۰ بیت کد درهم از اعمال SHA-1 به ۸۹۶ بیت M محاسبه می‌شود.

H = 1CF7A997 4518E555 C1802CB8 10A23C27 4FCFAA73

یک شناسه در فیلد پشت‌بند تابع درهم‌سازی که در حال استفاده است را نشان می‌دهد. استاندارد ISO/IEC 10118-3 شناسه تابع درهم‌ساز اختصاص یافته ۳ را برابر با مقدار ۳۳ قرار می‌دهد. بنابراین فیلد پشت‌بند T متشکل از ۱۶ بیت زیر خواهد بود.

T = 33CC

در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طورکلی قابل بازیابی باشد. بنابراین آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۸۴۰ بیت سمت چپ.
- M_2 متشکل است از ۵۶ بیت باقیمانده یعنی ۷ هشت‌تایی.

```
M  6162636  62636465  63646566  6465666  6566676  6667686  6768696  68696A6
   696A6B6  6A6B6C6  6B6C6D  6C6D6E  6D6E6F  6E6F70  6F70717  7071727
   7172737  72737475  73747576  7475767  7576777  7677787  7778797   78797A
   797A616  7A61626  61
```

M_2 626364 62636465

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن دو بیت سرآیند با مقدار ۰۱، بیت بیشتر داده برابر با ۱ ، چهار (۴-۱۶-۱۶۰-۸۴۰-۱۰۲۴) بیت لایه‌گذاری برابر با 0 ، بیت مرزی برابر ۱، ۸۴۰ بیت M_1 ، ۱۶۰بیت H و ۱۶ بیت فیلد پشت‌بند T تشکیل شده‌است. رشته قابل بازیابی S_r از جایگزینی نیبل مرزی که برابر با ۱ است با نیبلی برابر با A منتج می‌شود.

```
S  6A61626  6462636  65636465  6664656  6765666  6866676  6967686  6A68696
```

6B696A	6C6A6B	6D6B6C	6E6C6D	6F6D6E	706E6F7	716F707	72707172
7371727	7472737	75737475	7674757	7775767	7876777	7977787	7A78797
61797A6	627A616	63611CF	A997451	E555C1	2CB810	3C274F	AA7333

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. از آن‌جایی که ژاکوبی f_r نسبت به n برابر ۱- می‌شود، $J=f_r/2$ عدد صحیح نمایشگر آن است.

J	3530B13	B23131	32B1B23	B33232B	33B2B33	B43333B	34B3B43	B53434B
	35B4B5	B63535	36B5B63	B73636B	37B6B73	B83737B	38B7B83	B93838B
	39B8B9	BA3939	3AB9BA	BB3A3A	3BBABB	BC3B3B	3CBBBC	BD3C3C
	30BCB	B13D30	31B08E7	D4CBA2	72AAE0	165C085	1E13A7	D53999E

J به توان s به پیمانه n افزایش می‌یابد و نتیجه به‌صورت زیر خواهد بود.

AD8302	FB27EC	E5F8FD	8E10481	35CB879F	62BC218	A17D84	9C65FF9
728DEA	6848885	AC9986	0B93704	2FF8C5E	33DA98	E75D54	59CC12
E9AF94	80E3154	A96FD2	4B1AD9	0032373A	208D496	0870EEB	A771F3
74B0838	95F0B1	F0CE526	679B161	A1BCAA	45AE466	421339D	6398C11

نتیجه فوق بزرگتر از n/2 بوده و در نتیجه امضاء به‌صورت $\sum = n - J^s$ خواهد بود.

0F682C1	32F4A28	B3C398	6AE8D5	D2831F4	649FB00	2F5039F	85742A6
2BE5266	35684936	04F87B	9C7EFB	FD1AE5	657DDD	F332253	08FB24
775A3E	C9BFCA	0A13D4	73FD26	1425297	6ACB74	F8543CF	1593B6
49AB21	50816E9	159EE5	34555C	D9EF07	B1044FC	C22A7A	0C04606

پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۷ هشت‌تایی از قسمت غیر قابل بازیابی M_2تنها ۲۳ هشت‌تایی از پیام M بیشتر است.

ث-۲-۳-۱-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح مجذور و به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	3530B13	B23131	32B1B23	B33232B	33B2B33	B43333B	34B3B43	B53434B
	35B4B5	B63535	36B5B63	B73636B	37B6B73	B83737B	38B7B83	B93838B
	39B8B9	BA3939	3AB9BA	BB3A3A	3BBABB	BC3B3B	3CBBBC	BD3C3C
	30BCB	B13D30	31B08E7	D4CBA2	72AAE0	165C085	1E13A7	D53999E

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جایی که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۱۱۰ هستند، $f_r' = 2f_s$ خواهد بود.

f_r	6A61626	6462636	65636465	6664656	6765666	6866676	6967686	6A68696
	6B696A	6C6A6B	6D6B6C	6E6C6D	6F6D6E	706E6F7	716F707	72707172
	7371727	7472737	75737475	7674757	7775767	7876777	7977787	7A78797
	61797A6	627A616	63611CF	A997451	E555C1	2CB810	3C274F	AA7333

f_r' یک عدد صحیح مثبت بدون علامت است که توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود.

- هشت‌تایی سمت چپ S_r' برابر با 6A است. این هشت‌تایی شامل سرآیند برابر با ۰۱، بیت بیشتر- داده برابر با ۱ (بازیابی جزیی)، یک بیت لایه‌گذاری برابر با 0 و یک نیبل مرزی برابر با A است. این هشت‌تایی از سمت چپ S_r' حذف می‌شود.
- هشت‌تایی سمت راست S_r' برابر با CC است. بنابراین پشت‌بند متشکل است از دو هشت‌تایی و برابر است با 33CC. این هشت‌تایی نیز از سمت راست S_r' حذف می‌شود.

شناسه تابع درهم‌ساز برابر ۳۳ است؛ بنابراین تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۳ است.

رشته ۱۰۰۰ بیتی باقی‌مانده نیز به دو قسمت تقسیم می‌شود:

- M_1^* متشکل است از ۸۴۰ بیت سمت چپ
- H' متشکل است از ۱۶۰ بیت سمت راست

M_1	6162636	62636465	6364656	6465666	6566676	6667686	6768696	68696A6
	696A6B	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	7374757	7475767	7576777	7677787	7778797	78797A
	797A616	7A61626	61					

H'	1CF7A997	4518E555	C1802CB8	10A23C27	4FCFAA73

از آن‌جا که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^*، قسمت بازیابی‌شده، و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

M_1	6162636	62636465	6364656	6465666	6566676	6667686	6768696	68696A6
	696A6B	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	7374757	7475767	7576777	7677787	7778797	78797A
	797A616	7A61626	6162636	6263646				

H'' (دیگر تابع درهم‌ساز) از اعمال تابع درهم‌ساز اختصاصی ۳ به M^* پیام بازیابی‌شده به‌دست می‌آید.

H''	1CF7A997	4518E555	C1802CB8	10A23C27	4FCFAA73

از آن‌جایی که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲-۳-۲ مثال طرح امضای ۳

این مثال از تابع درهم‌ساز اختصاصی ۱ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت RIPEMD-160 نیز شناخته می‌شود.)

ث-۲-۳-۲-۱ فرآیند امضاء

این مثال نمایانگر امضای پیامی به طول ۱۳۲ هشت‌تایی یا همان۱۰۵۶ بیت است.

M	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432

FEDCBA

۱۶۰ بیت سالت S تولید می‌شوند.

S = 78E29320 3CBA1B7F 92F05F4D 171FF8CA 3E738FF8

در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طورکلی قابل بازیابی باشد. بنابراین، آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۶۸۰ بیت سمت چپ.
- M_2 متشکل است از ۳۷۶ بیت یا همان ۴۷ هشت‌تایی باقی‌مانده.

M FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 76

M FEDCBA 765432
FEDCBA 765432 FEDCBA 765432 FEDCBA 765432 FEDCBA 765432
FEDCBA

۱۶۰ بیت کد درهم به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی با طول ۱۰۶۴ (۱۶۰+۱۶۰+۶۸۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C، طول پیام قابل بازیابی، ۶۸۰ بیت قسمت قابل بازیابی پیام M_1، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام $h(M_2)$ و ۱۶۰ بیت سالت S تشکیل شده است. $H=h(C \parallel M_1 \parallel h(M_2) \parallel S)$

H = A4B517F2 E820B81F 26BCE7C6 6F48A2DB 12A8F3D7

یک شناسه در فیلد پشت‌بند T تابع درهم‌سازی که در حال استفاده است را نشان می‌دهد. استاندارد ISO/IEC 10118-3 شناسه تابع درهم‌ساز اختصاص یافته ۱ را برابر با مقدار ۳۱ قرار می‌دهد. بنابراین، فیلد پشت‌بند T متشکل از ۱۶ بیت زیر خواهد بود.

T = 31CC

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۷ (۱-۱۶-۱۶۰-۱۶۰-۶۸۰-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت مرزی برابر ۱، ۶۸۰ بیت M_1، ۱۶۰بیت L، ۱۶۰ بیت H و ۱۶ بیت فیلد پشت‌بند T تشکیل شده است.

S 01FEDC 9876543 10FEDC 987654 10FEDC 9876543 10FEDC 9876543
10FEDC 9876543 10FEDC 987654 10FEDC 9876543 10FEDC 9876543
10FEDC 9876543 10FEDC 987654 10FEDC 987678 93203CB 1B7F92F
5F4D171 F8CA3E 8FF8A4B 17F2E8 B81F26B E7C66F A2DB12 F3D731

رشته بازیابی‌شده S_r از اعمال تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. از آن‌جایی که δ = ۱ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود.

S 01402B2 ABA104 9677CE C3D5A8 B24494D F9508B4 96484F5 3CC7E8
CC4DDE 81F21C 9D4F94 D2CCCB FCEDA0 8FFD4E EAE72C EB4A26
F0A34A0 49664C DB7233 759D758 36C8BA AC4348 6958AC9 AE0B5A

195B57A FB9971 1337A4 17F2E82 B81F26B E7C66F A2DB12 F3D731

عدد صحیح قابل بازیابی f_r یک عدد صحیح مثبت بدون علامت است که توسط S_r نشان داده می‌شود. از آن‌جایی که ژاکوبی f_r نسبت به n برابر ۱- می‌شود، $J=f_r/2$ عدد صحیح نمایشگر آن است.

J 00A0159 D5D082 CB3BE7 E1EAD42 D9224A 7CA845 CB2427 9E63F45
E626EF3 40F90E5 4EA7CA 696665A FE76D0 47FEA7 7573967 F5A513
7851A50 24B3266 EDB919 BACEBA 1B645D 5621A4 34AC56 5705AD
8CADAB FDCCB8 099BD25 8BF9741 5C0F93 73E337 516D895 79EB98

J به توان s به پیمانه n افزایش می‌یابد و نتیجه به‌صورت زیر خواهد بود.

= 66313F1 BCE72A 7D3235 DAF0D5 3915C83 D12F5C DFC76A 557D27F
B41CF2 94EB610 6E029B C4F91C2 D687FA 26BA47 05AD83 FE5CF98
EF6B1B 282460B 77A8C1 2628F25 519EF21 E2C1EB 019CE73 747F435
6DB21E 28A96A 76289A 99D3225 4167D93 5C3F3D 84AE87 2AA23A

نتیجه فوق بزرگتر از n/2 بوده و در نتیجه امضاء به‌صورت $\sum = n - J^s$ خواهد بود.

56B9EF 713563C 1C8A60 1E0848 CF38DE F62C754 F106548 CC5D01
EA561E 08C5708 438F65B E3194F 568BB0E 729E2E4 D4E1F6 646A3E
719EB73 227E7F8 3BDAE6 98EF0D C2B86E8 A896D3 FF28446 4886667
50A986 BDC8B5 90449CF 021D50 3A43D93 9A7358 7F8F2C 44FAE7

پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۴۷ هشت‌تایی از پیام غیر قابل بازیابی M_nتنها ۴۳ هشت‌تایی از پیام M بیشتر است.

ث-۲-۳-۱-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح مجذور شده و به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f BC4B19 584C0C CE80AE 170E497 2F2C5C7 4AB38B 05A9972 8376359
B84C21 5CB7C3 62EA371 3EAC05 2E9CDB 5159CEC 651BE37 6D2224
E8B82D 25EFB9 C5CA8D 0449450 F8F3039 353719E CC18D5 65FFFC
31ADF9 E8A566 FCD1654 0FF6FE 1F9C1F0 82CF5E8 B2D02B F5B188

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جایی که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۱۱۱ هستند، $f_r' = 2(n - f_s)$ خواهد بود.

f 01402B2 ABA104 9677CE C3D5A8 B24494D F9508B4 96484F5 3CC7E8
CC4DDE 81F21C 9D4F94 D2CCCB FCEDA0 8FFD4E EAE72C EB4A26
F0A34A0 49664C DB7233 759D758 36C8BA AC4348 6958AC9 AE0B5A
195B57A FB9971 1337A4 17F2E82 B81F26B E7C66F A2DB12 F3D731

f_r' به‌صورت یک عدد صحیح مثبت بدون علامت توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. تابع تولید ماسک MGF1 به ۸۴۸ (۱۶-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' اعمال شده و S_i' رشته میانی بازیابی‌شده را نتیجه می‌دهد.

S_i	01FEDC	9876543	10FEDC	987654	10FEDC	9876543	10FEDC	9876543
	10FEDC	9876543	10FEDC	987654	10FEDC	9876543	10FEDC	9876543
	10FEDC	9876543	10FEDC	987654	10FEDC	987678	93203CB	1B7F92F
	5F4D171	F8CA3E	8FF8A4B	17F2E8	B81F26B	E7C66F	A2DB12	F3D731

S_i' نشان‌دهنده رشته میانی بازیابی شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که ۱= δ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۷ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت مرزی نیز مقدار ۱ را به خود می‌گیرد. این هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با CC است. بنابراین پشت‌بند متشکل از دو هشت‌تایی است و مقداری برابر 31CC دارد. این دو هشت‌تایی نیز از سمت راست S_i' حذف می‌شود.

از آن‌جایی که شناسه تابع مقداری برابر با ۳۱ دارد، تابع درهم‌ساز درحال استفاده تابع درهم‌ساز اختصاصی ۱ است.

باقی رشته ۱۰۰۰ بیتی به سه قسمت تقسیم می‌شود.

- M_1^* شامل ۶۸۰ بیت سمت چپ می‌شود.
- S^* شامل ۱۶۰ بیت سمت راست می‌شود.
- H' شامل ۱۶۰ بیت سمت راست می‌شود.

$_1^*$=	FEDCB	7654321	FEDCB	7654321	FEDCB	7654321	FEDCB	7654321
	FEDCB	7654321	FEDCB	7654321	FEDCB	7654321	FEDCB	7654321
	FEDCB	7654321	FEDCB	7654321	FEDCB	76		

S^* 78E29320 3CBA1B7F 92F05F4D 171FF8CA 3E738FF8

H' A4B517F2 E820B81F 26BCE7C6 6F48A2DB 12A8F3D7

از آن‌جایی که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^* قسمت بازیابی‌شده و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

M	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432	FEDCBA	765432
	FEDCBA							

H''، کد درهم دیگر، نیز به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی با طول ۱۰۶۴ (۱۶۰+۱۶۰+۶۸۰+۶۴) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C طول پیام بازیابی‌شده، ۶۸۰

بیت قسمت بازیابی‌شده پیام M_1^* ، ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام ($h(M_2^*)$ و ۱۶۰ بیت سالت بازیابی شده S^* تشکیل شده است. ($H''=h(C \parallel M_1^* \; h(M_2) \parallel S^*)$.

H'' A4B517F2 E820B81F 26BCE7C6 6F48A2DB 12A8F3D7

از آن‌جایی که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

ث-۲-۳-۳ مثال طرح امضای ۳

این مثال از تابع درهم‌ساز اختصاصی ۱ از استاندارد ISO/IEC 10118-3 استفاده می‌کند. (به‌صورت RIPEMD-160 نیز شناخته می‌شود.)

ث-۲-۳-۳-۱ فرآیند امضاء

رشته زیر پیام مورد نظر برای امضاء است که از ۱۱۲ نویسه کدگذاری شده ASCII تشکیل شده است.

abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq
opqrpqrsqrstrstustuvtuvwuvwxvwxywxyzxyzayzabzabcabcdbcde

در مبنای شانزده، پیام M رشته هشت‌تایی زیر با طول ۱۱۲ هشت‌تایی، یعنی ۸۹۶ بیت است.

M	6162636	62636465	63646566	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	73747576	7475767	7576777	7677787	7778797	78797A
	797A616	7A61626	61626364	6263646				

از آن‌جایی که این طرح امضاء از نوع قطعی است، یک مقدار سالت S با طول صفر انتخاب می‌شود.

در این حالت پیام بزرگتر از آن است که توسط فرآیند درستی‌سنجی به‌طورکلی قابل بازیابی باشد. بنابراین آن‌را به دو قسمت تقسیم می‌کنیم:

- M_1 متشکل است از ۸۴۸ بیت سمت چپ.
- M_2 متشکل است از ۴۸ بیت یا همان ۶ هشت‌تایی باقی‌مانده.

M	6162636	62636465	63646566	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	73747576	7475767	7576777	7677787	7778797	78797A
	797A616	7A61626	6162					

M_2 6364 62636465

۱۶۰ بیت کد درهم H به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی با طول ۱۰۷۲ (۶۴+۸۴۸+۱۶۰) محاسبه می‌گردد. این رشته از کنار هم قرار دادن ۶۴ بیت C، طول پیام قابل بازیابی، ۸۴۸ بیت قسمت قابل بازیابی پیام M_1 و ۱۶۰ بیت کد درهم قسمت غیر قابل بازیابی پیام ($H=h(C \parallel M_1 \parallel h(M_2))$

H = 15F000AC 58EE3FFF 144845E7 71907C0C 83324A6F

تابع درهم‌ساز در حال استفاده به‌طور ضمنی معلوم است. بنابراین، فیلد پشت‌بند T متشکل از ۸ بیت زیر خواهد بود.

$T = BC$

۱۰۲۴ بیت رشته میانی S_i از کنار هم قرار دادن ۷ (۱-۸-۱۶۰-۸۴۸-۱۰۲۴) بیت لایه‌گذاری برابر با 0، بیت مرزی برابر ۱، ۸۴۸ بیت M_r، قسمت قابل بازیابی پیام، ۱۶۰بیت H و ۸ بیت فیلد پشت‌بند T تشکیل شده است.

S	0161626	64626364	65636465	6664656	6765666	6866676	6967686	6A68696
	6B696A6	6C6A6B6	6D6B6C6	6E6C6D	6F6D6E	706E6F	716F707	7270717
	7371727	74727374	75737475	7674757	7775767	7876777	7977787	7A78797
	61797A6	627A616	63616215	F000AC5	EE3FFF	4845E7	907C0C	324A6FB

رشته بازیابی‌شده S_r از اعمال تابع تولید ماسکMGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_i به‌دست می‌آید. از آن‌جایی که $\delta = ۱$ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_r نیز برابر 0 قرار داده می‌شود.

S	6F2BB97	71FE2EF	05B6600	E9DD06	6655C19	7F374E	66D6365	6A5FEE
	AF64555	B25F455	7C4EE53	1F96FE	6508C90	9E3F11	6E8D49	39ED3E5
	ECE4286	A6FB3A	17DAFB	3019D93	1D382D	7264FE	D9797D	0B77793
	7CA7E7	E440D88	5B7DDF	F000AC	EE3FFF1	4845E77	907C0C	324A6F

عدد صحیح قابل بازیابی f_r عدد صحیح مثبت بدون علامت نمایش داده شده توسط S_r است. از آن‌جایی که ژاکوبی f_r نسبت به n برابر ۱ است، نتیجه حفظ می‌شود. f_r با توان s به پیمانه‌ی n افزایش داده شده است. نتیجه حاصله توسط عدد صحیح مثبت بدون علامت موقت t نمایش داده شده‌است.

t	A1B2C6	971FD3	83DE75	6A69EA	262F2A0	DB41B5	E048DEB	15DDCA
	37A04E1	87372B	740CE25	3EF1EE	F68D478	819F797	DA8AD7	F4D7EB
	C7CE09	937FC7	452BAB	56C9DE	CEE7C8	C285AA	09674464	BDD470
	F37BC8	753C7E	9D76EB	522F7FB	6ABCC2	591DF88	33B736C	8269091

از آن‌جایی که نتیجه فوق بزرگتر از n/2 است، آن‌را با مکملش نسبت به n جای‌گذاری می‌کنیم. رشته دودویی نمایش‌دهنده آن عدد صحیح که به‌صورت یک عدد صحیح مثبت بدون علامت است امضای $\sum = n - t$ است.

1B38688	96FCBA	15DE20	8E8F33	E21F7C	EC1A1B	F084E02	0BFC5F
66D2C30	1679A61	3D851F	69207C	3686642	17B8FC	0004A24	6DEF4C
993BC91	B72318D	6E57FB	684E21	456F984	C8D313	F75DE7	FF31394
CADFDC	7135A13	68F64C	49C0F3	10EEEF	9D949D	D0867D	ED3418

پیام امضاء شده شامل ۱۲۸ هشت‌تایی امضاء $\sum$ است که همراه با ۶ هشت‌تایی از پیام غیر قابل بازیابی M_2 تنها ۲۲ هشت‌تایی از پیام M بیشتر است.

ث-۲-۳-۳-۲ فرآیند درستی‌سنجی

امضاء $\sum$ یک رشته دودویی نمایش‌دهنده یک عدد صحیح بدون علامت کمتر از n/2 است. این عدد صحیح مجذور شده و به پیمانه n می‌رسد و عدد صحیح f_s را نتیجه می‌دهد.

f	6F2BB97	71FE2EF	05B6600	E9DD06	6655C19	7F374E8	66D6365	6A5FEE
	AF64555	B25F455	7C4EE53	1F96FE	6508C90	9E3F11	6E8D49	39ED3E
	ECE4286	A6FB3A	17DAFB	3019D93	1D382D	7264FE9	D9797D	0B77793
	7CA7E7	E440D88	5B7DDF	F000AC	EE3FFF1	4845E77	907C0C	324A6F

فرآیند درستی‌سنجی شامل ژاکوبی نمی‌شود. از آن‌جایی که سه بیت کم ارزش f_s، عدد صحیح حاصله، برابر با ۱۰۰ هستند، $f_r' = f_s$ خواهد بود.

f_r' به‌صورت یک عدد صحیح مثبت بدون علامت توسط رشته بازیابی‌شده S_r' نمایش داده می‌شود. تابع تولید ماسک MGF1 به ۸۵۶ (۸-۱۶۰-۱۰۲۴) بیت سمت چپ S_r' اعمال شده و S_i' رشته میانی بازیابی‌شده را نتیجه می‌دهد.

S_i	0161626	64626364	65636465	6664656	6765666	6866676	6967686	6A68696
	6B696A	6C6A6B	6D6B6C6	6E6C6D	6F6D6E	706E6F	716F707	7270717
	7371727	74727374	75737475	7674757	7775767	7876777	7977787	7A78797
	61797A6	627A616	63616215	F000AC	EE3FFF	4845E7	907C0C	324A6F

S_i' نشان‌دهنده رشته میانی بازیابی‌شده است که به‌شرح زیر به‌دست می‌آید:

- از آن‌جایی که $\delta = 1$ ((۱۰۲۴-۱) به پیمانه ۸) است، چپ‌ترین بیت S_i' برابر 0 قرار داده می‌شود. ۷ بیت سمت چپ رشته دودویی حاصله برابر 0 قرار داده شده و بیت مرزی نیز مقدار ۱ را به خود می‌گیرد. این هشت‌تایی از سمت چپ S_i' حذف می‌شوند.
- سمت راست‌ترین هشت‌تایی S_i' برابر با BC است. این هشت‌تایی نیز از سمت راست S_i' حذف می‌شود.

از آن‌جا که پشت‌بند برابر BC است، تابع درهم‌ساز درحال استفاده به‌طور ضمنی معلوم است که در این مثال همان RIPEMD-160 است.

باقی رشته ۱۰۰۸ بیتی به دو قسمت تقسیم می‌شود.

- M_1^* شامل ۸۴۸ بیت سمت چپ می‌شود.
- H' شامل ۱۶۰ بیت سمت راست می‌شود.

=	6162636	62636465	6364656	6465666	6566676	6667686	6768696	68696A6
	696A6B	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	7374757	7475767	7576777	7677787	7778797	78797A6
	797A616	7A61626	6162					

$H' =$ 15F000AC 58EE3FFF 144845E7 71907C0C 83324A6F

از آن‌جایی که بازیابی جزیی است، پیام بازیابی‌شده M^* از کنارهم نهادن M_1^* قسمت بازیابی‌شده و M_2^* قسمت غیر قابل بازیابی تشکیل می‌شود.

=	6162636	62636465	6364656	6465666	6566676	6667686	6768696	68696A6
	696A6B6	6A6B6C6	6B6C6D	6C6D6E	6D6E6F	6E6F70	6F70717	7071727
	7172737	72737475	7374757	7475767	7576777	7677787	7778797	78797A6
	797A616	7A61626	6162636	6263646				

H''، کد درهم دیگر، نیز به‌وسیله اعمال تابع درهم‌ساز اختصاصی ۱ به رشته دودویی با طول ۱۰۷۲ (۶۴+۸۴۸+۱۶۰) محاسبه می‌شود. این رشته از کنار هم قرار دادن ۶۴ بیت C' طول پیام بازیابی‌شده، ۸۴۸ بیت قسمت بازیـابی‌شده پیـام M_1^* ، ۱۶۰ بیت کد درهم قسمت غیـر قابل بازیابی پیام ($h(M_2^*)$ تشکیل شـده است. $H''=h(C' \| M_1^* \| h(M_2))$.

H'' 15F000AC 58EE3FFF 144845E7 71907C0C 83324A6F

از آن‌جایی که هر دو کد درهم H' و H'' یکسان هستند، امضاء $\sum$ مورد پذیرش قرار خواهد گرفت.

کتاب‌نامه

[1] M. Bellare and P. Rogaway, ‘Random oracles are practical: a paradigm for designing efficient Protocols, In Proceedings of the first annual conferen ce on Computer and Communications Security, ACM, 1993, pp.62-73

[2] M. Bellare and P. Rogaway, ‘Optimal asymmetric encryption – how to encrypt with RSA’. In: A. De Santis (editor), Advances in Cryptology – Eurocrypt ’94, Lecture Notes in Computer Science 950 (1995), Springer-Verlag, pp.92-111

[3] M. Bellare and P. Rogaway, ‘the exact security of digital signatures: How to sign with RSA and Rabin’. In: U.M. Maurer (editor), Advances in Cryptology – Eurocrypt ’96 , Lecture Notes in Computer Science 1070 (1996), Springer-Verlag, pp.399-416

[4] J.-S. Coron, ‘On the exact security of full domain hashing’. In: M. Bellare (editor), Advances in Cryptology – Crypto 2000, Lecture Notes in Computer Science 1880 (2000), Springer-Verlag, pp.229-235

[5] J.-S. Coron, D. Naccache, and J.P. Stern, ‘On the security of RSA padding’. In: M.J. Wiener (editor), Advances in Cryptology – Crypto ’99, Lecture Notes in Computer Science 1666 (1999), Springer-Verlag, pp.1-18

[6] J.-S. Coron, D. Naccache, M. Tibouchi, and R.-P. Weinmann. ‘Pract ical Cryptanalysis of ISO 9796-2 and Europay-Mastercard-Visa Signatures’. In: S. Halevi (editor), Advances in Cryptology – Crypto 2009, Lecture Notes in Computer Science 5677 (2009), Springer-Verlag, pp.428-444

[7] M. Girault and J.-F. Misarsky, ‘Cryptanalysis of countermeasures proposed for repairing ISO 9796-1’. In: B. Preneel (editor), Advances in Cryptology – Eurocrypt 2000, Lecture Notes in Computer Science 1807 (2000), Springer-Verlag, pp.81-90

[8] F. Grieu, ‘A chosen messages attack on the IS O/IEC 9796-1 signature scheme’. In: B. Preneel (editor), Advances in Cryptology – Eurocrypt 2000, Lecture Notes in Computer Science 1807 (2000), Springer-Verlag, pp.70-80

[9] IEEE Std 1363-2000, Standard specifications for public key cryptography

[10] IEEE Std 1363a-2004, Standard specifications for public key cryptography — Amendment 1: Additional techniques

[۱۱] استاندارد ملی ۳-۹۷۹۶: سال۱۳۸۸، فناوری اطلاعات- فنون امنیتی- طرح‌های امضای دیجیتال با قابلیت بازیابی پیام- قسمت سوم: سازوکارهای مبتنی بر لگاریتم گسسته

[12] ISO/IEC 9797-2:2002, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function

[13] ISO/IEC 9798-1:1997), Information technology — Security techniques — Entity authentication — Part 1: General

[۱۴] استاندارد ملی ۱-۱۱۴۹۴: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیت- امضاءهای دیجیتال با پیوست- قسمت ۱- کلیات

[15] J. Jonsson, ‘Securit y proofs for the RSA-PSS signat ure scheme and its variants’. Proceedings of the 2nd NESSIE Workshop, Royal Holloway, University of London, September 2001. Full version available in IACR cryptology archive 2001/053

[16] B. Kaliski, ‘On hash function firewalls in signature schemes’. In: B. Preneel (editor), Cryptographers' Track RSA Conference 2002, Lecture Notes in Computer Science 2271 (2002), Sprin