INSO
17914-2
1st. Edition
2014

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

استاندارد ملی ایران

۱۷۹۱۴-۲
چاپ اول
۱۳۹۳

فناوری اطلاعات - فنون امنیتی – کدهای اصالت‌سنجی پیام (MACs) قسمت ۲: سازوکارهای استفاده کننده از تابع درهم‌ساز اختصاصی

Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function

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 - کدهای اصالت‌سنجی پیام (MACs) قسمت۲: سازوکارهای استفاده کننده تابع درهم‌ساز اختصاصی»

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سراج زاده، هادی (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا
(فوق لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی - کدهای اصالت‌سنجی پیام (MACs) قسمت ۲: سازوکارهای استفاده کننده تابع درهم‌ساز اختصاصی » که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و چهارمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۳ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه 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 تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 9797-2:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function

فناوری اطلاعات - فنون امنیتی - کدهای اصالت‌سنجی پیام (MACs)[1] - قسمت ۲: سازوکارهای استفاده کننده تابع درهم‌ساز اختصاصی[2]

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین سه الگوریتم MAC است که با استفاده از یک کلید پنهان و یک تابع درهم‌ساز (یا تابع گردکننده[3] آن) با یک نتیجه n بیتی، یک MAC با طول m بیت را محاسبه می‌کند. این سازوکارها می‌توانند به عنوان سازوکارهای یکپارچگی داده‌ای، جهت درستی‌سنجی این که داده‌ها به روشی غیر مجاز تغییر نیافته‌اند، به کار روند. همچنین برای تضمین این که پیام از هستاری سرچشمه گرفته که کلید پنهان را در اختیار خود دارد، می‌توانند به عنوان سازوکارهای اصالت‌سنجی پیام به کار روند. قدرت سازوکارهای یکپارچگی داده و اصالت‌سنجی پیام به آنتروپی[4] و پنهان بودن کلید، به طول هر کد درهم‌ساز تولید شده توسط تابع درهم‌ساز (n بر حسب بیت)، به قدرت تابع درهم‌ساز، به طول MAC (m بر حسب بیت) و به سازوکار خاص بستگی دارد.

سه سازوکار مشخص شده در این استاندارد بر اساس تابع درهم‌ساز اختصاصی مشخص شده در استاندارد ISO/IEC 10118-3[5] است. سازوکار اول به طور معمول با عنوان MDx-MAC شناخته می‌شود. این سازوکار، تابع درهم‌ساز را یک بار فراخوانی می‌کند، ولی با اضافه کردن یک کلید به ثابت های جمعی[6] در تابع گردکننده، تعدیل کوچکی در تابع گردکننده در تابع درهم‌ساز به وجود می آورد. سازوکار دوم به طور معمول با عنوان HMAC شناخته می‌شود. این سازوکار، تابع درهم‌ساز را دو بار فراخوانی می‌کند. سازوکار سوم نوع دیگری از MDx-MAC است که تنها رشته‌های کوتاه (بیشینه۲۵۶ بیت) را به عنوان ورودی می‌گیرد. این سازوکار برای برنامه‌های کاربردی که با رشته‌های داده ورودی کوتاه کار می‌کنند، کارایی‌های بالاتری ارائه می‌دهد.

این استاندارد می‌تواند در خدمات امنیتی هر معماری، فرآیند یا برنامه کاربردی امنیتی به کار برده شود.

یادآوری- چارچوبی کلی برای تامین خدمات یکپارچگی در استاندارد ISO/IEC 10181-6[7] مشخص شده است.

---

1 - Message Authentication Codes
2 - Dedicated hash-function
3 - Round-function
4 - Entropy
۵ - استاندارد بین‌المللی ISO/IEC 10118-3:2004 در سال ۱۳۹۱ با شماره ملی ۹۵۹۸-۳ منتشر شده است.
6 - Additive constants
۷ - استاندارد بین‌المللی ISO/IEC 10181-6:1996 در سال ۱۳۸۸ با شماره ملی ۱۰۱۸۱-۶ منتشر شده است.

۲ مراجع الزامی

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

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 10118-3:2004, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-function

2-2 ISO/IEC 10118-3:2004/Amd.1:2006, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions — Amendment 1: Dedicated Hash-Function 8 (SHA-224)

۳ اصطلاحات وتعاریف

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

۳-۱
بستک[1]

رشته بیتی با طول L_1، یعنی طول اولین ورودی به تابع گرد کننده است.

[ISO/IEC 10118-3]

۳-۲
تابع درهم‌ساز مقاوم در برابر برخورد[2]

تابع درهم‌ساز که دارای خاصیت زیر است:

- یافتن هر دو ورودی مجزایی که به خروجی یکسان نگاشت شود، از نظر محاسباتی غیر ممکن است.

[ISO/IEC 10118-1][3]

1 - Block

2 - Collision-resistant hash-function

۳ - استاندارد بین‌المللی ISO/IEC 10118-1:2000 در سال ۱۳۸۶ با شماره ملی ۹۵۹۸-۱ منتشر شده است.

۳-۳
انتروپی
مجموع کل اطلاعات حاصل شده توسط مجموعه‌ای از بیت‌ها است که نشان دهنده تلاش کاری مورد نیاز برای یک رقیب است تا قادر به بازتولید همان مجموعه از بیت‌ها باشد.

[ISO/IEC 18032][1]

۴-۳
رشته داده ورودی[2]
رشته‌ای از بیت‌ها که ورودی تابع درهم‌ساز است.

۵-۳
کد درهم‌ساز [3]
رشته‌ای از بیت‌ها که خروجی تابع درهم‌ساز است.

[ISO/IEC 10118-1]

۶-۳
تابع درهم‌ساز [4]
تابعی که رشته‌هایی از بیت‌ها را به رشته‌های با طول ثابت از بیت‌ها نگاشت می‌کند و دارای خصوصیات زیر است:

- برای خروجی داده شده، یافتن یک ورودی که به این خروجی نگاشت شود، از نظر محاسباتی غیر ممکن است.

- برای ورودی داده شده، یافتن یک ورودی دوم که به این خروجی نگاشت شود، از نظر محاسباتی غیر ممکن است.

[ISO/IEC 10118-1]

۷-۳
مقدار اولیه[5]
مقدار مورد استفاده در تعریف نقطه شروع تابع درهم‌ساز است.

[ISO/IEC 10118-1]

---

۱ - استاندارد بین‌المللی ISO/IEC 18032:2005 در سال ۱۳۸۷ با شماره ملی ۱۰۸۲۳ منتشر شده است.

2 - Input data string
3 - Hash-code
4 - Hash-function
5 - Initializing value

۸-۳
کلید الگوریتم MAC[1]
کلیدی که عملکرد الگوریتم MAC را کنترل می‌کند.

[ISO/IEC 9797-1][2]

۹-۳
کد اصالت‌سنجی پیام(MAC) [3]
رشته‌ای از بیت‌ها که خروجی الگوریتم MAC است.

یادآوری- یک MAC گاهی اوقات مقدار وارسی رمزنگاشتی[4] نامیده می‌شود (برای مثال به ISO 7498-2[5] مراجعه شود).

[ISO/IEC 9797-1]

۱۰-۳
الگوریتم کد اصالت‌سنجی پیام(MAC) [6]
الگوریتم برای محاسبه تابعی که رشته‌هایی از بیت‌ها و یک کلید پنهان را به رشته‌های بیتی با طول ثابت نگاشت می‌کند، و دارای دو خصوصیت زیر است:

- برای هر کلید و هر رشته ورودی، تابع می‌تواند به طور موثری محاسبه گردد.

- برای هر کلید ثابتی، بدون داشتن دانش قبلی در مورد کلید، محاسبه مقدار تابع در هر رشته ورودی جدید از نظر محاسباتی ممکن نیست، حتی با داشتن اطلاعات در مورد مجموعه رشته‌های ورودی و مقادیر تابع مربوطه، به طوری که ممکن است مقدار رشته ورودی i ام بعد از مشاهده مقدار i-1 مقادیر تابع اولیه، انتخاب شده باشد (برای عدد صحیح $i>1$)

یادآوری ۱- الگوریتم MAC گاهی اوقات تابع وارسی رمزنگاشتی نامیده می‌شود (برای مثال به ISO 7498-2 [۱] مراجعه شود).

یادآوری ۲- محاسبات قابل اجرا به نیازهای امنیتی مشخص شده و شرایط کاربر بستگی دارد.

[ISO/IEC 9797-1]

---

1 - MAC algorithm key

۲ - استاندارد بین‌المللی ISO/IEC 9797-1:2011 در سال ۱۳۹۰ با شماره ملی ۹۷۹۷-۱ منتشر شده است.

3 - Message Authentication Code

4 - Cryptographic check value

۵ - استاندارد بین‌المللی ISO/IEC 7498-2:1989 در سال ۱۳۹۱ با شماره ملی ۱۶۲۷۴-۲ منتشر شده است

6 - Maintenance

۱۱-۳
تبدیل خروجی [1]
تابعی که در پایان الگوریتم MAC، قبل از عملیات کوتاه‌سازی به کار برده می‌شود.

[ISO/IEC 9797-1]

۱۲-۳
لایه‌گذاری [2]
افزودن بیت‌های اضافی به رشته داده است.

[ISO/IEC 10118-1]

۱۳-۳
تابع گردکننده
تابعی که دو رشته دودویی با طول L_1 و L_2 را به رشته دودویی با طول L_2 تبدیل می‌کند.

یادآوری ۱- این تابع به طو رمکرر به عنوان قسمتی از تابع درهم‌ساز به کار برده می‌شود، به طوری که یک رشته داده با طول L_1 را با خروجی قبلی با طول L_2 ترکیب می‌کند.

[ISO/IEC 10118-1]

یادآوری ۲- این تابع همچنین به عنوان تابع فشرده‌سازی در یک متن تابع درهم‌ساز خاص مورد ارجاع قرار می‌گیرد.

۱۴-۳
قدرت امنیتی [3]
عددی در ارتباط با مقدار کاری (یعنی تعداد عملیات) که برای شکستن یک الگوریتم یا سامانه رمزنگاشتی مورد نیاز است.

یادآوری- قدرت امنیتی بر حسب بیت مشخص می‌شود، و مقدار خاصی از مجموعه {۸۰ ,۱۱۲ ,۱۲۸ ,۱۹۲ ,۲۵۶} است. قدرت امنیتی b بیت به این معنی است که 2^b عملیات جهت شکستن سامانه مورد نیاز است.

۱۵-۳
کلمه [4]
رشته‌ای از ۳۲ بیت مورد استفاده در توابع درهم‌ساز اختصاصی یک، دو، سه، چهار و هشت، یا رشته‌ای از ۶۴ بیت استفاده شده در توابع درهم‌ساز اختصاصی پنج و شش از استاندارد ISO/IEC 10118-3 است.

1 - Output transformation
2 - Padding
3 - Security strength
4 - Word

۴ نمادها و نشانه‌گذاری

در این استاندارد از نمادها و نشانه‌گذاری‌های تعیین شده در استاندارد ISO/IEC 9797-1 به کار می‌رود:

m	طول MAC (بر حسب بیت).
q	تعداد بستک‌ها در رشته داده ورودی D بعد از فرآیند لایه‌گذاری و تقسیم.
$j \sim X$	رشته به دست آمده از رشته X، با برداشتن تعداد j بیت از سمت چپ‌ترین بیت‌های مربوط به رشته X
$X \oplus Y$	یای انحصاری[1] بیت به بیت رشته‌های بیت X و Y
$X \| \| Y$	الحاق رشته‌های بیت X و Y (به همان ترتیب)
$:=$	نمادی که بر عملیات «مجموعه برابر با» که در مشخصات رویه‌ای الگوریتم‌های MAC استفاده می‌شود، دلالت دارد، که در آن نشان می‌دهد که مقدار رشته در سمت چپ نماد باید با مقدار عبارت در سمت راست نماد مساوی باشد.

در این استاندارد نمادها و نشانه‌گذاری‌های زیر به کار می‌رود:

$\overline{\mathrm{D}}$	رشته داده لایه‌گذاری شده
h	تابع درهم‌ساز
h'	تابع درهم‌ساز h با ثابت‌های تعدیل شده و IV اصلاح شده.
$\bar{h}$	تابع درهم‌ساز ساده شده h بدون لایه‌گذاری و اضافه طول، و بدون کوتاهی خروجی تابع گردکننده (L_2 بیت) به چپ‌ترین بیت L_H **یادآوری ۱-** تابع $\bar{h}$ باید برای رشته‌های ورودی با طولی که مضرب عدد صحیح مثبت از L_1 است، به کار برده شود. **یادآوری ۲-** توصیه می‌شود خروجی $\bar{h}$ به جای L_H بیت L_2 بیت باشد. توابع درهم‌ساز اختصاصی شش و هشت در استاندارد ISO/IEC 10118-3 تعریف شده و در

1 - Exclusive-or

	آن L_H همیشه کوچک‌تر از L_2 است.
H'، H''	رشته‌های L_2 بیت که در محاسبه الگوریتم MAC جهت حفظ یک نتیجه میانی به کار می‌رود.
IV'، IV_1، IV_2	مقادیر اولیه
k	طول کلید الگوریتم MAC (بر حسب بیت)
K	کلید پنهان الگوریتم MAC
K'، K_0، K_1، K_2، $\bar{K}$، $\bar{K}_1$، $\bar{K}_2$	کلیدهای مشتق شده پنهان الگوریتم MAC
KT	اولین رشته ورودی تابع $\emptyset'$ مورد استفاده در مرحله تبدیل خروجی الگوریتم یک MAC
$\tilde{L}$	رشته بیتی که طول پیام در الگوریتم سه MAC را کدبندی می‌کند
$OPAD$، $IPAD$	رشته‌های ثابت مورد استفاده در الگوریتم دوم MAC
R، S_0، S_1، S_2	رشته‌های ثابت مورد استفاده در محاسبه ثابت‌ها برای الگوریتم یک MAC و الگوریتم سوم MAC
T_0، T_1، T_2	رشته‌های ثابت مورد استفاده در اشتقاق کلید[1] برای الگوریتم یک MAC و الگوریتم سوم MAC
U_0، U_1، U_2	رشته‌های ثابت مورد استفاده در اشتقاق کلید برای الگوریتم یک MAC و الگوریتم سوم MAC
$\emptyset'$	تابع گردکننده با ثابت‌های تعدیل شده
$K_1[i]$	کلمه iام از رشته K_1 یعنی $K1 = K1[0] \| \| K1[1] \| \| K1[2] \| \| K1[3]$.

در این استاندارد از نمادها و نشانه‌گذاری‌های تعیین شده در استاندارد ISO/IEC 10118-1 به کار می‌رود:

H	کد درهم‌ساز

1 - Key derivation

IV	مقدار اولیه
L_X	طول رشته بیت X (بر حسب بیت)

در این استاندارد از نمادها و نشانه‌گذاری‌های تعیین شده در استاندارد ISO/IEC 10118-3 به کار می‌رود:

C'_i،C_i	کلمه‌های ثابت مورد استفاده در تابع گردکننده
L_1	طول اولین رشته‌های ورودی به تابع گردکننده $\emptyset$ (بر حسب بیت)
L_2	طول (بر حسب بیت) دومین رشته ورودی به تابع گردکننده $\emptyset$، طول رشته خروجی از تابع گردکننده $\emptyset$ و VI
w	طول (بر حسب بیت) یک کلمه، w موقع به کارگیری توابع درهم‌ساز اختصاصی ۱،۲،۳،۴ و ۸ مربوط به ISO/IEC 10118-3، 32، و w موقع به کارگیری توابع درهم‌ساز اختصاصی ۵ و ۶ مربوط به ISO/IEC 10118-3، 64 است.
$\emptyset$	تابع گردکننده، یعنی اگر X و Y رشته‌های بیتی به ترتیب با طول‌های L_1 و L_2 باشند، آنگاه $\emptyset(X,Y)$ رشته به دست آمده از اعمال $\emptyset$ در X و Y هستند.
Ψ	عملیات افزایشی پیمانه 2^w، که w تعداد بیت‌های یک کلمه است. بنابراین، اگر A و B دو کلمه باشند، پس $A\Psi B$ کلمه‌ای است که از طریق تلقی کردن A و B به عنوان بازنمایی دودویی اعداد صحیح و محاسبه مجموع آن‌ها با پیمانه 2^w به دست آمده است، و نتیجه محدود به قرار گرفتن بین ۰ و 2^w-1 است. مقدار w در توابع درهم‌ساز اختصاصی ۱، ۲، ۳، ۴ و ۸، ۳۲ و در توابع درهم‌ساز اختصاصی ۵ و ۶، ۶۴ است.

۵ الزامات

کاربرانی که خواهان به کارگیری الگوریتم MAC از این استاندارد هستند، باید موارد زیر را انتخاب کنند:

- یک الگوریتم MAC از میان آن‌هایی که در بندهای ۶، ۷ و ۸ مشخص شده‌اند؛
- یک تابع درهم‌ساز اختصاصی از توابع مشخص شده در استاندارد ISO/IEC 10118-3؛ و
- طول MAC (m بر حسب بیت).

یادآوری ۱- به کارگیری الگوریتم‌های MAC به شماره‌های یک و سه با توابع درهم‌ساز اختصاصی هفت از استاندارد ISO/IEC10118-3 در این استاندارد مشخص نشده است.

توافق در زمینه‌ی این انتخاب‌ها در میان کاربران، برای استفاده از سازوکار یکپارچگی داده ضروری است.

کلید K استفاده شده در الگوریتم MAC باید دارای انتروپی باشد کـه بـرآورده کننـده و یـا فراتـر از قـدرت امنیتی ارائه شده توسط الگوریتم MAC باشد.

یادآوری ۲- در هر حال کلید K الگوریتم MAC باید به نحوی انتخاب شود کـه احتمـال انتخـاب تمـامی کلیـدهای محتمـل یکسان باشد.

برای الگوریتم های MAC یک و دو، طول m باید یک عدد صـحیح مثبـت کمتـر یـا مسـاوی بـا طـول کـد درهم‌ساز L_H باشد. در مورد الگوریتم MAC سه، طول m باید عدد صحیح مثبت کمتر یـا مسـاوی بـا نصـف طول کد درهم‌ساز باشد یعنی، $m \leq L_H/2$

برای الگوریتم های MAC یک و دو، طول (بر حسب بیت) رشته داده‌های ورودی D موقع به کارگیری توابع درهم‌ساز اختصاصی یک، دو، سه، چهـار و هشـت بایـد بیشـینه $۲^{۶۴}-۱$ باشـد و بـا اعمـال توابـع درهـم‌سـاز اختصاصی پنج و شش بیشینه $۲^{۱۲۸}-۱$ باشد. در مورد الگوریتم MAC دو، با اعمال توابع درهم‌ساز اختصاصـی هفت، بیشینه باید $۲^{۲۵۶}-۱$ باشد. برای الگوریتم MAC سه، باید بیشینه ۲۵۶ باشد.

انتخاب یک الگوریتم MAC خاص، تابع درهم‌ساز اختصاصی، و مقدار m فراتر از دامنه این استاندارد است.

یادآوری ۳- این انتخاب‌ها بر سطح امنیت الگوریتم MAC تاثیر می‌گذارد. برای جزییات بیشتر به پیوست پ مراجعه شود.

کلید به کار برده شده برای محاسبه و درستی‌سنجی MAC بایـد یکسـان باشـد. اگـر رشـته داده‌ای ورودی رمزنگاشتی شده باشد، کلید مورد استفاده برای محاسبه MAC باید متفاوت با نمونه به کار برده شـده بـرای رمزنگاشتی باشد.

یادآوری ۴- باید در نظر داشت جهت رمزنگاشتی خوب، کلیدهای مستقل برای محرمانگی و یکپارچگی داده‌ها باید در اختیـار داشت.

۶ الگوریتم MAC یک

یادآوری ۱- این بند شامل توصیف MDx-MAC با توابع درهم‌ساز اختصاصی یک تا شش و هشـت اسـت. جـدول ۱ نـام‌هـای شناخته شده MDx-MAC با توابع درهم‌ساز اختصاصی منحصر به فرد آن‌ها را نشان می‌دهد.

جدول ۱- الگوریتم MDx-MAC با توابع درهم‌ساز اختصاصی متفاوت

توابع درهم‌ساز اختصاصی	الگوریتم MDx-MAC شناخته شده تحت عنوان
توابع درهم‌ساز اختصاصی یک	RIPEMD-160-MAC
توابع درهم‌ساز اختصاصی دو	RIPEMD-128-MAC
توابع درهم‌ساز اختصاصی سه	SHA-1-MAC

توابع درهم‌ساز اختصاصی	الگوریتم MDx-MAC شناخته شده تحت عنوان
توابع درهم‌ساز اختصاصی چهار	SHA-256-MAC
توابع درهم‌ساز اختصاصی پنج	SHA-512-MAC
توابع درهم‌ساز اختصاصی شش	SHA-384-MAC
توابع درهم‌ساز اختصاصی هشت	SHA-224-MAC

یادآوری ۲- به کارگیری الگوریتم MAC یک، با تابع درهم‌ساز اختصاصی هفت مربوط به ISO/IEC 10118-3 در این استاندارد مشخص نشده است.

الگوریتم MAC یک، به یک بار به کار بردن تابع درهم‌ساز جهت محاسبه مقدار MAC نیاز دارد، اما مستلزم آن است که ثابت‌ها در تابع‌های گرد شده متناظر اصلاح شده باشند.

تابع درهم‌ساز باید از توابع درهم‌ساز اختصاصی یک تا شش از استاندارد ملی ایران به شماره ۹۵۹۸-۳ : سال ۱۳۹۱، و تابع درهم‌ساز اختصاصی هشت از ISO/IEC 10118-3:2004/Amd.1:2006 انتخاب شود.

طول بیتی کلید K باید بیشینه ۱۲۸ بیت باشد.

۶-۱ توصیف الگوریتم MAC یک

الگوریتم MAC یک شامل ۵ مرحله زیر است:

بسط کلید، تعدیل ثابت‌ها و IV، عملیات درهم‌ساز، تبدیل خروجی و کوتاه‌سازی.

۶-۱-۱ مرحله یک (بسط کلید)

اگر K کوتاه‌تر از ۱۲۸ بیت باشد، K را $\lceil 128/K \rceil$ بار به خود الحاق کنید و از نتیجه، سمت چپ‌ترین ۱۲۸ بیت را جهت تشکیل دادن کلید K' ۱۲۸ بیتی انتخاب کنید (اگر طول (بر حسب بیت) K برابر با ۱۲۸ باشد، $K' := K$ خواهد بود):

$$K' := 128 \sim (K \,||\, K \,||\, \ldots. \,||\, K).$$

زیرکلیدهای K_0، K_1، و K_2 را مانند زیر محاسبه کنید:

$$K_0 := \bar{h}\ (K' \,||\, U_0 \,||\, K')$$

$$K_1 := 128 \sim \bar{h}(K' \,||\, U_1 \,||\, K'),$$ در صورت استفاده از توابع درهم‌ساز اختصاصی ۱،۲ و ۳

$$K_1 := 256 \sim \bar{h}(K' \,||\, U_1 \,||\, K'),$$ در صورت استفاده از توابع درهم‌ساز اختصاصی ۴، ۵، ۶ و ۸

$$K_2 := 128 \sim \bar{h}(K' \,||\, U_2 \,||\, K').$$

در این‌جا U_0، U_1، و U_2 ثابت‌های ۷۶۸ بیتی هستند که در زیربند ۶-۳ تعریف شده‌اند، و $\bar{h}$ یک تابع درهم‌ساز ساده شده h را مشخص می‌کند یعنی بدون لایه‌گذاری و افزایش طول و بدون کوتاه کردن خروجی (L_2 بیتی) تابع گردکننده به L_H بیت سمت چپ است.

یادآوری ۱- لایه‌گذاری و افزایش طول حذف شده‌اند، به دلیل این که در این مورد طول رشته ورودی یا L_1 بیت یا $2L_1$ بیت است.

یادآوری ۲- کوتاه‌سازی حذف گردید به دلیل این که در این مورد طول K_0 همواره L_2 بیت است، که کمینه L_H است.

در مورد به کارگیری توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، پنج و شش، کلید مشتق شده K_1 به چهار کلمه ذکر شده توسط $K_1[i]\ (0 \leq i \leq 3)$ تقسیم می‌شود، یعنی:

$$K_1 = K_1[0] \,||\, K_1[1] \,||\, K_1[2] \,||\, K_1[3].$$

در مورد به کارگیری توابع درهم‌ساز اختصاصی چهار و هشت، کلید مشتق شده K_1 به هشت کلمه ذکر شده توسط $K_1[i]\ (0 \leq i \leq 7)$ تقسیم می‌شود، یعنی:

$$K_1 = K_1[0] \,||\, K_1[1] \,||\, K_1[2] \,||\, K_1[3] \,||\, K_1[4] \,||\, K_1[5] \,||\, K_1[6] \,||\, K_1[7].$$

برای تبدیل یک رشته به کلمات، یک قرارداد مرتب‌سازی بایت مورد نیاز است. قرارداد مرتب‌سازی بایت برای این تبدیل، همان قراردادی است که برای تابع درهم‌ساز اختصاصی انتخاب شده در استاندارد ISO/IEC 10118-3 تعریف شده است.

۶-۱-۲ مرحله دو (تعدیل ثابت‌ها و *IV*)

موقع به کارگیری توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، پنج، شش و هشت، ثابت‌های افزایشی به کار رفته در تابع گردکننده توسط پیمانه اضافی 2^w از یک کلمه K_1 تعدیل می‌شوند. برای مثال :

$$C_0 := C_0 \,\Psi\, K_1[0].$$

زیربند ۶-۳ نشان می‌دهد کدام یک از کلمه‌های K_1 به هر ثابتی اضافه شده است.

مقدار اولیه *IV* از تابع درهم‌ساز توسط $IV' := K_0$ جایگزین شده است.

تابع حاصل در نتیجه تغییرات در این مرحله توسط *h'*، مشخص شده است و تابع گردکننده آن از طریق $\emptyset$ بیان شده است.

۶-۱-۳ مرحله سه (عملیات درهم‌ساز)

رشته‌ای که ورودی تابع درهم‌ساز تعدیل شده h'، است مساوی با رشته داده ورودی D است یعنی :

$$H' := h'(D).$$

۶-۱-۴ مرحله چهار (تبدیل حروجی)

تابع گردکننده‌ی تعدیل شده $\emptyset$ یک بار دیگر اعمال می‌شود، با اولین رشته ورودی KT (در زیر تعریف شده) و دومین ورودی رشته H' (نتیجه مرحله سه) یعنی:

$$H'' := \emptyset'(KT, H').$$

برای توابع درهم‌ساز اختصاصی یک، دو، سه، چهار و هشت،

$$KT = K_2 || (K_2 \oplus T_0) || (K_2 \oplus T_1) || (K_2 \oplus T_2)$$

برای توابع درهم‌ساز اختصاصی پنج و شش،

$$KT = K_2 || (K_2 \oplus T_0) || (K_2 \oplus T_1) || (K_2 \oplus T_2) || K_2 || (K_2 \oplus T_0) || (K_2 \oplus T_1) || (K_2 \oplus T_2).$$

در این جا T_0،T_1 و T_2رشته‌های ۱۲۸ بیتی تعریف شده در زیربند ۶-۳ برای هر تابع درهم‌ساز اختصاصی هستند.

یادآوری- تغییر خروجی مربوط به پردازش بستک داده‌ای اضافی از K_2 بعد از لایه‌گذاری و افزایش طول مشتق شده است.

۶-۱-۵ مرحله پنج (کوتاه‌سازی)

تعداد m بیت MAC، با در نظر گرفتن سمت چپی ترین m بیت رشته H'' مشتق شده است یعنی:

$$\text{MAC} := m \sim H''.$$

۶-۲ کارایی

اگر رشته داده لایه‌گذاری شده (در مورد الگوریتم‌های لایه‌گذاری شده وابسته به تابع درهم‌ساز انتخاب شده) شامل q بستک باشد، پس الگوریتم MAC یک، به $q+7$ برنامه کاربردی از تابع گردکننده نیاز دارد.

این می‌تواند به q+1 کاربرد از تابع گردکننده از طریق پیش محاسبه مقادیرK_0، K_1، و K_2 و از طریق جایگزینی مقدار اولیه IV با IV' در کاربرد تابع درهم‌ساز کاهش یابد. توصیه می‌شود ایجاد تعدیل در کد تابع درهم‌ساز همراه با تعدیل اجباری مورد نیاز در مرحله دو صورت گیرد.

برای رشته‌های ورودی بلند، الگوریتم MAC یک، دارای عملکردی است که قابل مقایسه با عملکرد تابع درهم‌ساز استفاده شده است.

۶-۳ محاسبه ثابت‌ها

ثابت‌های تعریف شده در این بند در الگوریتم‌های MAC یک و سه، استفاده می‌شود. الگوریتم MAC سه، در بند ۸ مشخص شده است.

رشته‌های T_i و U_i $(0 \le i \le 2)$عناصر ثابت در توصیف الگوریتم MAC هستند. آن‌ها (فقط یکبار) با استفاده از تابع درهم‌ساز مورد محاسبه قرار می‌گیرند، آن‌ها برای هر هفت تابع درهم‌ساز متفاوت هستند.

ثابت‌های ۱۲۸ بیتی T_i و ۷۶۸ بیتی U_i به صورت زیر تعریف شده‌اند. تعریف T_i شامل۴۹۶ بیت از ثابت $R = "ab \dots yzAB \dots YZ01 \dots 89"$ و شانزده بیت از ثابت‌های S_0، S_1، S_2 است، به طوری که رشته S_i شانزده بیتی شکل گرفته توسط تکرار دو بار بازنمایی هشت بیتی i است (برای مثال بازنمایی مبنای شانزده برای S_1 ، ۳۱۳۱ است). در هر دو مورد کدگذاری ASCII مورد استفاده قرار گرفته است، این کدگذاری معادل با کدگذاری مورد استفاده در استاندارد ISO/IEC 646:1991 است.

$For\ i := 0\ to\ 2$
$T_i := 128 \sim \bar{h}\ (S_i \,||\, R)$

برای توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، شش و هشت،

$T_i := 128 \sim \bar{h}\ (S_i \,||\, R \,||\, 0^{512})$

برای توابع درهم‌ساز اختصاصی ۵ و ۶، به طوری که 0^{512}، تعداد ۵۱۲ بیت '0 است.

$For\ i := 0\ to\ 2$
$U_i = T_i \,||T_{i+1}\,||T_{i+2}\,||T_i\,||T_{i+1}\,||T_{i+2}$.

که زیرنویس‌ها در T_i طبق پیمانه ۳ گرفته شده باشند.

در توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، پنج، شش و هشت، برای کلیه ثابت‌های C_i، C'_i و تمامی کلمه‌های K_1 [i] با اهمیت‌ترین بیت مربوط به سمت چپ‌ترین بیت است. ثابت‌های C_i و C'_i با استفاده از بازنمایی مبنای شانزده نشان داده می‌شود.

۶-۳-۱ تابع درهم‌ساز اختصاصی یک (RIPEMD-160)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی یک به شرح زیر تعریف شده است (بازنمایی مبنای شانزده):

T_o= 1CC7086A046AFA22353AE88F3D3DACBE

T_1 = E3FA02710E491D851151CC34E4718D41

T_2 = 93987557C07B8102BA592949EB638F37

دو دنباله از کلمات ثابت C_0، C_1، ...، C_{79} و C'_0، C'_1، ...، C'_{79} در تابع گردکننده تابع درهم‌ساز اختصاصی یک استفاده شده‌اند. این دنباله‌ها به صورت زیر تعریف می‌شود:

$$Ci = K_1[0] \Psi \text{ 00000000}, \ (0 \leq i \leq 15),$$

$$Ci = K_1[1] \Psi \text{ 5A827999}, \ (16 \leq i \leq 31)$$

$$Ci = K_1[2] \Psi \text{ 6ED9EBA1}, \ (32 \leq i \leq 47),$$

$$Ci = K_1[3] \Psi \text{ 8F1BBCDC}, \ (48 \leq i \leq 63)$$

$$Ci = K_1[0] \Psi \text{ A953FD4E}, \ (64 \leq i \leq 79),$$

$$C'_i = K_1[1] \Psi \text{ 50A28BE6}, \ (0 \leq i \leq 15),$$

$$C'_i = K_1[2] \Psi \text{ 5C4DD124}, \ (16 \leq i \leq 31)$$

$$C'_i = K_1[3] \Psi \text{ 6D703EF3}, \ (32 \leq i \leq 47),$$

$$C'_i = K_1[0] \Psi \text{ 7A6D76E9}, \ (48 \leq i \leq 63)$$

$$C'_i = K_1[1] \Psi \text{ 00000000}, \ (64 \leq i \leq 79)$$

۶-۳-۲ تابع درهم‌ساز اختصاصی دو (RIPEMD-128)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی دو به شرح زیر تعریف شده است (بازنمایی مبنای شانزده):

T_o= FD7EC18964C36D53FC18C31B72112AAC

T_1 = 2538B78EC0E273949EE4C4457A77525C

T_2 = F5C93ED85BD65F609A7EB182A85BA181

دو دنباله کلمات ثابت C_0،C_1،....، C_{63} و C'_0،C'_1،....، C'_{63} در تابع گردکننده تابع درهم‌ساز اختصاصی دو استفاده شده‌اند. این دنباله‌ها به صورت زیر تعریف می‌شود:

$$Ci = K_1[0] \Psi \text{ 00000000}, \ (0 \leq i \leq 15),$$

$$Ci = K_1[1] \Psi \text{ 5A827999}, \ (16 \leq i \leq 31)$$

$$Ci = K_1[2] \Psi \text{ 6ED9EBA1}, \ (32 \leq i \leq 47),$$

$$Ci = K_1[3] \Psi \text{ 8F1BBCDC}, \ (48 \leq i \leq 63)$$

$$C'_i = K_1[0] \Psi \text{ 50A28BE6}, \ (0 \leq i \leq 15),$$

$C'_i = K_1[1] \Psi$ 5C4DD124, $(16 \leq i \leq 31)$

$C'_i = K_1[2] \Psi$ 6D703EF3, $(32 \leq i \leq 47)$,

$C'_i = K_1[3] \Psi$ 00000000, $(48 \leq i \leq 63)$.

۶-۳-۳ تابع درهم‌ساز اختصاصی سه (SHA-1)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی سه به شرح زیر تعریف شده است (بازنمایی مبنای شانزده):

T_o= 1D4CA39FA40417E2AE5A77B49067BBCC

T_1 = 9318AFEF5D5A5B46EFCA6BEC0E138940

T_2 = 4544209656E14F97005DAC76868E97A3

دنباله کلمات ثابت C_0،C_1 ،...،C_{79} در تابع گردکننده تابع درهم‌ساز اختصاصی سه استفاده می‌شود. این دنباله به صورت زیر تعریف می‌شود:

$Ci = K_1[0] \Psi$ 5A827999, $(0 \leq i \leq 19)$,

$Ci = K_1[1] \Psi$ 6ED9EBA1, $(20 \leq i \leq 39)$

$Ci = K_1[2] \Psi$ 8F1BBCDC, $(40 \leq i \leq 59)$,

$Ci = K_1[3] \Psi$ CA62C1D6, $(60 \leq i \leq 79)$.

۶-۳-۴ تابع درهم‌ساز اختصاصی چهار (SHA-256)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی چهار به ترتیب زیر تعریف شده است (به طوری که $\bar{h}$ نسخه ساده شده تابع درهم‌ساز اختصاصی چهار تعریف شده در زیربند ۶-۱-۱ است):

$T_0 := 128 \sim \bar{h}\,(S_0 \,||\, R)$,

$T_1 := 128 \sim \bar{h}\,(S_1 \,||\, R)$,

$T_2 := 128 \sim \bar{h}\,(S_2 \,||\, R)$.

دنباله کلمات ثابت C_0، C_1، ...، C_{63} در تابع گردکننده تابع درهم‌ساز اختصاصی چهار استفاده می‌شود. این دنباله به صورت زیر تعریف می‌شود:

$C_i = K_1[i \bmod 8] \Psi\, C''_i$, $(0 \leq i \leq 63)$.

به طوری که دنباله C''_0،C''_1 ،...،C''_{63} در بازنمایی مبنای شانزده (که در آن با اهمیت‌ترین بیت مربـوط بـه سمت چپ‌ترین بیت است) به ترتیب زیر تعریف می‌شود، به گونه‌ای که کلمات به ترتیب C''_0،C''_1 ،...،C''_{63} فهرست شده اند.

```
428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
e49b69c1 efbe4786 0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208 90befff a a4506ceb bef9a3f7 c67178f2
```

یادآوری- این مقادیر اولین ۳۲ بیت قسمت‌های کسری ریشه‌های مکعب از اولین ۶۴ عدد اول هستند. آن‌ها دنباله ثابت مـورد استفاده در SHA-256 هستند.

۶-۳-۵ تابع درهم‌ساز اختصاصی پنج (SHA-512)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی پنج به ترتیب زیر تعریف شده است (بـه طـوری که $\bar{h}$ نسخه ساده شده تابع درهم‌ساز اختصاصی پنج تعریف شده در زیربند ۶-۱-۱ است):

T_o= 85f6e8b28ba014ed11d076ead90412a5

T_1 = 33a6da6c7aaaf2149104fe4183152828

T_2 = 7682094a7e45cf6bf27d19c2c7d6cf77

دنباله کلمات ثابت C_0،C_1 ،...،C_{79} در تابع گردکننده تابع درهم‌ساز اختصاصی پنج استفاده می‌شود. این دنباله به صورت زیر تعریف می‌شود:

$$C_i = K_1[i \bmod 4] \Psi C''_i, \quad (0 \leq i \leq 79).$$

به طوری که دنباله C''_0،C''_1 ،...،C''_{79} در بازنمایی مبنای شانزده (که در آن با اهمیت‌ترین بیت مربـوط بـه سمت چپ‌ترین بیت است) به ترتیب زیر تعریف می‌شود، به گونه‌ای که کلمات به ترتیب C''_0،C''_1 ،...،C''_{79} فهرست شده‌اند.

```
428a2f98d728ae22  7137449123ef65cd  b5c0fbcfec4d3b2f  e9b5dba58189dbbc
3956c25bf348b538  59f111f1b605d019  923f82a4af194f9b  ab1c5ed5da6d8118
d807aa98a3030242  12835b0145706fbe  243185be4ee4b28c  550c7dc3d5ffb4e2
72be5d74f27b896f  80deb1fe3b1696b1  9bdc06a725c71235  c19bf174cf692694
e49b69c19ef14ad2  efbe4786384f25e3  0fc19dc68b8cd5b5  240ca1cc77ac9c65
2de92c6f592b0275  4a7484aa6ea6e483  5cb0a9dcbd41fbd4  76f988da831153b5
983e5152ee66dfab  a831c66d2db43210  b00327c898fb213f  bf597fc7beef0ee4
```

c6e00bf33da88fc2	d5a79147930aa725	06ca6351e003826f	142929670a0e6e70
27b70a8546d22ffc	2e1b21385c26c926	4d2c6dfc5ac42aed	53380d139d95b3df
650a73548baf63de	766a0abb3c77b2a8	81c2c92e47edaee6	92722c851482353b
a2bfe8a14cf10364	a81a664bbc423001	c24b8b70d0f89791	c76c51a30654be30
d192e819d6ef5218	d69906245565a910	f40e35855771202a	106aa07032bbd1b8
19a4c116b8d2d0c8	1e376c085141ab53	2748774cdf8eeb99	34b0bcb5e19b48a8
391c0cb3c5c95a63	4ed8aa4ae3418acb	5b9cca4f7763e373	682e6ff3d6b2b8a3
748f82ee5defb2fc	78a5636f43172f60	84c87814a1f0ab72	8cc702081a6439ec
90befffa23631e28	a4506cebde82bde9	bef9a3f7b2c67915	c67178f2e372532b
ca273eceea26619c	d186b8c721c0c207	eada7dd6cde0eb1e	f57d4f7fee6ed178
06f067aa72176fba	0a637dc5a2c898a6	113f9804bef90dae	1b710b35131c471b
28db77f523047d84	32caab7b40c72493	3c9ebe0a15c9bebc	431d67c49c100d4c
4cc5d4becb3e42b6	597f299cfc657e2a	5fcb6fab3ad6faec	6c44198c4a475817

یادآوری- این مقادیر اولین ۶۴ بیت قسمت‌های کسری ریشه‌های سوم از اولین ۸۰ عدد اول هستند. آن‌ها دنباله ثابت مورد استفاده در SHA-512 هستند.

۶-۳-۶ تابع درهم‌ساز اختصاصی شش (SHA-384)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی شش به ترتیب زیر محاسبه می‌شود (به طوری که $\bar{h}$ نسخه ساده شده تابع درهم‌ساز اختصاصی شش تعریف شده در زیربند ۶-۱-۱ است):

T_o= 33bfc7a7db2d833c1fa120f248ea0c68

T_1 = 0f53e26170ddedf90aa666a58accf8c4

T_2 = f9371fddd155caefbd989e1270066c7c

دنباله کلمات ثابت C_0،C_1، ...،C_{79} در تابع گردکننده تابع درهم‌ساز اختصاصی شش استفاده می‌شود. این دنباله به صورت زیر تعریف می‌شود:

$$C_i = K_1[i \bmod 4] \Psi C''_i \quad (0 \leq i \leq 79),$$

به طوری که دنباله C''_0،C''_1، ...،C''_{79} یکسان با دنباله تابع درهم‌ساز اختصاصی پنج در زیربند ۶-۳-۵ است.

۶-۳-۷ تابع درهم‌ساز اختصاصی هشت (SHA-224)

رشته‌های ثابت ۱۲۸ بیتی T_i برای تابع درهم‌ساز اختصاصی هشت به ترتیب زیر محاسبه می‌شود (به طوری که $\bar{h}$ نسخه ساده شده تابع درهم‌ساز اختصاصی هشت تعریف شده در زیربند ۶-۱-۱ است):

$$T_0 := 128 \sim \bar{h}\,(S_0 \,||\, R),$$

$$T_1 := 128 \sim \bar{h}\,(S_1 \,||\, R),$$

$$T_2 := 128 \sim \bar{h}\,(S_2 \,||\, R).$$

دنباله کلمات ثابت C_0،C_1 ،...،C_{63} در تابع گردکننده تابع درهم‌ساز اختصاصی شش استفاده می‌شود. این دنباله به صورت زیر تعریف می‌شود:

$$C_i = K_1[i \bmod 8]\,\Psi\, C''_i, \quad (0 \le i \le 63).$$

به طوری که دنباله C''_0،C''_1 ،...،C''_{63} یکسان با دنباله تابع درهم‌ساز اختصاصی چهار در زیربند ۶-۳-۴ است.

۷ الگوریتم MAC دو

یادآوری ۱- این بند شامل توصیفی از HMAC [۷] است.

الگوریتم MAC دو، به دو کاربرد از تابع درهم‌ساز جهت محاسبه مقدار MAC نیاز دارد.

تابع درهم‌ساز باید از استاندارد ISO/IEC 10118-3 انتخاب شود، با الزام این که L_1 یک عدد صحیح مثبت مضرب ۸ بوده و $L_2 \le L_1$ باشد.

یادآوری- توابع درهم‌ساز اختصاصی یک تا هفت در استاندارد ISO/IEC 10118-3:2004 و تابع درهم‌ساز اختصاصی هشت در استاندارد ISO/IEC 10118-3/Amd:2006 این شرایط را برآورده می‌کنند.

اندازه کلید k بر حسب بیت باید حداقل L_2 باشد، به طوری که L_2 اندازه کد درهم‌ساز بر حسب بیت بوده و بیشینه L_1 است، به طوری که L_1 اندازه داده ورودی تابع گردکننده بر حسب بیت است. یعنی، $L_2 \le k \le L_1$.

۷-۱ توصیف الگوریتم MAC دو

الگوریتم MAC دو، نیاز به چهار مرحله زیر دارد:

بسط کلید، عملیات درهم‌ساز، تبدیل خروجی و کوتاه‌سازی.

۷-۱-۱ مرحله یک (بسط کلید)

تعداد (L_1 - k) بیت صفر به سمت راست کلید k پیوست نمایید؛ رشته حاصل به طول L_1 توسط $\bar{K}$ نشان داده می‌شود.

کلید $\bar{K}$ جهت ایجاد دو زیرکلید $\bar{K}_1$ و $\bar{K}_2$ بسط داده می‌شود:

- رشته *IPAD* را به عنوان الحاق تعداد $L_1/8$ رونوشت از مقدار مبنای شانزده «36» (و یا مقدار دودویی «00110110»)تعریف کنید. سپس مقدار $\bar{K}_1$ را به عنوان عطف انحصاری $\bar{K}$ و رشته *IPAD* محاسبه کنید، یعنی:

$$\bar{K}_1 := \bar{K} \oplus IPAD.$$

- رشته $OPAD$ را به عنوان الحاق تعداد $L_1/8$ رونوشت از مقدار مبنای شانزده «5C» (و یا مقدار دودویی «01011100»)تعریف کنید. سپس مقدار $\bar{K}_2$ را به عنوان عطف انحصاری $\bar{K}$ و رشته $OPAD$ محاسبه کنید، یعنی:

$$\bar{K}_2 := \bar{K} \oplus OPAD.$$

۷-۱-۲ مرحله دو (عملیات درهم‌ساز)

رشته ورودی به تابع درهم‌ساز مساوی با الحاق $\bar{K}_1$ و D است، یعنی:

$$H' := h(\bar{K}_1 \| D).$$

۷-۱-۳ مرحله سه (تبدیل خروجی)

رشته ورودی به تابع درهم‌ساز مساوی با الحاق $\bar{K}_2$ و H' است، یعنی:

$$H'' := h(\bar{K}_2 \| H').$$

۷-۱-۴ مرحله چهار (کوتاه‌سازی)

مقدار MAC به طول m بیت، با برداشتن m بیت سمت چپ‌ترین از رشته H'' مشتق می‌شود، یعنی:

$$\text{MAC} := m \sim H''.$$

۷-۲ کارایی

اگر رشته داده‌ی لایه‌گذاری شده (موقعی که الگوریتم لایه‌گذاری برای تابع درهم‌ساز انتخاب شده شناخته شده است) حاوی q بستک باشد، آنگاه الگوریتم MAC دو، نیاز به q+3 کاربرد از تابع گردکننده دارد.

این می‌تواند به q+1 کاربرد تابع گردکننده از طریق تعدیل کد تابع درهم‌ساز کاهش یابد. می‌توان مقادیر $IV_1 := \emptyset(\bar{K}_1, IV)$ و $IV_2 := \emptyset(\bar{K}_2, IV)$ را از قبل محاسبه کرد و مقدار اولیه IV را با IV_1 در اولین کاربرد تابع درهم‌ساز جایگزین کرد، و با IV_2 در تبدیل خروجی (دومین کاربرد تابع درهم‌ساز). این مورد به یک تعدیل در روش لایه‌گذاری نیاز دارد، در واقع، ورودی واقعی به تابع درهم‌ساز در حال حاضر L_1 بیت کوتاه‌تر است. به این معنا است که مقدار L_1 باید به مقدار L_D اضافه شود.

برای رشته‌های ورودی بلند، الگوریتم MAC دو، کارایی قابل مقایسه با تابع درهم‌ساز به کار رفته دارد.

۸ الگوریتم MAC سه

یادآوری- این بند شامل نوعی الگوریتم MAC یک، است که برای ورودی‌های کوتاه بهینه سازی شده است (بیشینه ۲۵۶ بیت).

الگوریتم MAC سه، به هفت کاربرد تابع گردکننده ساده شده جهت محاسبه مقدار MAC نیاز دارد، اما این می‌تواند به یک کاربرد این تابع گردکننده از طریق اجرای پیش محاسبات معین کاهش یابد.

تابع درهم‌ساز باید از توابع درهم‌ساز اختصاصی یک تا شش از استاندارد ملی ایران به شماره ۹۵۹۸-۳ : سال ۱۳۹۱، و تابع درهم‌ساز اختصاصی هشت از ISO/IEC 10118-3 Amd1:2006 انتخاب گردد.

اندازه کلید k بر حسب بیت بیشینه ۱۲۸ بیت، و طول MAC، m بر حسب بیت باید بیشینه $L_H/2$ باشد.

۸-۱ توصیف الگوریتم MAC سه

این الگوریتم نیاز به پنج مرحله زیر دارد:

بسط کلید، تعدیل ثابت‌های تابع گردکننده، لایه گذاری، به کارگیری تابع گردکننده و کوتاه‌سازی.

۸-۱-۱ مرحله یک (بسط کلید)

اگر K کوتاه‌تر از ۱۲۸ بیت باشد، به تعداد دفعات کافی K را به خود الحاق نمایید و سمت چپ‌ترین ۱۲۸ بیت را جهت ایجاد کلید ۱۲۸ بیتی K' انتخاب کنید (اگر طول K (بر حسب بیت) مساوی ۱۲۸ باشد، آنگاه $K' := K$).

$$K' := 128 \sim (K \,||\, K \,||\, \dots \,||\, K).$$

زیرکلیدهای K_0، K_1، و K_2 را مانند زیر محاسبه نمایید:

$$K_0 := \bar{h}\ (K' \,||\, U_0 \,||\, K')$$

$$K_1 := 128 \sim \bar{h}(K' \,||\, U_1 \,||\, K'),$$ در صورت استفاده از توابع درهم‌ساز اختصاصی ۱،۲ و ۳

$$K_1 := 256 \sim \bar{h}(K' \,||\, U_1 \,||\, K'),$$ در صورت استفاده از توابع درهم‌ساز اختصاصی ۴، ۵، ۶ و ۸

$$K_2 := 128 \sim \bar{h}(K' \,||\, U_2 \,||\, K').$$

در اینجا U_0، U_1، و U_2 ثابت‌های ۷۶۸ بیتی هستند که در زیربند ۶-۳ تعریف شده‌اند، و $\bar{h}$ بیانگر تابع درهم‌ساز h بدون لایه‌گذاری و افزایش طول و بدون کوتاه کردن خروجی (L_2 بیت) تابع گردکننده به سمت چپ‌ترین L_H بیت است.

یادآوری ۱- لایه‌گذاری و افزایش طول حذف شده‌اند، به دلیل این که در این مورد طول رشته ورودی یا L_1 بیت یا $2L_2$ بیت است.

یادآوری ۲- کوتاه‌سازی حذف گردید به دلیل این که در این مورد طول K_0 هموارهL_2 بیت است، که بزرگ‌تر و مساوی L_H است.

در هنگام به کارگیری توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، پنج و شش، کلید مشتق شده K_1 به چهار کلمه ذکر شده توسط $K_1[i]\ (0 \le i \le 3)$ تقسیم می‌شود، یعنی:

$$K_1 = K_1[0] \,||\, K_1[1] \,||\, K_1[2] \,||\, K_1[3].$$

در مورد به کارگیری توابع درهم‌ساز اختصاصی چهار و هشت، کلید مشتق شده K_1 به هشت کلمه ذکر شده توسط $K_1[i]\ (0 \leq i \leq 7)$ تقسیم می‌شود، یعنی:

$$K_1 = K_1[0] \,||\, K_1[1] \,||\, K_1[2] \,||\, K_1[3] \,||\, K_1[4] \,||\, K_1[5] \,||\, K_1[6] \,||\, K_1[7].$$

برای تبدیل یک رشته به کلمات، یک قرارداد مرتب‌سازی بایت مورد نیاز است. قرارداد مرتب‌سازی بایت برای این تبدیل همان است که برای هر تابع درهم‌ساز اختصاصی در ISO/IEC 10118-3 تعریف شده است.

۸-۱-۲ مرحله دو (تعدیل ثابت‌ها و IV)

موقع به کارگیری توابع درهم‌ساز اختصاصی یک، دو، سه، چهار، پنج، شش و هشت، ثابت‌های افزایشی به کار رفته در تابع گردکننده توسط پیمانه اضافی 2^w از یک کلمه K_1 تعدیل می‌شوند. برای مثال:

$$C_0 := C_0 \,\Psi\, K_1[0].$$

زیربند ۶-۳ نشان می‌دهد که کدام کلمه K_1 به هر ثابت اضافه می‌شود.

مقدار اولیه IV از تابع درهم‌ساز توسط $IV' := K_0$ جایگزین می‌شود. تابع گردکننده حاصل با $\emptyset'$ نشان داده می‌شود.

۸-۱-۳ مرحله سه (لایه گذاری)

بیت‌های لایه‌گذاری که به رشته‌های داده‌ای اصلی اضافه شده‌اند فقط در محاسبه MAC به کار رفته‌اند. در نتیجه، این بیت‌های لایه‌گذاری نیازی به ذخیره شدن و انتقال با داده را ندارند. درستی‌سنج باید آگاه باشد که آیا بیت‌های لایه‌گذاری ذخیره و یا انتقال داده شده‌اند یا نه.

رشته داده‌ای D وارد شده در الگوریتم MAC باید با چند (در حد امکان هیچ) بیت «0» لازم جهت به دست آوردن یک رشته داده $\overline{D}$ به طول ۲۵۶ بیت از سمت راست لایه‌گذاری شود.

یادآوری- اگر رشته داده ورودی تهی است، رشته داده‌ای لایه‌گذاری شده $\overline{D}$ شامل ۲۵۶ بیت «0» خواهد بود.

۸-۱-۴ مرحله چهار (کاربرد تابع گردکننده)

رشته بیت $\tilde{L}$ به عنوان بازنمایی دودویی طول L_D از رشته داده D، که با چند بیت «0» لازم جهت به دست آوردن یک رشته ۱۲۸ بیتی از سمت چپ لایه‌گذاری شده است، محاسبه می‌شود. سمت راست‌ترین بیت رشته بیتی $\tilde{L}$ متناظر با کم ارزش‌ترین بیت بازنمایی دودویی L_D است.

رشته‌ای که به عنوان ورودی تابع گردکننده $\emptyset'$ (با ثابت‌های تعدیل شده) است مساوی با الحاق K_2، $\overline{D}$ و عطف انحصاری K_2 و $\tilde{L}$ است.

برای توابع درهم‌ساز اختصاصی یک، دو، سه، چهار و هشت،

$$H' := \emptyset'(K_2 || \bar{D} || (K_2 \oplus \tilde{L}), IV').$$

برای تابع درهم‌ساز اختصاصی پنج و شش،

$$H' = \emptyset'(K_2 || \bar{D} || (K_2 \oplus \tilde{L}) || K_2 || \bar{D} || (K_2 \oplus \tilde{L}), IV').$$

۸-۱-۵ مرحله پنج (کوتاه‌سازی)

مقدار MAC با طول m بیت، با برداشتن m بیت سمت چپ‌ترین از رشته H' مشتق می‌شود، یعنی:

$$\text{MAC} := m \sim H'.$$

۸-۲ کارایی

الگوریتم MAC سه، نیاز به ۷ کاربرد تابع گردکننده دارد.

این تعداد می‌تواند از طریق پیش محاسبه مقادیر K_0، K_1 و K_2 به یک کاربرد تابع گردکننده کاهش یابد.

پیوست الف

(الزامی)

پودمان[1] نشانه‌گذاری نحو انتزاعی یک (ASN.1)[2]

این پیوست، پودمان ASN.1 را که در ارتباط با سازوکارهای MAC مشخص شده است را در ISO/IEC 9797-2، مشخص می‌کند.

```
MechanismsUsingADedicatedHashFunction {
iso(1) standard(0) message-authentication-codes(9797) part(2)
asn1-module(0) mechanisms-using-a-dedicated-hash-function(0) version2(2)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ALL;
IMPORTS
OID, ALGORITHM, HashFunctions, HashFunctionAlgs
FROM DedicatedHashFunctions {iso(1) standard(0)
hash-functions(10118) part(3)
asn1-module(1) dedicated-hash-functions(0)};
-- OID assignments
-- ===============
is9797-2 OID ::= {iso standard message-authentication-codes(9797) part(2)}
id-mac-1 OID ::= {is9797-2 macAlgorithm-1(1)}
id-mac-2 OID ::= {is9797-2 macAlgorithm-2(2)}
id-mac-3 OID ::= {is9797-2 macAlgorithm-3(3)}
-- MAC algorithm identifier type and the set of recognized MAC algorithms
--
=====================================================================
AlgorithmIdentifier {ALGORITHM:IOSet} ::= SEQUENCE {
algorithm ALGORITHM.&id({IOSet}),
parameters ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
MessageAuthenticationCode ::= AlgorithmIdentifier{{MacAlgorithms}}
MacAlgorithms ALGORITHM ::= {
{OID id-mac-1 PARMS MacParameters} |
{OID id-mac-2 PARMS MacParameters} |
{OID id-mac-3 PARMS MacParameters} ,
... -- additional algorithms expected --
}
-- MAC parameter type definitions
-- ==============================
-- The optional parameters may be agreed upon by other means
MacParameters ::= SEQUENCE {
dhfAlgo HashFunctions OPTIONAL,
m INTEGER (1..MAX)
}
END -- MechanismsUsingADedicatedHashFunction --
```

1- Module
2 - Abstract Syntax Notation one

پیوست ب
(اطلاعاتی)
مثال‌ها

ب-۱ عمومی

این پیوست مثال‌هایی برای محاسبه الگوریتم‌های MAC یک، دو و سه، ارائه می‌کند. مثال‌های الگوریتم‌های MAC یک و سه، از توابع درهم‌ساز یک تاشش و هشت، استفاده می‌کنند. مثال‌های الگوریتم MAC دو، از توابع درهم‌ساز اختصاصی یک تا هشت استفاده می‌کند. توابع درهم‌ساز اختصاصی یک تا هفت در استاندارد ملی ایران به شماره ۹۵۹۸-۳ : سال ۱۳۹۱، و تابع درهم‌ساز اختصاصی هشت در استاندارد ISO/IEC 10118-3/Amd1:2006 مشخص شده است. ۹ مثال از محاسبه کد درهم‌ساز برای الگوریتم‌های MAC یک و دو، ارائه می‌شود. رشته‌های ورودی با شماره‌های ۱ تا ۹ در جدول ب-۱ گنجانده شده است. تنها ۵ مثال اول برای الگوریتم MAC سه، ارائه می‌شود.

در سرتاسر این پیوست به کدگذاری ASCII رشته داده‌ها ارجاع داده می‌شود؛ این کدگذاری معادل کدگذاری استفاده شده در استاندارد ISO/IEC 646 است.

جدول ب-۱ - رشته‌های ورودی برای مقادیر آزمون

شماره	رشته ورودی
۱	"" (رشته تهی)
۲	"a"
۳	"abc"
۴	"message digest"
۵	"abcdefghijklmnopqrstuvwxyz"
۶	"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"
۷	"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
۸	"1234567890" هشت بار تکرار می‌شود تا به ۸۰ نویسه برسد
۹	"a" یک میلیون بار تکرار می‌شود تا به یک میلیون نویسه برسد

دو مقدار کلید استفاده شده، به صورت رشته ۱۲۸ بیتی زیر است:

key 1 = `00112233445566778899AABBCCDDEEFF`

key 2 = `0123456789ABCDEFFEDCBA9876543210`.

ب-۲ الگوریتم MAC یک

برای مثال‌های این قسمت، مقدار $m = L_H /2$ انتخاب شده است، که برای توابع درهم‌ساز اختصاصی یک و سه، $m=$ ۸۰ و برای تابع درهم‌ساز اختصاصی دو، $m=$ ۶۴ است.

ب-۲-۱ تابع درهم‌ساز اختصاصی ۱ (RIPEMD-160)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
B7F4508111EB8C3B5229C6AED406DE9ECA640133	۱
BC78F55933BCEB1EE85A906F9E18374F23E310F9	۲
6300DC20E97A5AA29DB9C7D607D23D126FA36863	۳
3A2AC89B78EEAB8759F5112BCAD4CD405EEB5D35	۴
16DC174925BBC27E0C93D426C346846F97F8BC69	۵
E062210BA5C9C94737BF3A6E85B3B5664FBD1D4E	۶
9B462D5CBDAE1485FFE10BC001EF9E3AF6D128B5	۷
88E73A01A1DE36C92D6F9E41F7278D407B4A4CCD	۸
E7B128E4A1842B750F1E61A486C867C4887A4B21	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
B45D6CA84CFB9020E0D5ABA2A7609D3D81F3F57F	۱
8844375992037D1BCD0D118EE548D70C3F19CBBB	۲
917C59B8AC7FC19DC25BEF82766412FA16BBC6A7	۳
E0737CC7976D8F424390CB8798D623D751AFE15A	۴
D57FAE836870718EFA4BD4A5F2F322A179A8735E	۵
42B20D4C8FD5E8672760CF83C0478D7BF8021404	۶
42B20D4C8FD5E8672760CF83C0478D7BF8021404	۷
10441DF4F68CE8815818DC0FB370ABF87BCA4464	۸
E06AD21D2AF04DD4217AB03B1A578F036997D01A	۹

ب-۲-۲ تابع درهم‌ساز اختصاصی دو (RIPEMD-128)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
A47A64E9EDE0741B3FDDE33E5C1C6D78	۱
51355051852FDC79FB228EAC905633AD	۲
D83940DAFFBD4CBBE6BA30A6F9E63F5F	۳
1A7CFE2BB26E973E213C1CB96FA4C2EF	۴
798AEAC6046B31907C197BD68E59D376	۵
0B8E1D4A571F32657189E22A1F2F4A53	۶
B814730F482300C6E474FD255A66D680	۷
9060A30758EBE3368D939AC168F1A9FD	۸
20763FDEDF01E56FF5756954302C7DE0	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
35FA3AC39F50F2A4E3FFC7AF5776B4EB	۱
A89E25E6796747B630A2A00B802EA53E	۲
66339027A36608EBD932DD551616E7B2	۳
1F8779BAD84B50373931211A2761EAD3	۴
31BF5B5B7ABAC2567DC0E02F1C3A25D7	۵
B5B8BA3B8EA895FBC83CB7588FBD2656	۶
8D27BBEC257C848D5CF375EB5EDA4CC7	۷
B40B5BF6727DE90B26F770850F059C89	۸
76C7BC831B0BCE593DFD44E8E054A373	۹

ب-۲-۳ تابع درهم‌ساز اختصاصی سه (SHA-1)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
C8A8B3C75E6CE7C6C4F79CC19853CCD54ABCB079	۱
8DD9AE643BF10BBB7B978EF13EE6C0F480618FB0	۲
A738B26A8BD318184E76707A99CAE14C670B9711	۳
1EBFE413E55D6B288A2BD01D294A21FD8D4B20BF	۴
0CE7BF40A73D977AB4999CF3A9BD1C5BEDC442E9	۵
12A6823CC181294F95109073A6AA0C8961B14386	۶
9369EE4A043AF1CA6E078D0B8A9CE5C1545440BA	۷
B00D37D70A84B762FC0A8A9BC1B15F0E517B5EDF	۸
DDDF44613E8559D12C150D022D5FE33F9E0FBACE	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
C3A5ECD1E715C7272CFE78BC278086587B040422	۱
D5D50FFA7EFDF1B17E96E2EC14DBC4412F7B771F	۲
01BFDD568008D412158F5B0C90AE2730DCFB77FB	۳
9982E0EE91DB89AE7E7618AD1D649BA43406DBDD	۴
ACD04E1004FCE53DECA9EE7AB95DAF97B7C44AA8	۵
FADF62DCE789E86E60756AA819EF62C3E5C25E94	۶
46DB9A49FB4976D007B14B1574843D019CA99445	۷
4EF5BED3E816C530B23F491583C038596BB76FDB	۸
BAC6BE6BE6153FECE2891F9DA03824DD4D535D19	۹

ب-۲-۴ تابع درهم‌ساز اختصاصی چهار (SHA-256)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
76D91CA2337FF25EF66DF2AE7172626C5544428822B9E1B9C94121D384489C09	۱
479DA7965233CB2133C6B949AD82CBC5B29F528DB90FF04A1496323D77D15FFD	۲
BE6E923798F594BC529C87DF5A42333EE18BE88FED984B0EFE092BF31D570FAE	۳
664AA91CFF68C786E943FEB0E6BB465213FFC57AF5C8F973827DF67956FC21D6	۴
D7A7A1D1007CB2D3DC578BB4FDA4A5B1B2EBF7B27C9CC43BDF7A382851DF91AB	۵
BC9853B4E7AE574B3DCF4728BF44FC27A3C04C5AB90EA189DD175B6F5ECB4335	۶
66F3238A2C2B6A3AB86089B9DF33BA6420F7E66F5DE6856D79CCA908DFE57BFE	۷
B1A59E0905F8EE9ACF5C77E67883C8C3CA10DA965BE31F75A47AD85015CD478B	۸
15FC09FABB62AADEE831B9988E2DE2F41A3C685D28E4C06720ED6E8493CD060A	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
F0400A79DD136B4E83EB507E23F98C1A54E7DCA33A38C75902008F90B003C37A	۱
407FA9A8170113C1C0B06B8FDC32AB5914343D0CBEBEE5B1C84008182794CD8C	۲
7E02C2AB8B8115B446E80C70CE4A0126E83E0208420E39965272D6497EE16B86	۳
BEFC08E950BF7CD6B6BA0026A910328ACF45551DB93180099D0893C8415314F1	۴
00019D3C8D5D563A9A24462029171C6D4CF29BCF8CC6D60BF76584A6B4F696ED	۵
383F7B8050D7B08DEAEEB3B5B04496669815277968D5A2ACDEF04D37C596E2E7	۶
FFEE6E137909EF2140A87619B51CF6C7FBAFC6EF5B8388C8ACF0F7DE5AA8E7BB	۷
511855ADB1B5FE79C1C04B565CD40359B5DFA474AC52BE7F4CB2753285B90D0C	۸
8F6D5B1C7CC360DC4E4320755684B24726B8C4312A12B329ADC8C2550C3FEB08	۹

ب-۲-۵ تابع درهم‌ساز اختصاصی پنج (SHA-512)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
A4D628912D3CDA87D92F4597B7385E9BEB6161A2C12D412E3EAA7B4FD1003ABE D6EBE9C7418D60905267A84F0A2B22865D8E21F1E48D4E105F6C3A653D5C63E2	۱
DBBD9316AAE10399C742C212365A529B7EE5F9BBDB96BA9A14A078010AF81806 AF4635AADA77595FE21B7B5C552038AAE38CF32C4D4E480855560E98AC25297F	۲
C9598B319F5DA537044289553FB7B0FAC95B51569BD08DB4A45995CB75A344FE 88ABF5001694497ED71B5CAB3C5D4212E937E50712CCFAFF5C8B3D4C23EABDF5	۳
B22A1CD30D3AF351931E746542BEFAD2985BD6838831BDBCFEE3B9DA48AA8996 76C4ADF4278D79D45A6C6E4AEA613B5F3FDE4E6F4FE06854B9736B9355EE0A6B	۴
EC807431CE07B43F95E001B562525B0F49EC6BD5B91055C030D79D5E462008A8 B9D862ABD3E8517D59FE3F3E60424EFC1327D67D53A04F4871076999619D4327	۵
176422D10271BD8A22AFA4164F62439DEFAF0B4901AF4F8FD366C79055280635 175B8D920574AC85B493FBA1EFFDD46233C54BAEC783FF3030BADF6FB37413AD	۶
22E8A8624F3982CA3A7B18635E4029FB6CD3B771EAFF7BAD5A00C064C1099B99 7BCF7FA529D5864BEA94DA7EB5367D8C27763B7303FAD4F517D598AC7453A60A	۷
17A2D95A4935C88234EEBFBA29140B57ACECA329E513AA7BD7110283759FA6E6 D9457D4B58C7DE765A495703B04AA476E5412DDE52E799C841EAF37925A37CB3	۸
F807A843A14B94B977259556B656A7A401C3D026B5FDC993BC1E6A2E0E5AC7EC 7CAA611C9EB3F4609E7699F43A305BDC4818B823B219BE7AB5C54A4AC01F5E4B	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
14D4BDDF705DEFA756AE8154FA09792D1D86EF52A88E8552CA4DB56420F6BD08 0D3114F626B90B59EA1D0C7E4187678E22C263FE94D074D70477252CDDA86C04	۱
C340C2B6F8C606AD499747EC6239DF94D5365047061EB4A26789EB83177B002A 2F8C1F5B866A23389CAE742A057C4ECBDC7F7C20266BC99625A974DC345B0EE0	۲
AE0343C78F41BB04026B8BC36C7D09BDB7E6C8450FE340A7223274C5F61DBA14 5C776D694C3B05E8BEBB1A494607A00E363E21B3BCC7ADB5FAE52F20D4F2B210	۳
F98F58C4C7498F17A70FB5A86CA0D2AE86DA99E318CF0B8A801639A6DC7B3DB7 C57B975EA6347B55D68C6E8B34C185CB06972370B15EADBB4F35C8277AFB7D79	۴
7B073E2F13EB203BF937567D6A42F4F80A7BBD47E120226B2B1171C8F62BCC53 CC0DA4F0DD78C5534C1370E3DAEA81DD2EA6DF7EDD7BEE7334065A6A2B0A0FB8	۵
641BBAA2591C17B1D73435DE640A22FAC1A2C38D11BC025F6991ACF667096011 D6E48F27826F06BB006425DC4EBBE9EE7CDE3CF1C3A9592C674CCEEDA0F10BE4	۶
B0025F9B04BDD64D15AA61D0A5CF8CE5C1FC0A55830CF81FEAB1A3854D5D3E41 F111918913E9638292B9BF752C6B6F0626A322FC89C28E03C80816F5115C7753	۷
5E9A6219308123921A527502526DA57957E0C2C00601CA5224769DD925FC43F4 7FEAC4163B0D62CBCC7E4537859792DF8E4CCFEA4E8E3D387014A514F42B6CA3	۸
CDB9961A62447DAAEA3046E59517DFBAA8C7E51C7B45A4561918B8B5CFD3EF89 96B36921490049A70AA19CFAF88F017BDC03FC1CE419BAB718642186C17502FC	۹

ب-۲-۶ تابع درهم‌ساز اختصاصی شش (SHA-384)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
3148BD96B4CAB64EE95C6444EAE0053E783AC28949FE05D0 52A1FCCE7DB8A619A1D0BC858FAF013E53BD2A24AAEA03E8	۱
735E4ED128DDF2EEC1FDF0370BF32517DF63E836FC0CBBB9 A1C5CEFEC32CFB5586E2AA3A85ABD08FC6EB8EB9E777CB52	۲
15B7AF6E28E6AC436DB405B706078ED88F0F9D292C4C1A4A 5EF1FAF0BA315683439D0DFE325283C1C83DE846C23DA890	۳
F49C22A8E48D0B4C145EEFDDE51027248A2BCD341FE43504 4DC980C38333D5F197CE08BF26354C545690C805D6AB1E9F	۴
9DB498C5971A668857AD56C724F82104C2CC78D90701A29A E97D9D269180FC64E35E058CE8898927001D20BBFF3B472A	۵
3D782A279E1D683623EE34D9935D43D9627CF5D045DBEB7D FFF8C29CB3916A4F0FF00C012CE125956655873A3D883812	۶
3A9AFFFEBF68E5660606797A5BAFDBC2B47DE1DEDA40AC48 0F535583D9544A63210ACE4DA24F997786C2F80367FA5284	۷
0309E1B60798568E00522AC145ABB39AA19C5066549E07AA 5D6ADDEED34B4F2F3DF166C9C3915F44F92D79A049E7B753	۸
343CC7791B07C4D26E5735224B302C495D9CB2A92EA27BDB 2A96487C9CB3EC09D75C9E0179F73180E24D78000D45D8FD	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
FE10F454AD0EAA717123E77AF83760DA2B5F27AAB2BBE4D3 5C4AE1352D54CA36554EA206475F1BC5D24060CAF17E7432	۱
BCE4739807A7BD64F709605DBE1A2B572D963CFF5CAF557F 194F18CB924A6B90B2A54E3844701A77D459A64AB3142A1C	۲
86CD24861B303510FA374D2AA5E2CA78F329138D5B9C2E04 3C0FFC5E0AB37342B7859AE8B7CD8D6F3B1833F81628CA9E	۳
B03FC36C1FA2C72EF1EC1C9B8E9E322EA23C1A0F6C5AC5E9 AB2BA60D560D7156385D8D2DB0B117C71340E053DE4A08EA	۴
3B923573C9598E5F78EED06EADFCD6DAE2F8C762A8BBDFDE 8F0986934F5DD4A212B3493DD190E723A17B51D4F4F351AA	۵
0188E2DDA587AD67E91DD38C247051E1446CEDA39EDF33B0 DD9BFC4310BAFE41887638216955F6E31E683420D858D16B	۶
269010C8844FECCF00F3EC33E600DD6F1BA56DA91F1F1257 575BD5C5EBE6931F212CC8FDF81EA70C0CDCFBF20D06E84C	۷
92CF0571CD8AD78C1CD43E847837A849EC8B92CEAAEED5E7 541E23B14C4FF713A40C94D6A34E731543E1D3EC52B69BEA	۸
95FA93E72585717CA74701D46EF9E25A9E2FD10FE015CD8F 04427323315A60B074E1A1134F18B2154644658C24EB3D36	۹

ب-۲-۷ تابع درهم‌ساز اختصاصی هشت (SHA-224)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
065B86EDEE58E12C4D83C7AD1500EB4CD313DC3AA2147A12F39B7AFE	۱
73D5627C9DBDE736841766FE543B7954D59AEE1F5C6823BCE7E77351	۲
A4F4EA69DF69D9705D71305817B38AFE1EF6ECF724C3F6743B26A9D2	۳
E8E14D49D6C2A88D4A717A276693FF3D03444AC43FE02C99B6919A23	۴
38CB47CB00B57B858A0ABB864F05B8E83EE4A250A5794740796FAA05	۵
64ACE1CD852195AC765764DBA813749BDECB15498C30FB6CA73E0F71	۶
570E89F76E8435B945CF47AF5B054262C654636AEB955FD951076B91	۷
CCC8BDEED3869F5D8E2013EDFCE22A36185C5403103F04E586F987C5	۸
E0BEA67230DA03039540FA70CB0FBD69464E9DEE3C3FF80CD5D76646	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
FD5B8A7CD44B62730BF4DE82D7E2D70135E29FAEB1E66933D54BFF68	۱
E70AB63A4D92C3B2A6975BB24B9380B5320D7E510107D27CC97F0086	۲
36C19C58F5F13B43544424A085EB5E822AF4BD7F32B7AD190B5CA3BB	۳
DC53898B38F96269AAF0890A3A4D7E00B03B931C3AF7C80C8BBCF6EC	۴
446B9988D8C5B35A20DD6B71B5F1E3E048144CD082C801449B5497EA	۵
48E72C0EDC3E52370EF2DAE859A5462D60C735DA3F0B7494AFB0D5AB	۶
3E048D2F615BC681D1B2FD59A37F7D8972AE7C8096603B859F771223	۷
E2CC9DFD0A2945F8F2C3003ADD8AAA493BB0C72BFAA82B7CA8B1F289	۸
552A67693AB02EC7D0AF18075DA9875B8B5D1DB89F6CFC73EA7151DE	۹

ب-۲ الگوریتم MAC دو

برای مثال‌های این قسمت، مقدار $m=$ ۸۰ انتخاب شده است.

ب-۳-۱ تابع درهم‌ساز اختصاصی یک (RIPEMD-160)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
9EBEA41FBC24CD80BF2ECFD5B8C8CC8181D3FCAE	۱
75CB722C50024C0E8A7A0DBA7D5C36B86D9D1DD5	۲
5B48C1749DDED71EDFE0ADE2B944E808E4A65820	۳
F9033064567F541235C3944EE95CB476055985D1	۴
B37885405B71E025AF0CB574021A562A62733628	۵
5C6429B982C8054B5B3348A0D7D2CE24D7032BC1	۶
B0A4A451D0926855E52428E16D1FEAA241C4DD9B	۷
1CCEEC5122F08A76EBCD8E3DE88610D942D8A5F6	۸
45D61908BFF6039E6DE3C037FDCE6191F19F6410	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
2FDE5DAF7050D14E6D7ACD2254D17FA3A8CBFCDD	۱
239C4020610429A8662BF81A2CAAEA47F8EA0A44	۲
89EFFB9F5A6BCEAE3C65D0C9803F3464E5E9E349	۳
F5FC87FD5702F5D4E7BB634DA4CB4B41CD505B6C	۴
5686C00F69E6C868732C67402AA107CEAB513439	۵
525EC4893A221EFD9B6DD351059B40C05B4CE2D3	۶
B975ED3893FC8D535376EF49211E2E6B1BB30B90	۷
BC201FFA581357C271DAE25104167F3DCC97BADC	۸
95A875A1D64D55E677D8E4455E1445E7E940F758	۹

ب-۳-۲ تابع درهم‌ساز اختصاصی دو (RIPEMD-128)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
AD9DB2C1E22AF9AB5CA9DBE5A86F67DC	۱
3BF448C762DE00BCFA0310B11C0BDE4C	۲
F34EC0945F02B70B8603F89E1CE4C78C	۳
E8503A8AEC2289D82AA0D8D445A06BDD	۴
EE880B735CE3126065DE1699CC136199	۵
794DAF2E3BDEEA2538638A5CED154434	۶
3A06EEF165B23625247800BE23E232B6	۷
9A4F0159C0952DA43A8D466D46B0AF58	۸
19B1B3AF333B894DD86D09427116D0AD	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
8931EEEE56A6B257FD1AB5418183D826	۱
DBBCF169EA7419D5BA7BD8EB3673FF2D	۲
2C4CD07D3162D6A0E338004D6B6FBC9A	۳
75BFB25888F4BB77C77AE83AD0817447	۴
B1B5DC0FCB7258758855DD1840FCDCE4	۵
670D0F7A697B18F1A8AB7D2A2A00DBC1	۶
54E315FDB34A61C0475392E5C7852998	۷
AD04354D8AA2A623E72E3594EE3535C0	۸
6F9B1C0FC06753618D6DB4B007733795	۹

ب-۳-۳ تابع درهم‌ساز اختصاصی سه (SHA-1)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
86C2962E58B3498A2608935AF7726311F2BFB538	۱
0497FF21DAE3251DA0ED2F47F5A3B74ABA6B2560	۲
6EE2A25F943E3F3EC05225FBB86BA73E2E5D51D2	۳
CD4C0D1328DC4A8DC2801001B129AEFC6E0CF9CE	۴
89ECE303FAD1E4313950CC3B008CB239B5B85844	۵
9DF741057D075D3C4E1533E38A5FF469647194B4	۶
188A58390A6EF9827035B81CDF1B5069211F0EE5	۷
98A98D6A81FD361030856D2C19742AD8DBC468E7	۸
D2986310BA18A78786534882F9C6BCBF06CCE9E3	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
2739B6BE63F539EB70FE250346F6382A2DFA345F	۱
A0C2711A6B1DA4CD8F85EF1E6FF7BF70B412B477	۲
18F570E864FF903D2773D53C2E114E1A62152953	۳
A80845A89BA15E941A2457084BC431F3E47759E1	۴
14143EA1057B02D20C0157216190A006E30F3D41	۵
DAB4B41BA639B4715889406FE18E0C037017E063	۶
AEAEA5415B4F266CB15CBEB844E56AEC2DABAD6D	۷
3DBA11471EB4FCCF21BAEB0BFF7E20150132C6CF	۸
3BB917B8BD8560E89FF9054FBE096CBACA109D5F	۹

ب-۳-۴ تابع درهم‌ساز اختصاصی چهار (SHA-256)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
E8A06537F096CCF1A3C425A56CEA054072C4A8DB67BD28CFB02FBEAF84B35F6C	۱
DDABFDF46CE93311868B7275E05730AD3E23192A575CC291AE3785289B94A2F3	۲
02581EA39A6CF2D752793FD782CFB9CF965BE72B32B322C9551D03510645FB31	۳
1F12288F42F42661349E5DB741CE19F3B8C3A8149FD4B8981237FA200FEB104F	۴
EA4A04E76EEC57D6906098AFA7AE0264072C09F0DB34269B117C68C3ED989C5E	۵
6EB683218305A862A1C1EFBA04A2A62DC4EC27886D3C79AFF7C493C2D6DFB080	۶
6DC64AC5C5F197EB5463474AA6B329DA9D5B3C6A3324B147469E06F21EB53C41	۷
8F4B417527DA9533408D95951ED6504525C9683B45637B246CE25C99ACC64698	۸
5E2E0579A26517B06D2933CF62DEA20347A0A8DF9D7C3D200FA5E894ED9C5EDF	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
DCC3C81236AAD92043D1478DF7926E78205F7BBD0C3001854BF9087261ACCE47	۱
AEE154DCF83568248DC228C8C3513E9BEEA268B4979FF17CDE5BE484F4919DDA	۲
C3B53B9897D72197B240F08715E5C830886FE2F2EFC2E5A8ACD9D5405098863B	۳
60CD78CAED2CC9BD3F5BDA6AAA81596B55556660B19A2DF2FF6C48F89C52CD7E	۴
6283D8BA031EE52E2D7EBA96287025F161A5219EF1FB59CEBE6133007B35A146	۵
3BB625768D0900710F0EF7E854990BBBA35AA9B7BD4B0133656D290992A9BF79	۶
98FF69D0048FF552843CB8D5DC686EB2FEC3600D664A464F7B88F7289CC41A78	۷
5893F4AD6CEBB85BB90CD4107BF85EEEBAB621C6EEB4EC487780A45DED09F5B2	۸
781BFEC8396C6268E5413D76EDAE0C90E6592B624BB4E0FB6137F4DF33FB91D1	۹

ب-۳-۵ تابع درهم‌ساز اختصاصی پنج (SHA-512)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
EEB2E7DC1EA7C75966552A7F45C9F30E3FB9A7EA1362BA6D7324DD7DEF461F88 B2B5E433CD7CA25A08554605B0B020C3A865434BABFC140DE5D55C8A94C7FDC6	۱
8A507C281F9155A086C97E3BDB14B658F6C901B1948674139389853F55B453C4 83DF9AB807269B286AFD6FBDB6A59E3CF190BB61951D8A89BB0F3D611DC012DC	۲
F5B41F81B56D9CEF4BFFFBDD659470CA9DE7348A23DAC136790B028986D13E7D 74DC59759FAEA253D5342ABD56CF6F5859145AD54BCA62E0C45245B7E4FA5C53	۳
2EEC2E512FFDAC27444A563B40BFE9EAF594D0C83947A374AC82797DA811466E 8DF8380836446B4B392E4E815B8E84695DB8253230635C18CFEB19CBE1CF012B	۴
DCD40B28C684428F83D1E7D457A906DFCAB55C2298B7A242C4F208F205E948A1 BA081A39C6DF60E2279DE4C3D6F82A4490ACCD6679AAF7FEA90DE4BAE06F2C32	۵
E78F92E31D7410DD16EC830B477FE703B79925811758F0D3A11F3E4F48DA0C26 87A797EB2E3D7E20026936A87E6903F9D8C93EF3E8FECF2CB2A42A720F301821	۶
49BCFE57FA600FDF68562B91E686B02DE81DE25CF4466C707298538980880BFD 339264B48F2BD712127A1C66D97D1B367DDD8656B996CBD8D5B7EDD561328CD5	۷
C4979A98F32B6DCAC7718B6089694DBFC6E6ACDF82724F1EFFB277593B716389 ECEA6F4C40EA524C84A1324C6AFABB78C0FE0AA008C1EA3427AF179540FDFBF3	۸
376DD55BA616E59FCD6249267577608563C168CBF82CC6A89B83BC9224641B28 CC944C6DFEEDE8CCF7FC6F61FF0D322B3183449677330B6EBD83BDD7B57FB846	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
42A0B3DC6AF1D40CF4D58E2E35832C5824AA77E6B685B3E3BBBE69A82C726DD8 B46C861BBE0DADFA359207426187A1675A054CE82905F5A2FCE5495D6BBB6957	۱
DAED898D6A86AFD1C622C96D33521175690365330EA0CEEEDB85292F8BBADFD8 67A7C1327356DFD75FA0C38B099BD229C39CF7CF07F479308F52A5C29CD284DA	۲
41A98A3AD2B5BF46C000DEB754D93C2D41C4EFBE272163346E8D78A1FA222BD8 046551C4FFE81E8BA0A0DBD746A25066DBFAE79B4040D964D8F2DE181E71212D	۳
1296CD85141D1D3BAA6C52ED6A1569925112AAB7820883B3369D278A5711C62C F483045B5F4172841BC917BF92D45EAFC448D975FCAF58D95E8E9AFD127BB7A6	۴
C0941AAEA51B8539592403C1CCBB98736F470F5F07C2FBB2374CEFDDE6BF0A34 EAA164B430B59E6921422D6E0C5BEA969FB9F6A7381AC9A8E0107D5BBDD11E3A	۵
B87B9328C0041DC4492C5F0AA613EBDC9E1D01156E4E0628705A27B3DCB6EEEC 20E862DA7971DC2B999B6C6952ADB7D8615E68384289076C4B752D0DF393F2E3	۶
CB102567BDB4AAB8833419ED3BB95F1875488439B5416FDD466B79CC73BD26E0 9690A3E94CF611D7532128224E225C671B50FC2BED4934516A4955931774B30E	۷
41B7CD308733F10CCCC0AE5CAD8AF9E0740317A0EE874489872EC640CC0CB16F 101A12E446F55585555E7AB5128B8D370C006FFA151C7FA35EE10144E1FDD16B	۸
2FFE4FEF445D76A2A41E5EDB715170D02ACAC44A580144C17ED65434A876CC99 568E39E97CE78E5325EE376B113C6D7C5247D96AA0DC1D91A0932C81B58D956F	۹

ب-۳-۶ تابع درهم‌ساز اختصاصی شش (SHA-384)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
7BEE4557700A1D8ECE045E8A6FC980F456D2FF4F5AA77BEA 3147F54DC77E8F6A2FA016E9BAA4E105D53B4631CE088CBE	۱
33B764BFC7E4A95BB432BD7766C3EB0F0AB686CAC8FD40CD A53A0B0D623D48373F36B321412C4D01E4AAF8BA53C77751	۲
67BF47CD4B410564245D335985B5DD404D085E2DB88F2A35 B0782C7FA4AEF3407D489D66EA8914E74752CD1913963139	۳
1522B5D65022C1CEBF2425EC914320CCDBE198251CFEA79F 499179A2025185B5CE6241E84A6FF0F9C83820FA83597E62	۴
98E3EA52031575D96489C7DB7AE3B4A4AE7D80E789958CE7 99350E2E07D7B852FC8BB3EFF3F2954A2C158BC3C70E8ED1	۵
34B80B9F2775DABB019819277302ADAEEC0CA6F0963B2979 314A44724B6318D9213DDFFA2E04B175E1E7D6778FC8A8A5	۶
5BF44F677E77FBEBE31516D80CED014DC99E7F51AC4CC41F 6401292990E3668319B137C2F1626C67BB92A1CED7BE15AA	۷
7A8610621AB18CA0C87AD25A984C333D3B4BE12E85DEB8E3 88E4656133115FD4710DF4B81D0A526E56553C25E6279131	۸
63490CBECD7350ACD6D9D5F485D323440A271555CC3C1E51 F245E0FE4D8DFE6340C6146D2EEB46DFF90A0D1970A30C52	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
6760086DFFB66B3AA619569BF567D6ACEFD52E2F3D90CC40 103346CB1EE0A493E159785876F8C310B44BF05B64E6B2FF	۱
6575DC9AF2E0A9D32D619465C95FED1FF5B1D3E65A2EAD93 405BD2DA82896EE3F9D336B374E5D015594EC44872EBF8C2	۲
A6685B72C7545F84405CF20CF17CB67B246FA914C59F335E 7F95B5B11963072777FA3B635AABF86D0D75B83D6365211D	۳
0D52B84209956EFD9F39DE27821D328CB0B3FCDEFCF64B99 ED2B65C4DE7A753BCA2361CBB26043649FDFCD8C757E700C	۴
9A50FF272D08AB3AD03911B4FB042E0CB8080C18F5938F0C 93340DA508722DBB799C72EA1274B67AD30EAE22E86213B3	۵
21BC7FA9F9E23536084CB65EE28727DDD378A1FD6D316D29 BFC3C8A39851EDE817A392D460A628E79A018989249A0CC0	۶
F291C145D2F9A10C76C5E40CD4C4027E2688799C95FE4C45 3042DED3EEE4C4331CDC5F571B8642C615DA2A1A854C6EA4	۷
23A9161DE7B21284446B49D5038F0D2823A0F05619B243F3 D0E114E3AA9AC905C506A9546E9EEB41F1DD1ABCE8F43B71	۸
D056C9491A84401387A18E6953C7157E86C3AD4D3E2B0971 5E91B486EE89C7FE17CE40A10C78EF819433F006F7779443	۹

ب-۳-۷ تابع درهم‌ساز اختصاصی هفت (WHIRLPOOL)

key 1 = 00112233445566778899AABBCCDDEEFF				
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین				شماره
5A77B599D2DB9B6B 47556A7EC5191745	8C8E5112DD5F0B88 4AAD7C63F5F9A7A9	719D60A4866688C2 439C7887DDD47DBF	DFF624A6EA4ADB62 E45B0A68ABE62A40	۱
177B98F9F215046E CCE9FDDCD3853303	640B8EFE3E723C4E B84821F0B070296C	7233C5E745B72DE9 EC039B7C86432B34	381D6A3F47E30F95 90520D5FB2585A19	۲
F92ECF9FB82E39EC 61D32FA9C99DCBC9	B2D3EC8CFEF76317 A7FF32E7643F6B00	A8C4E6F835BD4994 8B8D1510FB2A95D9	D4D156B68F640D37 A1AEC1CC15508634	۳
078067C14C1E3930 ECB7BA5D3225B39D	11BFE58E1E94F03F EE3B63A616368829	9062DA01378760A6 02EB3B4999CB227B	5F7BE1FF041B8087 60F1613C174DBBD3	۴
05411A95D2A5CDA0 C37973E0FE0EFCB1	CB4A7339A70E62FF 5F68EB1E06AA4E3C	790D945F25963F15 F15DEFA7E2A4A129	95E39486BAD88B2F B18F4C5C8B300B63	۵
8E2A8C15E9611E57 653C4CA5CD6FC863	5BF67165B38B0425 E6A6E0CFDAD1F5B7	9A30C8C15F9DE729 60E657B5365ADA57	97391B32575D9C78 04BA92ED92277DDF	۶
9A7D93D28BA451CD C2528ABA3661909A	E57570C1CC41E943 91044C6C1C8EA914	D288F3FD112C7E32 2F1FCFB07CE394A9	22185F2163AE9328 C0F31862B5A2328B	۷
A3676A07D9E79CAB D08E538430F7A050	DAA1DA6EAB3FBAD1 2E3504C51A5B2449	28114F4D7E00050A 2BE90403BA08B1A3	B7167400203585B6 D7C1E9E8B70B50E5	۸
521EA57548F1068E B6D4A01127D67966	C0364330ABEEAC85 157DEC38F1D77A35	9E008D976323B1BA 361BACDA62E506C4	13ECFB405E0909EB 59DE28298AEC9CCE	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210				
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین				شماره
FDB6120AFEDAEB87 C29A8B3524BA23F3	A4DDC952FE02C1EC 512765C83734D2A2	B17DDD6647D0FAB6 6D65139B49FE5A0D	7194CAA506EED1DB 8682E868353DA04B	۱
8B738011A43BD813 66D15236D52C5FF7	63C38B941E81975B 35CAA40ED5A49561	C2562EC9185B70B5 D57A5FB202386A21	503D34FEA89B0E3B E226335C78928E0D	۲
C97109474261CEDB 16D1F15A20C9844E	4FE524CE8319BD1E AEAE04EBA11D6D67	4FAD2DCA54348400 F1405C58A1779C5C	30238EB26812644D 0E4C2D6C42E7252A	۳
A320497D440E9452 FCE87CB6215E5ADD	846B80EFD4578628 711D76EF1C0573CD	ACD969D64A6EC42E D5C6E1F133F31472	F350F05BE6F604E8 776D37CE86E9B369	۴
E1C734A8E6301FD2 1B29C21F864E60AB	70655F5E6DACCE51 49FA8143BE4CF0F0	15083D3DA974D411 F12622BA4C6E2325	82C219F74F357E48 D09BDA7F634518BB	۵
66E060BF156AEC45 236D7C34E465105D	4058E4D4A88A0DA8 5AD7C6D7206801CE	8FAD6D118D5B7310 CC20CB08109486F6	60FA0BB68B673DDB 0E6B48FEAC3D5B77	۶
608FB970FD10D1BB DC7313D3D2C5FEC0	CEAEE1FA02E44C06 32A3DCA366CF7FBF	2F1711A214E2594B B0EBE2504F2C749C	E57A71FCC419042F D89E914D87292F11	۷
D3B314AD10D07CC4 CBB66497472C2E50	5708D35526B165A8 A91EE7705695D1AC	9B5AE596D24ABEAC 0750F2237CD78E8C	FCD3C0EF2DCCF196 D01C9891429CA501	۸
024F0B3B7A403417 1B0F8AFBC605AD78	B8191F8383DFFE55 3F5BE4F1D2B19C51	F23F5B1A29E3FC24 CEA40F91A5239B70	BB29097E294FE798 4A65ABF1DB054FC9	۹

ب-۳-۸ تابع درهم‌ساز اختصاصی هشت(SHA-224)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
B5BC4C46AE5F4E335792CE51304F986D3DD6EAB862933AB3EE7DB5D7	۱
63C3DB8305A361388FC52CF4567521303ADA68C31A6FA0638113D594	۲
B176AB2549522FD0B93EE32B99BD43C00388DF17FE2B827CE91FD603	۳
CD676B859E48A06EC59AE4BF8F341997D9E9FDBA4922ABC983D787A1	۴
4CA41164F2AC8F994CA036C8FF516142EED491D82FA6A9C51B44F817	۵
3BC5924DA588B993389429D0146FCCD64320CB69E1057C16CDA57AE1	۶
184AD4D6C9B1C5BC8FE7D4184C20F724E66C4F158DB41E3025B022D2	۷
39FC2867E4979919B1EE5A03D1B15571D69BABA4FED9891D9F97FBF1	۸
63859486E22F8C2E90E5F5BF510E732543414F6FB731B0A8E9807249	۹

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
13247FB84F20471BEC77D777E9648D2C2C4C7B7E132782FC3D1262A4	۱
F07713FCB295F3C9997E823B63D0C0B2170D7A6EF533E0F93076D235	۲
6F072241CED9E423F04B10F89D656CE36AC7AA6027CB22A6E1216A42	۳
9582A2C75DECBCD7E5378D583559B33F74AC61A4A3CF5AA25CD6E3A0	۴
47CA643A560DD0A7D06E86218A7E80256CA87FE6A29CCD2081F40EC4	۵
02358052E6DF1510771267593C2682814A8E4362E6DF0BDEB59D4DDD	۶
B08BCB38E974C3972451DA9805C977DF001CEA225FE3D8EA105938AE	۷
EB50337CE04D4131ABF837780BBBD9674473EA029A08E774F1DC6876	۸
6774049ADA46BCC6AD6BCAE615404A22704885B0627F1BDD74D2F8DA	۹

ب-۴ الگوریتم MAC سه

برای مثال‌های این قسمت، مقدار $m = L_H/2$ انتخاب شده است، که برای توابع درهم‌ساز یک و سه، $m=$ ۸۰ و برای تابع درهم‌ساز اختصاصی دو، $m=$ ۶۴ است.

ب-۴-۱ تابع درهم‌ساز اختصاصی یک (RIPEMD-160)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
6606EF2D3BBD010F516C65372C3CF0ACF111B3F7	۱
F0BC0C81307E17A71F4C40AE0B2AC39FCB23CE12	۲
7720FD23925B854F963E8812573CD86EBA61EB66	۳
2683D6CE053BA0420E76130EAE2367734B7D2D53	۴
DE532D156CBE12464BB6147E99470C471D91F1C6	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
4BD390E9EC460AD4866CCB32D091AFBF73E5B6DA	۱
CD2847BAB4636C9BCEADCF3D187122A9199DA670	۲
15C3910C42638E5EE6DEBD506BD8C4DB94713A3A	۳
04148DCB47728E3E57B836A66043D5145879796E	۴
829A24010704DBD0EE34A6D607F7B34829E04E95	۵

ب-۴-۲ تابع درهم‌ساز اختصاصی دو (RIPEMD-128)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
aeb2c45f13c0c6f5f10be2f1e3e9c322	۱
16874d0e17e4f1c290dd749cceff7834	۲
a289aa06aeb8fc99b989c377baadd9d4	۳
0d80db68bbf99442dc3d6b83d038def3	۴
11dc4a6bd375c64f78bb78ad265ed7cd	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۶۴ بیتی: ۶۴ بیت سمت چپ‌ترین	**شماره**
7248481816b8d3af29f5c002ff769ea5	۱
dfe1e36ce9792476e0889f1becef18a9	۲
9b4f1d21320f4a327f023947554bfc3b	۳
3d2d658d0196e4339f42ada50dfcfa6f	۴
0a34452d9da70c70183dffddb8eec056	۵

ب-۴-۳ تابع درهم‌ساز اختصاصی سه (SHA-1)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
708F4A226CDE708820643CBEEFDCBE6CB36FB269	۱
EAB87BE709D1E5CB62C7489C2B1407130B772760	۲
C1BD6F9C908132FEF5187CBE681B42A8C785FBF6	۳
F34DEB241D46C6448D67ACE6B8CD4DF00DA23EBC	۴
669DED2BD6A1AE0BCFF7D3B74494C1D8161FA0D8	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
EAF6F9DDBAFD299320FF0FC8E02E2BE62879F341	۱
2AAE9DE0A555E7CD7383C27506A467B8DF4E3A33	۲
FE6031710329D12090F73F55CFFCC6215F9BEAE9	۳
0CCDD9DAB6B0126800EC1CC7A02656E12EDEA42C	۴
ABDBC8AAAE4A8CE734432188740A149BDF2D215F	۵

ب-۴-۴ تابع درهم‌ساز اختصاصی چهار (SHA-256)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
B5FA90A26AC41FF4260BC38142032D5745C2635AEE274846DDAAAAB27ED9E77D	۱
3859B97FEF3B4FFF77813AA8E9310BFBB5A015D03564557EFAF3AAFA2888E830	۲
8800151E003F4956B4F351862587FCC40DF84D3EC691459DA9E6A8E55E8C3F60	۳
5708BD75C1B763B6ACE40E91E1B165C33ECB3EEA3D63B95FD31D895FBF6D46E9	۴
3865F84EE189730BB4FC387D42F8A86281DBE3687341C83BB7A5ED362D8094FE	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
5977BDB720997D17297835A553017D478A7F514990215A73A661089A9C5ABC7D	۱
E5C2A8C6328E749FAB5E983FCC9D213CB968B2CBFC8634A28DE38C17336DE017	۲
CBE66212BD2BF930C303399B2836C8A246FAFF28D34C2B389C6A16DD7F101A48	۳
6F7C08BA9AB6BFC73C157B55EEB892F11819B09915818F5B515E1486CB0167E0	۴
F519F962E848583855E2FAEFC5D89238B53126719CD62792FE1BA0039C51B3D3	۵

ب-۴-۵ تابع درهم‌ساز اختصاصی ۵ (SHA-512)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
CE19A0FCC29F1AB31C204973AC0BCF4AB1A044E187423DC5774C1EBA4D87450A 62FABB4ADC2F6FA8C37B1AF79D249967E89CDF9328312F3B077B9E408481DD06	۱
BB06A4991397163DC273F94F871BF4B61E1001ED9BEDD6E6282484464F7F60A6 FEAD67F105FFEC40AB367DB98DA8AB72E3EFF4CDE8ED61B64B2CAAB8278D32A3	۲
0FEA25FBC2C95D3D73EF4972FC2EE17D51F0CB354D3677BBBE41DBA70B78DB32 F11BAAB1C9A6BDFD22A60615929600C5594CC58798F979EEED931F21F4F6765D	۳
B38B47605771DC1F34DF203239C111BC44BFCC182A338259BBD89D6A468458DA AB551BFFC15F3681C3D3C3882669D441371427A1FF6BF25F08093AB399391F32	۴
AC2171E8EBC170C7C7556FEA4E4786DE7DCD8FF80A3C8C701E752ACA0BFDF478 C6A8F90C4D57275D97CF8E23F2F7BBC15847EB49666A63FD4F52B3EB9014F0AD	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
286800D1661857CE3DE713777E0302303A04C6DB6CA5D8D880DBA5328B498CBC 2A0F3353AADA7AD6DF456DF5FB08C067819BB0A29C46EEF7BB91E86DD85217F0	۱
758512264E54DD20394B5E90228FDD8BDC159D4F4F04B4AECC1CD51DCA88DD62 4F364B98B031A4175E2D896D883E1F280A6A27E005A6F7CB764A37676C231A62	۲
ADCC88C406F7118E6BC673FE38D7D16E42A7373892050044676BEDFAFA4CD23F 11B4253C6B4A1965EB8044E277962FE38A848CDE27C8AA84E2583A6F6A6C8EFB	۳
A18E3AF76F7D24AE7220A3DC9616675301025C007753BBFB7E6785D107DE656B 62DDEA8D58B03AF290C82E9C8429FB1DB45FE684D114E5D4FF1560B0495005B8	۴
988DF21325F32F1F4BB9C9F4DABDF9989CA976D5626C67FFEA7820060FFB3AE2 233A91F0E9AA99D82A41434CAB5A2B662D97353D22A12164A21A5492CCBD1C3A	۵

ب-۴-۶ تابع درهم‌ساز اختصاصی ۶ (SHA-384)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
20425431D9A664F039928CAEF044869B0FA02BD8D19504BE CE96A79318708202A92B4FB3ACF24BD0236EDFB7CE31C8FC	۱
75A2FB6690CA619F9A99704A1F94E7737E8FE9C0697AAC22 9DACC85F651CE67324E64E22095ED0A6182D1FB147EDD58E	۲
89CDF73409FC87BEE998DDFEE1B87C0903F92313D950BB2C B692CED9DFAE48AA50D8B43454469D84AFCF39EFFFC12669	۳
A5BE64C72729F20E8A429BD75002EE2B71769FAF8B114078 D2676002B04A8F04D4A4509A89EFA1D54B38846C23037336	۴
9ADE9EA42AD6C130931B1A56C771EA76EEF2D0E8217E413D 26D1E2881C8E20494F48236DB922B500194E164EE7D43376	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
BE7105BE54B7317D28B2F42122B37AC16042AD2EC2154765 CA08E95A8FC51CE4623B11CC770AB72CD835D4772DA97B6A	۱
CD1E2677F344EABB86D6818BC3F6A2B4D91ED101510E7940 058A4434BFD62E7B2D2D44A4CEFC4850850B6E025FC7E224	۲
AAA67DFDD03B318FE45C76ACD53DB05DA702CDFFF34B8E86 E241738B1D32AD551D9EBFCF402342EA875E48FECA6D59F3	۳
0E631958684F926D29494EF311440F34EB2B333A4CC62AC4 DCE7BF00F776DC37602EFF6DD09302DF58EA3DCA96EB30F5	۴
2D61AFADF130A8B67BD7D3163D2C4CCC8678A59594CDCC01 E33C7F1F5AEC71B8C7CC20736ADDAD7E7E9FC9DEDDEC5338	۵

ب-۴-۷ تابع درهم‌ساز اختصاصی ۸ (SHA-224)

key 1 = 00112233445566778899AABBCCDDEEFF	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
2E47E46A24AB4E7DF363DCC7A418B27F0DE8D8FB63183AA2CACC34BB	۱
BDE7A7F350661ABA5585F0B32C430874D12637E4AE7D2164AA112A6D	۲
073B15C8448DF8D65A0BC23546BF02C3A527884297DD2519BA170791	۳
18A89EC81098140110E97905BBCC072311929A19DD214118AB636702	۴
E7D1F07468AEFE9DC2E5AD9549523213F25043845A3CEA3E9E6A10C6	۵

key 2 = 0123456789ABCDEFFEDCBA9876543210	
نتیجه MAC ۸۰ بیتی: ۸۰ بیت سمت چپ‌ترین	**شماره**
559000BB6220FEF550B35EE119EA561CC4C393F03BB52E9267DE560D	۱
3CFF9B831C517828ADDBFAB6228BE80A1346F905BE32D109E34110FA	۲
73774106EA714A5CBD6682D83A6832E80C788E209174807F3273D8F5	۳
CF69464136119BD6B0E8C0D7037214F1CD61FA1EBBAF4BDFA4BDFAC3	۴
9517EEF881B9D989C402836D84AEDCF93037E70B6AEBEC1D4E311B37	۵

پیوست پ
(اطلاعاتی)
تحلیل امنیتی الگوریتم‌های MAC

این پیوست در مورد سطح امنیتی الگوریتم‌های MAC در این استاندارد به بحث می‌پردازد. هدف آن کمک به کاربران این استاندارد در انتخاب یکی از سازوکارها و مقادیر پارامترها است.

در این پیوست، $\mathrm{MAC}_K(D)$ بیانگر MAC محاسبه شده برای رشته D با استفاده از کلید K الگوریتم MAC است.

به منظور تعیین سطح امنیتی الگوریتم MAC، دو راهبرد حمله در نظر گرفته شده است:

حمله جعل[1]: این حمله شامل پیش بینی مقدار $\mathrm{MAC}_K(D)$ برای رشته داده‌ای D بدون داشتن آگاهی اولیه نسبت به K است. اگر مهاجم این را برای رشته داده‌ای منفرد انجام دهد، می‌توان گفت او قادر به جعل است. حمله‌های عملی اغلب نیاز به جعل قابل درستی‌سنجی دارد، یعنی این‌که MAC جعل شده از قبل با احتمال نزدیک به ۱ صحیح تشخیص داده شده است. علاوه بر این، در بسیاری از کاربردها رشته داده‌ای قالب ویژه‌ای دارد که محدودیت‌های اضافی به رشته داده‌ای D تحمیل می‌کند.

حمله بازیابی کلید[2]: این حمله شامل یافتن کلید K الگوریتم MAC از بین تعدادی زوج رشته داده‌ای/ MAC است.

امکان پذیری حمله بستگی به تعداد زوج‌ها MAC / رشته داده مورد نیاز شناخته شده و انتخاب شده و تعداد رمزبندی‌های خارج از خط دارد.

حمله‌های احتمالی علیه الگوریتم‌های MAC در زیر شرح داده شده است، هیچ‌گونه تضمینی در مورد این که این فهرست جامع باشد، وجود ندارد. دو حمله اول عمومی هستند، یعنی در مورد هر الگوریتم MAC اعمال می‌شوند. حمله بعدی به هر الگوریتم MAC تکرار شده اعمال می‌شود (برای جزییات بیشتر به [۹] مراجعه شود).

حدس زدن MAC: این حمله، جعلی است که قابل درستی سنجی نیست و بیشینه احتمال موفقیت ($۱/۲^m$، $۱/۲^k$) را دارد. این حمله به کلیه الگوریتم های MAC اعمال می‌شود، و تنها می‌توان با یک انتخاب آگاهانه m و K مانع از آن شد.

1 - Forgery attack
2 - Key recovery attack

بازیابی کلید با جستجوی فراگیر[1]: توصیه می‌شود این حمله به متوسط ۲^{k-1} عملیات نیاز داشته باشد؛ درستی‌سنجی چنین حمله‌ای نیاز به حدود k/m زوج MAC / رشته داده دارد. مجدد این حمله به کلیه الگوریتم‌های MAC اعمال می‌شود. با انتخاب آگاهانه مقدار k می‌توان مانع از آن شد. به طور متناوب، می‌توان از به دست آوردن k/m زوج MAC / رشته داده که برای شناسایی کلید به صورت یکتا ضروری است، جلوگیری کرد. برای مثال، اگر k=۱۲۸ و m=۶۴ باشد به طور تقریبی $۲^{۶۴}$ کلید مرتبط با زوج MAC / رشته داده هستند؛ اگر کلید متفاوتی برای محاسبه هر MAC به کار برده شود، بازیابی کلید با جستجوی فراگیر موثرتر از حدس زدن مقدار MAC نخواهد بود.

جعل روز تولد[2]**[۹]**: اگر دشمن نسبت به تعداد زیادی از زوج‌های MAC / رشته داده، اطلاع دارد، او انتظار دارد دو رشته داده‌ای D' و D را طوری که $\mathrm{MAC}_K(D) = \mathrm{MAC}_K(D')$ است و مقادیر ورودی تبدیل خروجی در محاسبات برابر هستند، پیدا کند. و این کار به عنوان یک برخورد داخلی[3] نامیده می‌شود. اگر D و D' برخورد داخلی را شکل دهند، برای هر رشته Y، $\mathrm{MAC}_K(D||Y) = \mathrm{MAC}_K(D'||Y)$ است. این کار امکان جعل روی یک رشته داده‌ای انتخاب شده را فراهم می‌کند زیرا یک مهاجم می‌تواند MAC را برای $D'||Y$ بعد از مشاهده MAC مربوط به $D||Y$ پیش بینی کند. این جعل در مورد رشته‌های داده‌ای شکل ویژه‌ای است، که ممکن است به عنوان یک نگرانی برای کلیه کاربردها نباشد. ولی بهتر است در نظر داشت که این حمله گستردگی داشته و به انعطاف پذیری بزرگ‌تری در رشته‌های داده‌ای اجازه می‌دهد. حمله نیازمند انتخاب یک رشته داده‌ای، و به طور تقریبی $۲^{n/2}$ رشته‌های داده‌ای شناخته شده و ۲^{n-m} رشته‌های داده‌ای انتخاب شده است.

با اضافه کردن یک بستک دارای شماره سری به رشته داده‌ای و تکمیل وضعیت کردن محاسبه MAC می‌توان از حمله جعل روز تولد جلوگیری کرد. این بدین معناست که پیاده‌سازی باید تضمین کند که هر شماره سری یک بار برای محاسبه MAC در طول عمر کلید مورد استفاده قرار می‌گیرد. این موضوع در همه محیط‌ها امکان پذیر نیست.

بازیابی کلید میانبر[4]: برخی از الگوریتم‌های MAC به طور بالقوه نسبت به حملات بر اساس برخورد داخلی آسیب پذیر هستند. هیچ گونه حمله میانبر برای الگوریتم‌های MAC توضیح داده شده در این استاندارد، گزارش نشده است.

اثبات‌های امنیت

ثابت شده است که الگوریتم MAC یک، در صورت داشتن فرضیات زیر امن است:

---

1 - Brute force
2 - Birthday forgery
3 - Internal collision
4 - Shortcut

- تابع گردکننده $\emptyset$ توسط مقدار اولیه IV کلید خورده و به وسیله ثابت اضافه شده یک تابع شبه تصادفی است.

یادآوری- یک تابع شبه تصادفی تابعی است با کلید پنهان که برای کسانی که شناختی از آن ندارند به عنوان تابع تصادفی ظاهر می‌شود (یعنی تشخیص آن از تابع تصادفی دشوار است).

ثابت شده است که الگوریتم MAC دو، در صورت داشتن فرضیات زیر امن است[۶]:

- تابع گردکننده $\emptyset$ که توسط مقدار اولیه IV کلید خورده است، یک الگوریتم MAC قوی است. (یعنی پیش بینی خروجی آن دشوار است)

امنیت الگوریتم MAC سه، مشابه فرضیات ایجاد شده برای تابع گردکننده $\emptyset$ جهت ثابت کردن امنیت الگوریتم‌های MAC یک و دو است.

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۱-۹۷۹۷: سال ۱۳۹۰، فناوری اطلاعات -فنون امنیتی -کدهای احراز هویت پیام (MAC) قسمت ۱- ساز و کارهای استفاده از رمز گذاری بلوکی

[۲] استاندارد ملی ایران شماره ۶-۱۰۱۸۱: سال ۱۳۸۸، فن آوری اطلاعات - اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز- چارچوب کاری تمامیت

[3] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[4] ISO/IEC 646:1991, Information technology — ISO 7-bit coded character set for information interchange

[5] ISO/IEC 10118-1:2000, Information technology — Security techniques — Hash-functions — Part 1:General

[6] BELLARE, M. "New proofs for NMAC and HMAC: Security without Collision-Resistance," Advances in Cryptology, Proceedings Crypto'06, LNCS 4117, C. Dwork, Ed., Springer-Verlag, 2006, pp. 602-619

[7] BELLARE, M., CANETTI, R., KRAWCZYK, H. "Keying hash functions for message authentication",Advances in Cryptology, Proceedings Crypto'96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 1-15

[8] BELLARE, M. CANETTI, R., KRAWCZYK, H. "Pseudorandom functions revisited: The cascade construction and its concrete security," Proc. 37th Annual Symposium on the Foundations of Computer Science, IEEE, 1996, pp. 514-523. Full version via http://www-cse.ucsd.edu/users/mihir

[9] PRENEEL, B. VAN OORSCHOT, P.C. "MDx-MAC and building fast MACs from hash functions," Advances in Cryptology, Proceedings Crypto'95, LNCS 963, D. Coppersmith, Ed., Springer-Verlag, 1995 ,pp. 1-14

[10] ISO/IEC 18032, Information technology — Security techniques — Prime number generation