INSO

18914

1st.Edition

2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۸۹۱۴
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیتی- رمزگذاری اصالت‌سنجی‌شده

Information technology — Security techniques — Authenticated Encryption

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به‌موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه 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 به‌موجب 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 حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیردولتی حاصل می‌شود .پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع 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 به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته‌شده 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 بین‌المللی استاندارد (ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی‌شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. هم‌چنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی 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- رمزگذاری اصالت سنجی‌شده»

رئیس:	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق‌لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق‌لیسانس مدیریت)	کارشناس مخابرات ایران
سجادیه، علیرضا (فوق‌لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سراج زاده، هادی (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
طی نیا، رضا (فوق‌لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق‌لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
قسمتی، سیمین (فوق‌لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
مغانی، مهدی (فوق‌لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی

نیسی مینایی، آصف
(فوق‌لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

پیش گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- رمزگذاری اصالت‌سنجی شده» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده است و در سیصد و پنجاه و پنجمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۰/۲۷ مورد تصویب قرارگرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن‌ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود .

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

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

ISO/IEC 19772:2009 + cor 1:2014, Information technology — Security techniques — Authenticated encryption.

مقدمه

لازم است زمانی که داده در حین ارسال از مکانی به مکان دیگر فرستاده می‌شود، به طریقی محافظت شود، به طور مثال در مقابل شنود[1] یا دست‌کاری غیرمجاز. به طور مشابه زمانی که داده در محیطی نگهداری می‌شود که امکان دسترسی طرف‌های غیرمجاز به آن هست، ممکن است نیاز به محافظت از آن باشد.

اگر نیاز به محافظت از محرمانگی داده مثلاً در مقابل شنود است، یکی از راه‌کارها استفاده از رمزگذاری است که در استاندارد ISO/IEC 18033[2] و استاندارد ISO/IEC 10116[3] مشخص شده است. هم‌چنین اگر نیاز به محافظت از داده در مقابل دست‌کاری باشد، یعنی محافظت از یکپارچگی، آنگاه کدهای اصالت‌سنجی پیام (MACs)[4] مشخص‌شده در استاندارد ISO/IEC 9797، یا امضای رقمی که در استانداردهای ISO/IEC 9796 و ISO/IEC 1488 می‌توانند استفاده شوند. اگر نیاز به محافظت از محرمانگی و یکپارچگی باشد، یکی از راه‌های ممکن استفاده از هردو روش رمزگذاری و MAC یا امضا است. اگرچه این‌گونه عملیات می‌تواند به روش‌های بسیاری ترکیب شوند، تمام ترکیب‌های این سازوکارها تضمین امنیت یکسانی را فراهم نمی‌کنند. در نتیجه بهتر است به طور دقیق مشخص شود که چگونه سازوکارهای یکپارچگی و محرمانگی برای ایجاد سطح بهینه‌ای از امنیت باید با یکدیگر ترکیب شوند. به‌علاوه در بعضی از موارد تعریف روشی منفرد برای پردازش داده با هدف به‌دست آوردن محرمانگی و یکپارچگی، می‌تواند بهبود کارایی قابل‌ملاحظه‌ای را فراهم کند.

در این استاندارد سازوکارهای رمزگذاری اصالت‌سنجی شده تعریف شده‌اند. این سازوکارها روش‌هایی برای پردازش داده به‌منظور محافظت از یکپارچگی و محرمانگی هستند. این سازوکارها به طور عمومی شامل ترکیبی مشخص از محاسبه MAC و رمزگذاری داده، یا استفاده از الگوریتم‌های رمزگذاری داده به روشی خاص که هم یکپارچگی و هم محرمانگی را فراهم می‌کنند، هستند.

روش‌های مشخص‌شده در این استاندارد برای بیشینه ساختن سطح امنیت و فراهم‌سازی پردازش کارآمد داده طراحی شده‌اند. بعضی از فنونی که اینجا تعریف شده‌اند دارای اثبات امنیت[5] ریاضیاتی هستند، یعنی دلایلی قوی که از صحت آن‌ها پشتیبانی می‌کنند.

1- Eavesdropping

۲- استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال: ۱۳۸۷ با منبع ISO/IEC 18033:2005 موجود است.

۳- استاندارد ملی ایران شماره ۹۶۰۰، سال: ۱۳۸۶با منبع ISO-IEC 10116:2006 موجود است.

4 - Message Authentication Codes

5 -Proofs of Security

فناوری اطلاعات- فنون امنیتی- رمزگذاری اصالت‌سنجی شده

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی تعیین شش روش رمزگذاری اصالت‌سنجی شده، یعنی روش‌های پردازش رشته داده‌ای با اهداف امنیتی زیر است:

- محرمانگی داده‌ها به معنی محافظت در برابر افشای غیرمجاز داده‌ها.
- یکپارچگی داده‌ها به معنی محافظتی که گیرنده‌ی داده می‌تواند دست‌کاری نشدن داده را تصدیق کند.
- اصالت‌سنجی مبدأ، به معنی محافظتی که گیرنده‌ی داده می‌تواند هویت فرستنده‌ی داده را تصدیق کند.

همه‌ی شش روش مشخص‌شده در این استاندارد بر اساس الگوریتم رمزگذاری بلوکی(بستک)[1] هستند و نیاز دارند گیرنده و فرستنده‌ی داده‌ی محافظت‌شده، کلید محرمانه‌ای را برای این رمز بلوک به اشتراک بگذارند. مدیریت کلید، خارج از محدوده‌ی این استاندارد است. مدیریت کلید در ISO/IEC 11770 تعریف شده است.

چهار سازوکار این استاندارد، به نام سازوکارهای ۱، ۳، ۴ و ۶ اجازه می‌دهند داده‌های رمزگذاری نشده اصالت‌سنجی شوند؛ به عبارت دیگر این سازوکارها اجازه می‌دهند رشته داده‌ای که باید محافظت شود به دو قسمت تقسیم شود، D داده‌ای است که باید رمزگذاری و از لحاظ یکپارچگی محافظت شود و A (داده اصالت‌سنجی شده افزونه) که از لحاظ یکپارچگی محافظت شده، اما رمزگذاری نشده است. در همه موارد رشته A ممکن است خالی باشد.

یادآوری- نمونه‌هایی از انواع داده‌ها که ممکن است نیاز باشد به‌صورت غیر رمزگذاری شده ارسال شوند، اما یکپارچگی آن‌ها باید حفظ شود، عبارت‌اند از: نشانی‌ها، شماره‌های درگاه، شماره‌های دنباله، شماره‌های نسخه پروتکل و سایر فیلدهای پروتکل شبکه که نشان می‌دهد چگونه متن ساده[2] باید سامان‌دهی، هدایت یا پردازش شود.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

1- Block
2- Plaintext

2-1 ISO/IEC 9797-1, Information technology - Security techniques - Message Authentication (MACs) - Part 1: Mechanisms using a block cipher[1]

2-2 ISO/IEC 10116, Information technology - Security techniques - Modes of operation for an n-bit block cipher[2]

2-3 ISO/IEC 18033-3, Information technology - Security techniques - Encryption algorithms - Part 3: Blockciphers[3]

۳ اصطلاحات و تعاریف

برای اهداف این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌روند:

۳-۱

رمزگذاری اصالت‌سنجی شده

تبدیل[4] (برگشت‌پذیر) داده‌ها به‌وسیله الگوریتم رمزگذاری به‌منظور ایجاد متن رمزگذاری شده است که بدون بررسی به‌وسیله یک موجودیت غیرمجاز، قابل‌تغییر نباشد، یعنی محرمانگی داده‌ها، یکپارچگی داده‌ها و اصالت‌سنجی مبدأ داده‌ها را فراهم کند.

۳-۲

سازوکار رمزگذاری اصالت‌سنجی شده

فن رمزگذاری است که برای حفاظت از محرمانگی و تضمین مبدأ و یکپارچگی داده استفاده شده است و شامل دو مؤلفه‌ی فرآیندی است: الگوریتم رمزگذاری و الگوریتم رمزگشایی[5]

۳-۳

رمز بلوکی[6]

سامانه‌ی رمزگذاری متقارن است، با این ویژگی که الگوریتم رمزگذاری روی یک بلوک از متن ساده، یعنی رشته‌ای از بیت‌ها با طول معین به‌منظور ایجاد بلوک متن رمزگذاری شده، عمل می‌کند.

[استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال: ۱۳۸۷]

۱- معادل فارسی این استاندارد برابر است با استاندارد ملی ایران شماره ۱-۹۷۹۷: سال۱۳۹۰، فناوری اطلاعات -فنون امنیتی - کدهای احراز هویت پیام (MAC) قسمت ۱ – سازوکارهای استفاده از رمزگذاری بلوکی

۲- معادل فارسی این استاندارد برابر است با استاندارد ملی ایران شماره ۹۶۰۰: سال۱۳۸۶، فن آوری اطلاعات -روش‌های امنیتی - حالت های عملیاتی یک الگوریتم رمزنگاری قطعه‌ای N بیتی

۳- معادل فارسی این استاندارد برابر است با استاندارد ملی ایران شماره ۳-۱۰۸۲۴: سال۱۳۸۷ فناوری اطلاعات -فنون امنیتی - الگوریتم‌های رمزنگاری-قسمت ۳-رمزهای بلوکی

4- Transformation
5- Decryption
6- Block Cipher

۴-۳

متن رمزی‌شده[1]

داده‌ای است که به‌منظور پنهان شدن محتوای اطلاعاتش تغییر داده شده است.

[استاندارد ملی ایران شماره ۹۶۰۰، سال: ۱۳۸۶]

۵-۳

یکپارچگی داده‌ها

ویژگی است که باعث می‌شود داده‌ها براثر یک رفتار غیرمجاز تغییر نکنند و خراب نشوند.

[استاندارد ملی ایران شماره ۱-۹۷۹۷، سال: ۱۳۹۰]

رمزگشایی

کنش عکس یک رمزگذاری متناظر است.

[ISO/IEC 18033-1]

۶-۳

رمزگذاری

تبدیل (برگشت‌پذیر) داده‌ها به‌وسیله یک الگوریتم رمزگذاری برای ایجاد متن رمزگذاری شده، یعنی مخفی کردن محتوای اطلاعاتی داده است.

[ISO/IEC 18033-1]

۷-۳

سامانه رمزگذاری

فن رمزگذاری است که برای حفاظت از محرمانگی داده استفاده می‌شود و شامل سه مؤلفه است: الگوریتم رمزگذاری، الگوریتم رمزگشایی و روشی برای تولید کلیدها

[ISO/IEC 18033-1]

۸-۳

کلید

دنباله‌ای از نمادها است که عملیات تبدیل رمزگذاری (یعنی رمزگذاری و رمزگشایی) را کنترل می‌کنند.

[ISO/IEC18033-1]

۹-۳

کد اصالت‌سنجی پیام

رشته‌ای از بیت‌ها که خروجی الگوریتم کد اصالت‌سنجی پیام (MAC) است.

1- Ciphertext

[استاندارد ملی ایران شماره ۱-۹۷۹۷، سال: ۱۳۹۰]

۳-۱۰

افراز[1]

فرآیند تقسیم رشته‌ای از بیت‌ها با طول دلخواه، به دنباله‌ای از بلوک‌ها است که طول هر بلوک باید n بیت باشد به‌جز بلوک آخر که باید r بیت باشد به گونه‌ای که $0 < r \leq n$.

۳-۱۱

متن ساده

اطلاعات رمزگذاری نشده است.

[استاندارد ملی ایران شماره ۹۶۰۰، سال: ۱۳۸۶]

۳-۱۲

کلید محرمانه

کلیدی است که در فنون رمزگذاری متقارن به‌وسیله‌ی موجودیتی خاص استفاده می‌شود.

[ISO/IEC 18033-1]

۳-۱۳

سامانه رمزگذاری متقارن

سامانه رمزگذاری مبتنی بر فنون رمزگذاری متقارن است که از کلید محرمانه یکسانی برای الگوریتم‌های رمزگذاری و رمزگشایی استفاده می‌کند.

[ISO/IEC 18033-1]

۴ نمادها (و کوته‌نوشت‌ها)

در این استاندارد ملی نمادها و نشانه‌گذاری زیر به‌کاربه‌کار می‌رود.

A داده اصالت‌سنجی شده افزونه.

C رشته داده رمزگذاری اصالت‌سنجی شده.

D رشته‌داده‌هایی که باید یک سازوکار رمزگذاری اصالت‌سنجی شده در آن به‌کاربرده شود.

d الگوریتم رمزگشایی رمز بلوک؛ $d_y(Y)$ نشان‌دهندهنشان‌دهنده نتیجه حاصل از رمزگشایی بلوکیِ بلوک n بیتی Y با استفاده از کلید محرمانه K است.

e الگوریتم رمزگذاری رمز بلوک؛ $e_K(X)$ نشان‌دهنده نتیجه حاصل از رمزگذاری بلوکیِ بلوک n بیتی X با استفاده از کلید محرمانه K است.

K کلید محرمانه رمزگذاری بلوکی که به‌وسیله گیرنده و فرستنده داده‌ای که باید سازوکار رمزگذاری

1-Partition

اصالت‌سنجی شده‌اصالت‌سنجی شده به آن اعمال شود، به اشتراک گذاشته می‌شود.

m تعداد بلوک‌ها در نسخه افراز شده D.

n طول بلوکِ رمز بلوک (به بیت).

t طول برچسب (به بیت).

0^i بلوکی از i بیت صفر.

1^i بلوکی از i بیت یک.

$\oplus$ یای انحصاری رشته‌های بیتی (با طول یکسان).

$||$ الحاق رشته بیت‌ها، یعنی اگر A و B بلوک‌هایی از بیت‌ها باشند، آنگاه $A||B$ بلوکی از بیت‌ها است که به‌وسیله الحاق A و B به ترتیب مشخص‌شده، ایجاد شده است.

$\#$ کارکردی که یک عدد را به بلوکی a بیتی از بیت‌ها تبدیل می‌کند. اگر k یک عدد صحیح باشد به‌طوری که $(0 \leq K < 2^k)$، آنگاه $\#_a(k)$ یک بلوک a بیتی است که اگر به‌عنوانبه‌عنوان بازنمایی دودویی یک عدد به‌صورت باارزش‌ترین بیت در سمت چپ تفسیر شود، معادل k می‌شود.

$\#^{-1}$ کارکردی که یک بلوک از بیت‌ها را به یک عدد تبدیل می‌کند. اگر A بلوکی از بیت‌ها باشد، $\#^{-1}(A)$ یک مقدار صحیح غیر علامت‌دار است که بازنمایی دودویی آن برابر A می‌شود. بنابراین اگر A دارای n بیت باشد، آنگاه داریم: $\#_n(\#^{-1}(A)) = A$.

$X|_s$ برش چپ یک بلوک از بیت‌ها به اسم X. اگر X طول بیتی بیشتر یا مساوی s داشته باشد، آنگاه $X|_s$ یک بلوک s بیتی است که s بیت سمت چپ X را در بر دارد.

$X|^s$ برش راست یک بلوک از بیت‌ها به اسم X. اگر X طول بیتی بیشتر یا مساوی s داشته باشد، آنگاه $X|^s$ یک بلوک s بیتی است که s بیت سمت راست X را در بر دارد.

$X \ll 1$ اانتقال به چپ مکانی بلوکی از بیت‌ها به اسم X. سمت راست‌ترین بیت از $Y = X \ll 1$ همیشه صفر می‌شود.

$X \gg 1$ انتقال به راست مکانی بلوکی از بیت‌ها به اسم X. سمت چپ‌ترین بیت از $Y = X \gg 1$ همیشه صفر می‌شود.

len کارکردی که رشته بیت X را به‌عنوان ورودی گرفته و تعداد بیت‌های آن را به‌عنوان خروجی می‌دهد.

mod اگر a و b اعداد صحیح بزرگ‌تر از صفر باشند، آنگاه a mod b عدد صحیح یکتایی را مشخص می‌کند به‌طوری که:

i. $0 \leq c < b$

ii. $a - c$ مضربی صحیح از b است.

۵ الزامات

سازوکار رمزگذاری اصالت‌سنجی شده‌ی مشخص‌شده در این استاندارد، الزامات زیر را دارد.

فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده در آن به‌کاربرده می‌شود باید:
الف- بر استفاده از یکی از سازوکارهای مشخص‌شده در این استاندارد توافق کند.
ب- بر استفاده از یک رمز بلوک مشخص در سازوکار توافق کند (یکی از رمز بلوک‌های مشخص‌شده در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷ باید استفاده شود).
پ- کلید محرمانه K را به اشتراک بگذارند: در تمامی سازوکارها به‌جز سازوکار پنجِ رمزگذاری اصالت‌سنجی شده، این کلید باید کلیدی برای رمز بلوک انتخاب‌شده باشد و در سازوکار پنج باید کلیدی باشد که به‌عنوان ورودی برای رویه[1]اشتقاق کلید[2] استفاده می‌شود.

۶ سازوکار شماره ۱ رمزگذاری اصالت‌سنجی شده

۶-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده که عموماً به‌عنوان OCB 2.0[3] شناخته می‌شود، تعریف شده است.

یادآوری– OCB 2.0 نتیجه کارهای Krovetz و Rogaway است. OCB 2.0 دارای اثبات امنیتی مبتنی بر این فرض است که رمز بلوک استفاده شده دارای ویژگی‌های ایده‌آل امنیتی مشخصی است.

۶-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری‌های زیر به‌کار می‌رود.

B بلوکی از بیت‌ها که در تعریف کارکرد J استفاده شده است.

$B_1, BB_2 \dots B_w$ دنباله‌ای از بلوک‌های بیت‌ها (هر کدام n بیت با استثناء احتمالی B_w) که در تعریف کارکرد J استفاده شده است.

$C_1, C_2 \dots C_m$ دنباله‌ای از بلوک‌های بیت‌ها (هر کدام n بیت با استثناء احتمالی C_m) که به‌عنوان بخشی از خروجی فرآیند رمزگذاری اصالت‌سنجی شده به‌دست آمده است.

$D_1, D_2 \dots D_m$ دنباله‌ای از بلوک‌هایِ بیت‌ها (هر کدام n بیت با استثناء احتمالی D_m) که در نتیجه افراز D به‌دست آمده است.

F بلوک n بیتی که در فرآیند رمزگذاری و رمزگشایی استفاده شده است.

H بلوک n بیتی که در فرآیند رمزگذاری و رمزگشایی استفاده شده است.

J کارکردی که در فرآیندهای رمزگذاری و رمزگشایی استفاده شده است.

K متغیری که در تعریف کارکرد J استفاده می‌شود.

M تعداد بلوک‌های n بیتی در پیامی که باید رمزگذاری شود (بلوک نهایی ممکن است

1- Procedure
2- Key derivation
3- Offset Codebook version 2.0

کمتر از n بیت داشته باشد)، یعنی پیام شامل $(m-1)n+r$ بیت است.

M_2 کارکرد استفاده‌شده در فرآیندهای رمزگذاری و رمزگشایی.

M_3 کارکرد استفاده‌شده در فرآیندهای رمزگذاری و رمزگشایی.

P بلوک n بیتی که در تعریف کارکرد M_2 استفاده شده است.

R تعداد بیت‌ها $(0 < r \leq n)$ در آخرین بلوک از پیامی که باید رمزگذاری شود، بعد از افراز پیام به بلوک‌های n بیتی. یعنی $len(D) = (m-1)n + r$

S متغیر آغازین (n بیتی).

T برچسب (t بیتی) که به‌منظور محافظت از یکپارچگی، به پیام رمزگذاری شده، الحاق شده است.

T' مقدار برچسب بازمحاسبه‌شده که در فرآیند رمزگشایی تولید شده است.

W متغیری که در تعریف کارکرد J استفاده شده است.

Z بلوک n بیتی که در فرآیند رمزگذاری و رمزگشایی استفاده شده است.

۶-۳ الزامات خاص

قبل از هرگونه استفاده از سازوکار، فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده روی آن اعمال می‌شود باید بر طول برچسب t بیت توافق نمایند که $0 < t \leq n$.

۶-۴ تعریف کارکرد M_2

تعریف رویه‌های رمزگذاری و رمزگشایی نیازمند تعریف کارکرد M_2 است که یک بلوک n بیتی را به‌عنوان ورودی گرفته و یک بلوک n بیتی را به‌عنوان خروجی می‌دهد. تعریف این کارکرد وابسته به بلوک n بیتی P است. از آنجا که n باید متناظر با طول رمز بلوک انتخاب‌شده از بین رمز بلوک‌های مشخص‌شده در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷ باشد، ما تنها P را برای $n = 64$ و $n = 128$ تعریف می‌کنیم.

الف- اگر $n = 64$ آنگاه $P = 0^{59}||11011$.

ب- اگر $n = 128$ آنگاه $P = 0^{120}||10000111$.

کارکرد M_2 به‌صورتی که در ادامه می‌آید تعریف می‌شود. اگر X یک بلوک n بیتی باشد، آنگاه:

الف- اگر سمت چپ‌ترین (باارزش‌ترین) بیت X صفر باشد، آنگاه $M_2(X) = X << 1$؛

ب- اگر سمت چپ‌ترین (باارزش‌ترین) بیت X یک باشد، آنگاه $M_2(X) = [X << 1] \oplus P$.

۶-۵ تعریف کارکرد M_3

تعریف رویه اداره داده اصالت‌سنجی شده افزونه، نیازمند تعریف تابع M_3 است که یک بلوک n بیتی را به‌عنوان ورودی گرفته و یک بلوک n بیتی را به‌عنوان خروجی بیرون می‌دهد. اگر X یک بلوک n بیتی باشد، آنگاه:

$$M_3(X) = M_2(X) \oplus X$$

۶-۶ تعریف کارکرد J

این کارکرد یک بلوک از بیت‌ها B (که $len(B) > 0$) را در ورودی گرفته و بلوک n بیتی $J(B)$ را به‌عنوان خروجی بیرون می‌دهد. مقدار $J(B)$ به روش زیر محاسبه می‌شود.

الف- B را به دنباله‌ای از بلوک‌های $B_1, B_2, \dots, B_w$ به شکلی که در ادامه می‌آید افراز کنید. فرض شود که B_1 اولین n بیت از B را داشته باشد، B_2 دومین n بیت از B و همین‌طور تا B_w که آخرین k بیت را دارد. بنابراین داریم: $len(B) = (w-1)n + k$.

ب- فرض شود که $F = M_3(M_3(e_K(0^n)))$.

پ- فرض شود که $C_0 = 0^n$.

ت- برای $i = 1,2, \dots, w-1$، دو گام زیر برداشته شود:

۱- فرض شود که $F = M_2(F)$.

۲- فرض شود که $C_i = C_{i-1} \oplus e_K(B_i \oplus F)$.

ث- فرض شود که $F = M_3(M_2(F))$.

ج- اگر $k < n$ باشد، دو گام زیر برداشته شود:

۱- فرض شود که $F = M_3(F)$.

۲- فرض شود که $B_w = B_w \,||\, 1 \,||\, 0^{(n-k-1)}$.

چ- $J(B) = e_K(C_{w-1} \oplus B_w \oplus F)$.

۶-۷ رویه رمزگذاری

فرستنده به‌منظور محافظت از رشته داده D باید گام‌های زیر را بردارد:

الف- متغیر شروع n بیتی S باید انتخاب شود. این متغیر برای هر پیامی که قرار است محافظت شود، باید متمایز بوده و باید در دسترس گیرنده پیام قرار گیرد، هرچند نیازی نیست این مقدار غیرقابل‌پیش‌بینی یا محرمانه باشد.

یادآوری- مقدار S مثلاً می‌تواند با استفاده از شمارشگری که به‌وسیله فرستنده نگهداری می‌شود، ایجاد و به‌صورت رمزگذاری نشده همراه با پیام محافظت‌شده ارسال شود.

ب- D به یک دنباله از بلوک‌های $D_1, D_2, \dots, D_m$ به‌طوری که در ادامه می‌آید افراز شود. فرض شود که D_1 شامل اولین n بیت باشد، D_2 شامل n بیت بعدی و الی‌آخر، تا D_m که r بیت نهایی را دارد، که $0 < r \le n$. بنابراین داریم: $\text{len(D)} = (\text{m}-1)\text{n} + \text{r}$.

پ- فرض شود که $F = e_K(S)$ و $\text{H} = 0^n$.

ت- برای $i = 1,2, \dots, m-1$ سه گام زیر برداشته شود:

۱- فرض شود که $F = M_2(F)$؛

۲- فرض شود که $H = H \oplus D_i$؛

۳- فرض شود که $C_i = F \oplus e_K(D_i \oplus F)$.

ث- فرض شود که $F = M_2(F)$.

ج- فرض شود که $Z = e_K(\#_n(r) \oplus F)$.

چ- فرض شود که $C_m = D_m \oplus Z|_r$.

ح- فرض شود که $H = H \oplus [D_m \,||\, (Z|^{n-r})]$.

خ- فرض شود که $T = [e_K(H \oplus M_3(F))]|_t$.

د- اگر $len\,(A) > 0$، آنگاه فرض شود که $T = T \oplus J(A)|_t$.

خروجی فرآیند بالا، یعنی نسخه رمزگذاری اصالت‌سنجی شده D باید رشته بیت زیر باشد:

$$C = C_1 \,||\, C_2 \,||\, \dots \,||\, C_m||\, T$$

یعنی رشته‌ای از $(m-1)n + r + t$ بیت که به طور دقیقاً شامل t بیت بیشتر از D است (اگرچه لازم است که متغیر آغازین n بیتی S و رشته بیت داده اصالت‌سنجی شده افزونه A که طول متغیر دارد نیز به گیرنده ارسال شوند).

۸-۶ رویه رمزگشایی

گیرنده برای رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده C باید گام‌های زیر را بردارد.

الف- اگر طول C کمتر از t است، توقف و نامعتبر را در خروجی نمایش‌داده‌شود.

ب- فرض شود که m و r اعداد صحیح منحصربه‌فردی باشند، طوری که C شامل $(m-1)n + r + t$ باشد، به‌طوری‌که $0 < r \leq n$. C به‌طوری‌که در ادامه می‌آید به دنباله‌ای از بلوک‌های $C_1, C_2, \dots, C_m, T$ افراز شود. فرض شود که C_1 اولین n بیت، C_2 دومین n بیت و الی‌آخر تا C_m آخرین r بیت از C را داشته باشند. در انتها فرض شود که T آخرین t بیت از C باشد.

پ- فرض شود که $F = e_K(S)$ و $H = 0^n$.

ت- برای $i = 1,2, \dots, m-1$ سه گام زیر برداشته شود:

۱- فرض شود که $F = M_2(F)$؛

۲- فرض شود که $D_i = F \oplus d_K(C_i \oplus F)$؛

۳- فرض شود که $H = H \oplus D_i$.

ث- فرض شود که $F = M_2(F)$.

ج- فرض شود که $Z = e_K(\#_n(r) \oplus F)$.

چ- فرض شود که $D_m = C_m \oplus Z|_r$.

ح- فرض شود که $H = H \oplus [D_m \,||\, (Z|^{n-r})]$.

خ- فرض شود که $T' = [e_K(H \oplus M_3(F))]|_t$.

د- اگر $len(A) > 0$ فرض شود $T' = T' \oplus J(A)|_t$.

اگر $T = T'$ آنگاه D و داده اصالت‌سنجی شده افزونه A در خروجی نمایش‌داده‌شود. در غیر این صورت نامعتبر در خروجی نمایش‌داده‌شود.

۷ سازوکار شماره ۲ رمزگذاری اصالت‌سنجی شده (پوشش کلید)

۷-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده‌ای که عموماً تحت عنوان پوشش کلید[1] شناخته شده است تعریف می‌شود.

یادآوری ۱- این طرح‌واره[2] در اصل برای رمزگذاری اصالت‌سنجی شده کلیدها و اطلاعات مرتبط طراحی شده بود. به این معنی که برای استفاده به همراه رشته‌ای داده‌ای کوتاه طراحی شده است. هرچند طرح‌واره می‌تواند با رشته‌های داده‌ای به طول دلخواه مورد استفاده قرار گیرد (حداکثر تا حدود 2^{67} بیت) اما برای محافظت از پیام‌های طولانی کارا[3] نیست.

یادآوری ۲- این حالت زمانی که رمز بلوک AES استفاده شود به‌عنوان پوشش کلید AES شناخته شده است که در آن AES نشان‌دهنده استاندارد رمزگذاری پیشرفته[4] است، الگوریتم رمزگذاری رمز بلوکی که در استاندارد ملی ایران شماره ۳-۱۰۸۲۴ سال ۱۳۸۷ مشخص شده است. پوشش کلید AES در [۹] و [۱۱] نیز تعریف شده است.

۷-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری زیر به‌کار می‌رود.

$C_0, C_1, \dots, C_m$ دنباله‌ای از $(m+1)$ بلوک ۶۴ بیتی که به‌عنوان خروجی فرآیند رمزگذاری اصالت‌سنجی شده به‌دست آمده است.

$D_1, D_2, \dots, D_m$ دنباله‌ای از m بلوک 64 بیتی که به‌وسیله افراز D به‌دست آمده است، یعنی $64m = len(D)$.

$R_1, R_2, \dots, R_m$ دنباله‌ای از m بلوک ۶۴ بیتی که در طول فرآیندهای رمزگذاری و رمزگشایی محاسبه می‌شوند.

Y بلوک ۶۴ بیتی که در طول فرآیندهای رمزگذاری و رمزگشایی استفاده شده است.

Z بلوک ۱۲۸ بیتی که در طول فرآیندهای رمزگذاری و رمزگشایی محاسبه شده است.

۷-۳ الزامات

رمز بلوکی که با این سازوکار استفاده می‌شود باید ۱۲۸ بیتی باشد، یعنی باید $n = 128$ داشته باشد.

رشته داده D که باید با این سازوکار محافظت شود، باید حداقل دارای ۱۲۸ بیت بوده و تعداد بیت‌هایی از مضرب ۶۴ داشته باشد (یعنی طول بیت‌های D باید $64m$ باشد که $m \geq 1$).

1- Key Wrap
2- Schema
3- Efficient
4- Advanced Encryption Standard

۴-۷ رویه رمزگذاری

فرستنده به‌منظور حفاظت از رشته داده D باید گام‌های زیر را بردارد:

الف- D به دنباله‌ای از بلوک‌های ۶۴ بیتی $D_1, D_2, \dots, D_m$ افراز شود، طوری که D_1، ۶۴ بیت اول را در بربگیرد، D_2، ۶۴ بیت بعدی و الی‌آخر.

ب- فرض شود که Y بلوکی ۶۴ بیتی باشد که مقدار شانزده‌تایی[1] A6A6A6A6A6A6A6A6 داشته باشد، یعنی مقدار دودویی آن برابر می‌شود با (10100110 10100110 ... 10100110).

پ- برای $i = 1,2, \dots, m$ فرض شود که $R_i = D_i$.

ت- برای $i = 1,2, \dots,6m$ چهار گام زیر برداشته شود:

۱- فرض شود که $Z = e_K(Y \,||\, R_1)$؛

۲- فرض شود که $Y = Z|_{64} \oplus \#_{64}(i)$؛

۳- برای $j = 1,2, \dots, m-1$ فرض شود که $R_j = R_{j+1}$؛

۴- فرض شود که $R_m = Z|^{64}$.

ث- فرض شود که $C_0 = Y$.

ج- برای $i = 1,2, \dots, m$ فرض شود که $C_i = R_i$.

خروجی فرآیند بالا یعنی نسخه رمزگذاری اصالت‌سنجی شده D باید رشته بیت زیر باشد:

$$C = C_0 \,||\, C_1 \,||\, \dots \,||\, C_m$$

یعنی رشته‌ای از $64(m+1)$ بیت، یعنی C دقیقاً ۶۴ بیت بیشتر از D دارد.

۵-۷ رویه رمزگشایی

گیرنده باید گام‌های زیر را برای رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده C بردارد.

الف- اگر $\text{len}(C)$ مضربی از ۶۴ نیست یا کمتر از ۱۹۲ است، توقف و در خروجی نامعتبر نمایش داده‌شود.

ب- C به دنباله‌ای از $m+1$ بلوک ۶۴ بیتی $C_1, C_2, \dots, C_m$ افراز شود به‌طوری‌که C_0، ۶۴ بیت اول از C را داشته باشد، C_1 دارای ۶۴ بیت بعدی و الی‌آخر.

پ- فرض شود که $Y = C_0$.

ت- برای $i = 1,2, \dots, m$ فرض شود که $R_i = C_i$.

ث- برای $i = 6m, 6m-1, \dots, 1$، چهار گام زیر برداشته شود:

۱- فرض شود که $Z = d_K([Y \oplus \#_{64}(i)] \,||\, R_m)$؛

۲- فرض شود که $Y = Z|_{64}$؛

۳- برای $j = m, m-1, \dots, 2$، فرض شود که $R_j = R_{j-1}$؛

۴- فرض شود که $R_1 = Z|^{64}$.

1- Hexadecimal

ج- اگر $D = R_1 \,||\, R_2 \,||\, \ldots \,||\, R_m$ آنگاه در خروجی $Y = (10100110\ 10100110\ \ldots\ 10100110)$ نمایش‌داده‌شود، در غیر این صورت نامعتبر در خروجی نمایش‌داده‌شود.

۸ سازوکار شماره ۳ رمزگذاری اصالت‌سنجی شده (CCM)

۸-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده‌ای که عموماً تحت عنوان CCM[1] شناخته می‌شود، تعریف شده است.

یادآوری- CCM نتیجه کار انجام پذیرفته در[۱۲] توسط Whiting، Housley و Fergusen است. نسخه CCM که اینجا تعریف شده است، مورد خاصی از CCM است که در[۱۰] و[۱۲] تعریف شده است.

۸-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری زیر به‌کار می‌رود.

B	بلوکی از بیت‌ها که در محاسبه مقدار برچسب استفاده شده است.
$B_1, B_2, \ldots, B_v$	دنباله‌ای از بلوک‌هایی از بیت‌ها (هر کدام n بیت) که در محاسبه مقدار برچسب استفاده شده است.
$C_1, C_2, \ldots, C_m$	دنباله‌ای از m بلوک ۱۲۸ بیتی که به‌عنوان بخشی از خروجی فرآیند رمزگذاری اصالت‌سنجی شده به‌دست آمده است.
$D_1, D_2, \ldots, D_m$	دنباله‌ای از m بلوک ۱۲۸ بیتی که در نتیجه افراز نسخه پرشده[2] D به‌دست آمده است.
F	پرچم هشتایی[3].
L	طول D (به‌صورت هشتایی)، به‌استثنای مقادیر پرشده و طول بلوک D_0 .
R	تعداد هشتایی‌های D در بلوک D_m.
S	متغیر آغازین[4] (از 120-8w بیت)
T	مقدار برچسب متن ساده.
T'	مقدار برچسب باز محاسبه‌شده[5] که در فرآیند رمزگشایی تولید می‌شود.
U	مقدار برچسب رمزگذاری شده (به طول t بیت).
V	متغیری که در محاسبه مقدار برچسب استفاده شده است.

1- Counter With CBC-MAC
2- Padded
3- Flag Octet
4- Startig Variable
5- Recomputed

W	طول فیلد طول پیام در مبنای هشتایی.
X	بلوک ۱۲۸ بیتی که در طول فرآیند رمزگذاری و رمزگشایی محاسبه شده است.
Y	بلوک ۱۲۸ بیتی که در طول فرآیند رمزگذاری و رمزگشایی محاسبه شده است.

۸-۳ الزامات

قبل از هرگونه استفاده از سازوکار، فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده روی آن اعمال می‌شود باید روی موارد زیر توافق کند:

الف- t، طول بیت‌های برچسب باید از مجموعه $\{32, 48, 64, 80, 96, 112, 128\}$ انتخاب شود.

ب- w، طول هشتایی[1] فیلد طول پیام باید از مجموعه $\{2, 3, 4, 5, 6, 7, 8\}$ انتخاب شود.

یادآوری- انتخاب w حداکثر طول پیامی را که می‌تواند محافظت شود، تحت تأثیر قرار می‌دهد. حداکثر طول پیام 2^{8w+3} بیت یعنی 2^{8w} 2^{8w} هشتایی است.

رمز بلوکی که باید به همراه این سازوکار استفاده شود باید رمز بلوک ۱۲۸ بیتی باشد یعنی باید $n = 128$.

رشته داده D که با به‌کارگیری این سازوکار باید محافظت شود و رشته داده اصالت‌سنجی شده افزونه A باید اعداد هشتایی صحیح داشته باشند، یعنی طول آن‌ها باید مضربی از ۸ بیت باشد (یعنی $\text{len}(D)$ و $\text{len}(A)$ باید هردو اعداد صحیحی از مضرب ۸ باشند).

۸-۴ رویه رمزگذاری

فرستنده برای محافظت از رشته داده D باید گام‌های زیر را بردارد. فرض شود که $L = \text{len}(D)/8$، یعنی L تعداد هشتایی‌های D است.

الف- یک متغیر آغازین S که شامل $15 - w$ هشتایی است (یعنی 120-8w بیت)، باید انتخاب شود. این متغیر برای هر پیام که قرار است محافظت شود، باید متمایز باشد و باید در دسترس گیرنده پیام قرار گیرد. هرچند لازم نیست این متغیر غیرقابل‌پیش‌بینی یا محرمانه باشد.

یادآوری- مقدار S مثلاً می‌تواند با استفاده از شمارشگری که به‌وسیله فرستنده نگهداری می‌شود، ایجاد و به‌صورت رمزگذاری نشده همراه با پیام محافظت‌شده ارسال شود.

ب- رشته داده D از سمت راست با $16 - r$ هشتایی صفر پر شود (یعنی بین صفر تا ۱۲۰ بیت صفر)، طوری که نسخه پرشده D مضربی از ۱۲۸ بیت داشته باشد. سپس نسخه پرشده از D به دنباله‌ای از m بلوک ۱۲۸ بیتی $D_1, D_2, \ldots, D_m$ افراز شود که D_1 اولین ۱۲۸ بیت از D را داشته باشد، D_2 دارای ۱۲۸ بیت بعدی باشد و الی‌آخر.

یادآوری- مقدار m باید شرط $16(m-1) < L \leq 16m$ را برآورده کند.

پ- اگر $\text{len}(A) = 0$ باشد، فرض شود که $F = 0^2 \,||\, \#_3((t-16)/16) \,||\, \#_3(w-1)$

ت- اگر $\text{len}(A) > 0$ باشد، فرض شود که $F = 0 \,||\, 1 \,||\, \#_3((t-16)/16) \,||\, \#_3(w-1)$

1- Octet Length

یادآوری- پرارزش‌ترین (سمت چپ‌ترین) بیت F، بیتِ ذخیره شده است، یعنی در نسخه‌ای از سازوکار که در اینجا مشخص شده، صفر قرار داده شده است، اما در آینده در نسخه‌های دیگری از سازوکار می‌تواند استفاده شود. بیت بعد از پرارزش‌ترین بیت F نیز صفر قرار داده شده است تا نشان دهد همه داده‌هایی که توسط سازوکار محافظت می‌شود، رمزگذاری شده است.

ث- فرض شود که $X = e_K(F \,||\, S \,||\, \#_{8w}(L))$.

ج- اگر $\text{len}(A) > 0$ باشد شش گام زیر برداشته شود:

۱- اگر $0 < len(A) < 65280$ آنگاه فرض شود که $B = \#_{16}(\text{len}(A)/8) \,||\, A$؛

۲- اگر $65280 \leq \text{len}(A) < 2^{32}$ فرض شود که $B = 1^{15} \,||\, 0 \,||\, \#_{32}(\text{len}(A)/8) \,||\, A$؛

۳- اگر $2^{32} \leq \text{len}(A) < 2^{64}$ آنگاه فرض شود که $B = 1^{16} \,||\, \#_{64}(\text{len}(A)/8) \,||\, A$؛

۴- B به دنباله‌ای از بلوک‌های $B_1, B_2, \dots, B_v$ افراز شود که B_1 اولین n بیت از B را داشته باشد، B_2 دارای n بیت بعدی باشد و الی‌آخر تا B_v که دارای k بیت آخری است، که $0 < k \leq n$ بنابراین $\text{len}(B) = (v-1)n + k$؛

۵- B_v با $n-k$ صفر پر شود یعنی $B_v = B_v \,||\, 0^{n-k}$؛

۶- برای $i = 1,2, \dots, v$ فرض شود $\text{let } X = e_K(X \oplus B_i)$.

چ- برای $i = 1,2, \dots, m$ فرض شود که $X = e_K(X \oplus Di)$.

ح- فرض شود که $T = X|_t$.

یادآوری- برچسب T متن ساده مساوی MAC محاسبه‌شده روی رشته داده $B_1, B_2, \dots, B_v, D_1, D_2, \dots, D_m$ است که با اصلاح جزیی الگوریتم یک MAC، مشخص‌شده در استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰، به‌دست آمده است.

خ- فرض شود که $F = (0^5 \,||\, \#_3(w-1))$ و $Y = (F \,||\, S \,||\, 0^{8w})$

یادآوری- دو بیت باارزش‌تر(یعنی سمت چپ‌ترین) بیت‌های F بیت‌های ذخیره شده‌اند، یعنی در نسخه‌ای از سازوکار که در اینجا مشخص شده، صفر قرار داده شده است، اما در آینده در نسخه‌های دیگری از سازوکار می‌تواند استفاده شود. سه بیت باارزش‌تر بعدی F صفر قرار داده شده‌اند که تضمین کند این هشتایی از هشتایی پرچم استفاده‌شده در گام پ متمایز است.

د- فرض شود که $U = T \oplus [e_K(Y)]|_t$.

ذ- برای $i = 1,2, \dots, m-1$ گام‌های زیر برداشته شود:

۱- فرض شود که $Y = (F \,||\, S \,||\, \#_{8w}(i))$؛

۲- فرض شود که $C_i = D_i e_K(Y)$.

ر- فرض شود که $Y = (F \,||\, S \,||\, \#_{8w}(m))$ و فرض شود که $C_m = [D_m \oplus e_K(Y)]|_{8r}$.

خروجی حاصل از فرآیند بالا، یعنی نسخه رمزگذاری اصالت‌سنجی شده D، باید رشته بیت زیر باشد:

$$C = C_1 \,||\, C_2 \,||\, \dots \,||\, C_{m-1} \,||\, C_m \,||\, U$$

یعنی رشته‌ای از $8L + t$ بیت، که C دقیقاً t بیت بیشتر از رشته اصلی D دارد(اگرچه ضروری است که متغیر آغازین $(120 - 8w)$ بیتی S و داده اصالت‌سنجی شده افزونه A که طولی متغیر دارد نیز به گیرنده منتقل شوند).

۵-۸ رویه رمزگشایی

گیرنده به‌منظور رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده C باید گام‌های زیر را بردارد:

الف- اگر C مقداری صحیح از هشتایی‌ها را در بر ندارد، توقف و در خروجی نامعتبر نمایش‌داده شود.

ب- اگر طول C کمتر از $(t+8)$ بیت است، توقف و در خروجی نامعتبر نمایش‌داده‌شود.

پ- فرض شود که m و r اعداد صحیح یکتایی باشند طوری که C شامل $t128(m-1)+8r$ بیت باشد، که $0<r\leq 16$. C به دنباله‌ای از بلوک‌های $C_1, C_2, \dots C_m, U$ به شکلی که در ادامه می‌آید افراز شود. فرض شود که C_1 شامل ۱۲۸ بیت اول از C باشد، C_2 شامل ۱۲۸بیت بعدی و الی‌آخر، تا C_m که شامل $8r$ بیت بعدی C است. در آخر هم فرض شود که U، آخرین t بیت از C باشد.

ت- فرض شود که $F = (0^5 \,||\, \#_3(w-1))$ و $Y = (F \,||\, S \,||\, 0^{8w})$

ث- فرض شود که $T = U \oplus [e_K(Y)]|_t$

ج- برای $i = 1,2,\dots,m-1$ گام‌های زیر برداشته شود:

۱- فرض شود که $Y = (F \,||\, S \,||\, \#_{8w}(i))$

۲- فرض شود که $D_i = C_i e_K(Y)$

چ- فرض شود که $Y = (F \,||\, S \,||\, \#8_w(m))$ و $D_m = C_m \oplus [e_K(Y)]|_{8r}$

ح- فرض شود که $D = D_1 \,||\, D_2 \,||\, \dots \,||\, D_m$ و $L = 16m - 16 + r$

خ- D_m از سمت راست با $128-r$ صفر پر شود ، یعنی فرض شود که $D_m = D_m \,||\, 0^{128-8r}$

د- اگر $len(A) = 0$ فرض شود که $F = 0^2 \,||\, \#_3((t-16)/16) \,||\, \#_3(w-1)$

ذ- اگر $len(A) > 0$ فرض شود که $F = 0 \,||\, 1 \,||\, \#_3((t-16)/16) \,||\, \#_3(w-1)$

ر- فرض شود که $X = e_K(F \,||\, S \,||\, \#_{8w}(L))$

ز- اگر $len(A) > 0$ آنگاه شش گام زیر برداشته شود:

۱- اگر $0 < len(A) < 65280$ آنگاه فرض شود که $B = \#_{16}(len(A)/8) \,||\, A$؛

۲- اگر $65280 \leq len(A) < 2^{32}$ آنگاه فرض شود که $B = 1^{15} \,||\, 0 \,||\, \#_{32}(len(A)/8) \,||\, A$؛

۳- اگر $2^{32} \leq len(A) < 2^{64}$ آنگاه فرض شود که $B = 1^{16} \,||\, 0 \,||\, \#_{64}(len(A)/8) \,||\, A$؛

۴- B را به دنباله‌ای از بلوک‌های $B_1, B_2, \dots, B_v$ به روشی که در ادامه می‌آید افراز شود. فرض شود که B_1 اولین n بیت از B را داشته باشد، B_2 دارای n بیت بعدی باشد، الی‌آخر، تا B_v که شامل k بیت آخری است که $0 < k \leq n$ بنابراین $len(B) = (v-1)n + k$؛

۵- B_vرا از سمت راست با $n-k$ صفر پر شود. یعنی $B_v = B_v \,||\, 0^{n-k}$؛

۶- برای $i = 1,2,\dots,v$ فرض شود که $X = e_K(X \oplus Bi)$.

ژ- برای$i = 1,2,\dots,m$ فرض شود که $X = e_K(X \oplus D_i)$.

س- فرض شود که $T' = X|_t$.

ش- اگر $T = T'$ آنگاه D (که در مرحله ح محاسبه شد) و A در خروجی نمایش‌داده‌شود، در غیر این صورت نامعتبر در خروجی نمایش‌داده‌شود.

۹ سازوکار شماره ۴ رمزگذاری اصالت‌سنجی شده

۹-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده‌ای که عموماً تحت عنوان EAX شناخته شده است، تعریف شده است.

یادآوری- EAX نتیجه کار انجام پذیرفته در [۳] توسط Bellare، Rogaway و Wagner است. حروف EAX به مورد خاصی اشاره نمی‌کنند.

۹-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری زیر به‌کار می‌رود.

$C_1, C_2, \dots, C_m$ دنباله‌ای از بلوک‌هایی از بیت‌ها (هر کدام n بیت با استثنای احتمالی C_m) که در نتیجه بخشی از خروجی فرآیند رمزگذاری اصالت‌سنجی شده به‌دست آمده است.

$D_1, D_2, \dots, D_m$ دنباله‌ای از بلوک‌هایی از بیت‌ها (هر کدام n بیت، با استثنای احتمالی D_m) که در نتیجه افراز D به‌دست آمده است.

E_0, E_1, E_2 بلوک‌های n بیتی که در فرآیندهای رمزگذاری و رمزگشایی محاسبه شده‌اند.

M کارکردی که در فرآیند رمزگذاری و رمزگشایی استفاده می‌شود.

S متغیرهای آغازین (n بیت)

T برچسب (t بیتی) که برای محافظت از یکپارچگی به پیام رمزگذاری شده الصاق شده است.

T' مقدار برچسب باز محاسبه‌شده، که در طول فرآیند رمزگشایی تولید شده است.

W بلوکی n بیتی که در طول فرآیندهای رمزگذاری و رمزگشایی محاسبه می‌شوند.

۹-۳ الزامات

قبل از هرگونه استفاده از سازوکار، فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده روی آن اعمال می‌شود باید بر موارد زیر توافق کنند:

الف- t، طول برچسب به بیت، که $0 < t \leq n$.

۹-۴ تعریف کارکرد M

تعریف رویه‌های رمزگذاری و رمزگشایی نیازمند تعریف کارکرد M است که یک رشته از بیت‌ها به طول دلخواه و یک کلید رمز بلوک را به‌عنوان ورودی گرفته و در خروجی یک بلوک n بیتی می‌دهد. تعریف این کارکرد به شرح زیر است.

اگر X رشته‌ای از بیت‌ها، و K کلیدی برای رمز بلوک انتخاب شده باشد، آنگاه $M_K(X)$ باید مساوی کد اصالت‌سنجی پیام، محاسبه‌شده روی رشته X با استفاده از کلید K و با استفاده از الگوریتم پنج MAC در استاندارد ملی ایران شماره ۱-۹۷۹۷، سال: ۱۳۹۰باشد، که رمز بلوک انتخاب‌شده در الگوریتم MAC باید همانند الگوریتم رمز بلوک انتخاب‌شده برای فرآیند رمزگذاری اصالت‌سنجی شده باشد.

یادآوری- الگوریتم پنج MAC از استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰تحت عنوان OMAC نیز شناخته شده است.

۹-۵ رویه رمزگذاری

فرستنده به‌منظور محافظت از رشته داده D باید گام‌های زیر را بردارد.

الف- یک متغیر آغازین S که شامل n بیت است باید انتخاب شود. این متغیر برای هر پیامی که قرار است محافظت شود، باید متمایز بوده و در دسترس گیرنده پیام قرار گیرد. هرچند لازم نیست که این متغیر غیرقابل‌پیش‌بینی یا محرمانه باشد.

ب- فرض شود که $E_0 = M_K(0^n||S)$.

پ- فرض شود که $E_1 = M_K(0^{n-1}||1||A)$.

ت- فرض شود که $W = E_0$.

ث- D به دنباله‌ای از بلوک‌های $D_1, D_2, \dots, D_m$ به شکلی که در ادامه می‌آید افراز شود. فرض شود که D_1 اولین n بیت از D را در بر داشته باشد، D_2 دارای n بیت بعدی و الی‌آخر، تا D_m که r بیت پایانی را در بر دارد که $0 < r \leq n$. بنابراین داریم $len(D) = (m-1)n + r$.

ج- برای i=1,2,...,m-1 دو گام زیر برداشته شود:

۱- فرض شود که $C_i = D_i \oplus e_K(W)$؛

۲- فرض شود که $W = \#_n(\#^{-1}(W) + 1 \bmod 2^n)$.

چ- فرض شود که $C_m = D_m \oplus [e_K(W)]|_r$.

ح- فرض شود که $E_2 = M_K(0^{n-2}||1||0||C_1||C_2|| \dots ||C_m)$.

خ- فرض شود که $T = [E_0 \oplus E_1 \oplus E_2]|_t$.

خروجی حاصل از فرآیند بالا یعنی نسخه رمزگذاری اصالت‌سنجی شده از D باید رشته بیت زیر باشد:

$$C = C_1 \,||\, C_2 \,||\, \dots \,||\, C_m \,||\, T$$

یعنی رشته‌ای از $(m-1)n + r + t$ بیت، که C دقیقاً حاوی t بیت بیشتر از D است (اگرچه ضروری است که متغیر آغازین n بیتی S و داده رمزگذاری اصالت‌سنجی شده افزونه A که طولی متغیر دارد نیز به گیرنده منتقل شوند).

۹-۶ رویه رمزگشایی

گیرنده برای رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده C باید گام‌های زیر را بردارد.

الف- اگر طول C کمتر از t است، توقف و در خروجی **نامعتبر** نمایش‌داده شود.

ب- فرض شود که اعداد صحیح منحصربه‌فرد m و r طوری تعریف شده‌اند که C شامل $(m-1)n+r+t$ بیت باشد که $0 < r \leq n$. C به دنباله‌ای از بلوک‌های $C_1, C_2, \dots, C_m, T$ به شکلی که در ادامه می‌آید افراز شود. فرض شود که C_1 شامل n بیت اول C باشد، C_2، حاوی n بیت بعدی باشد و الی‌آخر، تا C_m که r بیت بعدی C را در بر دارد. در انتها فرض شود T، آخرین t بیت از C را داشته باشد.

پ- فرض شود که $E_0 = M_K(0^n||S)$.

ت- فرض شود که $E_1 = M_K(0^{n-1}||1||A)$.

ث- فرض شود که $E_2 = M_K(0^{n-2}||1||0||C_1||C_2||\dots||C_m)$.

ج- فرض شود که $T' = [E_0 \oplus E_1 \oplus E_2]|_t$.

چ- اگر $T \neq T'$ آنگاه توقف و در خروجی نامعتبر نمایش‌داده‌شود.

ح- فرض شود که $W = E_0$.

خ- برای $i = 1,2, \dots, m-1$ گام‌های زیر برداشته شود:

۱- فرض شود که $D_i = C_i \oplus e_K(W)$

۲- فرض شود که $W = \#_n(\#^{-1}(W) + 1 \bmod 2^n)$

د- فرض شود که $D_m = C_m \oplus [e_K(W)]|_r$

ذ- در خروجی A و D نمایش‌داده‌شود.

۱۰ سازوکار شماره ۵ رمزگذاری اصالت‌سنجی شده

۱۰-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده‌ای که ترکیبی از هر سازوکار رمزگذاری و هر طرح‌واره‌ی MAC است، تعریف شده است. این طرح‌واره ابتدا شامل رمزگذاری داده‌ای است که باید محافظت شود و سپس محاسبه یک MAC روی‌داده رمزگذاری شده‌ی به‌دست آمده.

یادآوری- رویکرد «رمزگذاری سپس MAC»[1] به‌وسیله‌ی Bellare و Namprempre در[۲] تحلیل شده است که یک اثبات امنیتی روی این فرض که فن MAC و روش رمزگذاری استفاده‌شده دارای ویژگی‌های امنیتی معینی هستند، فراهم می‌کند.

۱۰-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری زیر به‌کار می‌رود.

C' رشته بیتی که به‌وسیله رمزگذاری رشته داده D به‌دست آمده است.

1- Encrypt then MAC

δ	کارکرد رمزگشایی، یعنی کارکردی که به‌عنوان ورودی کلید رمز بلوک K_1، متغیر آغازین S و رشته داده رمزگذاری‌شده C' را دریافت کرده و با استفاده از حالت عملیات انتخاب‌شده، یک رشته داده رمزگشایی‌شده را در خروجی می‌دهد. خروجی به‌صورت $\delta_{K_1,S}(C')$ نوشته می‌شود.
ε	کارکرد رمزگذاری، یعنی کارکردی که به‌عنوان ورودی کلید رمز بلوک K_1، متغیر آغازین S و رشته داده D را دریافت نموده و با استفاده از حالت عملیات انتخاب‌شده، رشته داده رمزگذاری شده را در خروجی می‌دهد. خروجی به‌صورت $\varepsilon_{K_1,S}(D)$ نوشته می‌شود.
f	کارکرد MAC: اگر X یک رشته ورودی و K_2 کلید MAC باشد، آنگاه MAC خروجی به‌صورت $f_{K_2}(X)$ مشخص می‌شود.
K_1	کلید محرمانه رمز بلوک.
K_2	کلید محرمانه کارکرد MAC.
S	متغیر آغازین (n بیت).
T	برچسب (t بیتی) که برای محافظت از یکپارچگی به پیام رمزگذاری شده الصاق شده است.
T'	مقدار برچسب باز محاسبه‌شده، که در طول فرآیند رمزگشایی تولید شده است.

۱۰-۳ الزامات

قبل از هرگونه استفاده از سازوکار، فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده روی آن اعمال می‌شود باید بر موارد زیر توافق شود:

الف- حالت عملیات رمز بلوک از بین موارد مشخص‌شده در استاندارد ملی ایران شماره ۹۶۰۰، سال ۱۳۸۶ (حالت ECB نباید استفاده شود).

ب- روشی برای محاسبه MAC، که باید از فنون مشخص‌شده در استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰ انتخاب شود (ما فرض می‌کنیم که روش انتخاب‌شده برچسبی به طول t تولید می‌کند)

پ- روشی برای اشتقاق یک زوج کلید محرمانه (K_1, K_2) از کلید محرمانه K، که K_1 کلیدی برای رمز بلوک انتخاب‌شده و K_2 کلیدی برای روش انتخاب‌شده محاسبه MAC است.

یادآوری ۱- مقدار K باید طوری انتخاب شود که تعداد مقادیر ممکن برای K حداقل به‌اندازه تعداد مقادیر ممکن برای کلید رمز بلوک بوده و همچنین حداقل به‌اندازه تعداد مقادیر ممکن برای کلید MAC بزرگ باشد.

۱۰-۴ رویه رمزگذاری

فرستنده به‌منظور محافظت از رشته داده D باید گام‌های زیر را بردارد.

الف- متغیر آغازین S مناسب برای استفاده با حالت عملیات رمز بلوک انتخاب‌شده باید انتخاب گردد. این متغیر باید برای هر پیامی که قرار است تحت کلید ارائه‌شده محافظت شود، متمایز باشد و باید در دسترس گیرنده پیام قرار گیرد. الزامات افزونه ممکن برای S در قسمت مناسب در استاندارد ISO/IEC 10116 شرح داده شده است و راهنمای بیشتر در پیوست الف-۷ ارائه شده است.

یادآوری- اگر متغیر آغازین به صورت یکنواخت به طور تصادفی از فضای تمام متغیرهای آغازین ممکن (که بسیار توصیه می‌شود) انتخاب شود – به پیوست الف-۷ مراجعه شود- و تعداد پیام‌های رمزگذاری‌شده با استفاده از کلید به طور مناسب محدود شود، استفاده از متغیرهای آغازین متمایز به شدت مناسب است، به طور مثال متغیرهای آغازین می‌توانند به عنوان تمایز آماری مد نظر قرار گیرند.

ب- $C' = \mathcal{E}_{K_1,S}(D)$ با استفاده از متغیر آغازین S فرض شود .

پ- $T = f_{K_2}(S \| C')$ فرض شود .

خروجی حاصل از فرآیند بالا، یعنی نسخه رمزگذاری اصالت‌سنجی شده D، باید رشته بیت زیر باشد:

$C = C' \| T$ به همراه متغیر آغازین S.

۱۰-۵ رویه رمزگشایی

گیرنده برای رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده رشته C با همراهی متغیر آغازین S گام-های زیر را بردارد.

الف- اگر طول C کمتر از t است، توقف و در خروجی نامعتبر نمایش‌داده‌شود.

ب- فرض شود که T سمت راست‌ترین t بیت از C باشد و فرض شود C' برابر C باشد که t بیت سمت راست آن حذف شده است، یعنی $C = C' \| T$.

پ- $T' = f_{K_2}(S \| C')$ فرض شود .

ت- اگر $T \neq T'$ آنگاه توقف و در خروجی نامعتبر نمایش‌داده شود.

ث- $D = \delta_{K_1,S}(C')$ با استفاده از متغیر آغازین S فرض شود.

ج- D در خروجی نمایش‌داده‌شود.

۱۱ سازوکار شماره ۶ رمزگذاری اصالت‌سنجی شده

۱۱-۱ مقدمه

در این قسمت سازوکار رمزگذاری اصالت‌سنجی شده‌ای که عموماً تحت عنوان GCM[1] شناخته شده، تعریف شده است.

یادآوری- GCM نتیجه کار McGrew و Viega در [۸] است.

1- Galois/Counter Mode (GCM)

۱۱-۲ نمادگذاری خاص

در این استاندارد ملی نمادها و نمادگذاری زیر به‌کار می‌رود.

$C_1, C_2, \ldots, C_m$ دنباله‌ای از بلوک‌های ۱۲۸ بیتی (با استثنای احتمالی C_m که ممکن است بین ۱ تا ۱۲۸ بیت داشته باشد) که در نتیجه بخشی از خروجی فرآیند رمزگذاری اصالت‌سنجی شده به‌دست آمده است.

$D_1, D_2, \ldots, D_m$ دنباله‌ای از بلوک‌های ۱۲۸ بیتی (با استثنای احتمالی D_m) که در نتیجه افراز D به‌دست آمده است.

G کارکردی که در فرآیندهای رمزگذاری و رمزگشایی استفاده شده است (در بخش ۱۱-۵ تعریف شده است).

H بلوکی ۱۲۸ بیتی که در فرآیندهای رمزگذاری و رمزگشایی استفاده شده است.

inc کارکردی که یک بلوک ۱۲۸ بیتی را در ورودی دریافت کرده و یک بلوک ۱۲۸ بیتی را در خروجی می‌دهد، طوری که اگر X یک بلوک ۱۲۸ بیتی باشد داریم:

$$\mathrm{inc}(X) = (X|_{96}) \,||\, \#_{32}(\#^{-1}(X|^{32}) + 1 \bmod 2^{32})$$

R تعداد بیت‌ها در آخرین بلوک از پیامی که باید رمزگذاری شود، بعد از شکسته شدن پیام به بلوک‌های n بیتی، یعنی پیام دارای $(m-1)n + r$ بیت است.

R بلوکی ۱۲۸ بیتی که در محاسبه ضرب $GF(2^{128})$ استفاده شده است.

S متغیر آغازین (با طول متغیر).

T برچسب (t بیتی) که برای محافظت از یکپارچگی به پیام رمزگذاری شده الصاق شده است.

T' مقدار برچسب باز محاسبه‌شده، که در طول فرآیند رمزگشایی تولید شده است.

U, V, W, Z بلوکی ۱۲۸ بیتی که در تعریف محاسبه ضرب $GF(2^{128})$ استفاده شده است.

$X_0, X_1, \ldots, X_{k+l+1}$ بلوک‌های ۱۲۸ بیتی که در محاسبه‌کارکرد G.

$Y_0, Y_1, \ldots, Y_m$ دنباله‌ای از بلوک‌ها ۱۲۸ بیتی که در فرآیندهای رمزگذاری و رمزگشایی استفاده می‌شوند.

{} یک رشته بیت با طول صفر.

• ضرب در فیلد[1] $GF(2^{128})$ چندجمله‌ای که باید به‌منظور تعیین بازنمایی $GF(2^{128})$ مورد استفاده قرار گیرد، $1 + \alpha + \alpha^2 + \alpha^7 + \alpha^{128}$ است.

1- Multiplication in the field

۱۱-۳ الزامات

قبل از هرگونه استفاده از سازوکار، فرستنده و گیرنده داده‌ای که سازوکار رمزگذاری اصالت‌سنجی شده روی آن اعمال می‌شود باید بر موارد زیر توافق کند:

الف- طول برچسب t به بیت، که t مضربی از ۸ است و باید $96 \leq t \leq 128$ باشد (در بعضی از کاربردهای خاص $t = 32$ و $t = 64$ نیز مجاز است).

رمز بلوکی که قرار است در این سازوکار استفاده شود باید رمز بلوک ۱۲۸ بیتی باشد، یعنی باید $n = 128$ باشد.

۱۱-۴ تعریف کارکرد ضرب •

فرض شود U و V بلوک‌های ۱۲۸ بیتی باشند، آنگاه $W = U \bullet V$ که W نیز بلوکی ۱۲۸ بیتی است به شکل زیر تعریف شده است. توجه کنید که در توصیف زیر، V_i نشان‌دهنده بیت i از V است، یعنی $V = v_0 || v_1 || \dots || v_{127}$، به شکلی مشابه z_{127} سمت راست‌ترین بیت Z را نشان می‌دهد.

الف- فرض شود که $R = 11100001 \,||\, 0^{120}$.

ب- فرض شود که $W = 0^{128}$.

پ- فرض شود که $Z = U$.

ت- برای $i = 1,2,\dots,127$ دو گام زیر برداشته شود:

۱- اگر $v_i = 1$ آنگاه فرض شود که $W = W \oplus Z$؛

۲- اگر $z_{127} = 0$ آنگاه فرض شود که $Z = Z >> 1$، در غیر این صورت فرض شود که:

$$Z = (Z >> 1) \oplus R$$

۱۱-۵ تعریف کارکرد G

رویه‌های رمزگذاری و رمزگشایی از کارکرد G استفاده می‌کنند که یک بلوک ۱۲۸ بیتی و دو رشته بیتی با طول دلخواه را به‌عنوان ورودی دریافت کنند و یک بلوک ۱۲۸ بیتی را در خروجی بدهند. فرض شود که H یک بلوک ۱۲۸ بیتی باشد و W و Z دو رشته به طول دلخواه (شاید تهی) باشند. فرض شود که k و u اعداد صحیح یکتایی هستند که $\text{len}(W) = 128(k-1) + u$ و $0 < u \leq 128$. به طور مشابه فرض شود که l و v اعداد صحیح یکتایی هستند که $\text{len}(Z) = 128(l-1) + v$ و $0 < v \leq 128$. فرض شود که $W_1, W_2, \dots, W_k$ دنباله‌ای از بلوک‌های ۱۲۸بیتی (با استثنای احتمالی W_k، که شامل u بیت آخر از W است) باشد که در نتیجه افراز W به‌دست آمده است. به طور مشابه فرض شود که $Z_1, Z_2, \dots, Z_l$ *دنباله‌ای از* بلوک‌های ۱۲۸بیتی (با استثنای احتمالی Z_l، که شامل v بیت آخر از Z است) باشد که در نتیجه افراز Z به‌دست آمده است.

آنگاه $G(H, W, Z)$ مقداری ۱۲۸ بیتی X_{k+l+1} است، که X_i به طور بازگشتی برای $i = 0,1,\dots,k+l-1$ به شکل زیر تعریف شده است:

الف- $X_0 = 0^{128}$

ب- $X_i = (X_{i-1} \oplus W_i) \bullet H$ (اگر $1 \leq i \leq k-1$، $k \leq 1$ این گام حذف

می‌شود)

پ- $X_k = (X_{k-1} \oplus (W_k || 0^{128-u})) \bullet H$ (اگر $k=0$ باشد این گام حذف می‌شود)

ت- $X_i = (X_{i-1} \oplus Z_{i-k}) \bullet H$ $k+1 \le i \le k+l-1$ (اگر $l \le 1$، این گام حذف می‌شود)

ث- $X_{k+l} = (X_{k+l-1} \oplus (Z_l || 0^{128-v})) \bullet H$ (اگر $l = 0$ باشد این گام حذف می‌شود)

ج- $X_{k+l+1} = (X_{k+l} \oplus [\#_{64}(len(W)) \,||\, \#_{64}(len(Z))]) \bullet H$

۱۱-۶ رویه رمزگذاری

فرستنده به‌منظور محافظت از رشته داده D و اطمینان از یکپارچگی رشته داده رمزگذاری اصالت‌سنجی شده A باید گام‌های زیر را بردارد:

الف- متغیر آغازین S با طول متغیر باید انتخاب شود. این مقدار برای هر پیامی که قرار است محافظت شود باید متمایز باشد و باید در دسترس گیرنده پیام قرار گیرد. هرچند لازم نیست این مقدار غیرقابل‌پیش‌بینی یا محرمانه باشد.

یادآوری- مقدار S مثلاً می‌تواند با استفاده از شمارشگری که به‌وسیله فرستنده نگهداری می‌شود، ایجاد و به‌صورت رمزگذاری نشده همراه با پیام محافظت‌شده ارسال شود.

ب- D به دنباله‌ای از بلوک‌های ۱۲۸ بیتی $D_1, D_2, \dots, D_m$ به شکلی که در ادامه می‌آید افراز شود. فرض شود که D_1 اولین 128 بیت از D را در برداشته باشد، D_2 دارای 128 بیت بعدی و الی‌آخر، تا D_m که r بیت پایانی را در بر دارد که $0 < r \le n$. بنابراین D شامل $(m-1)n + r$ بیت است.

پ- فرض شود که $H = e_K(0^{128})$.

ت- اگر $len(S) = 96$ آنگاه فرض شود که $Y_0 = S \,||\, 0^{31} \,||\, 1$ در غیر این صورت فرض شود که

$$Y_0 = G(H, \{\}, S)$$

ث- برای $i = 1,2, \dots, m-1$ دو گام زیر برداشته شود:

۱- فرض شود که $Y_i = inc(Y_{i-1})$؛

۲- فرض شود که $C_i = D_i \oplus e_K(Y_i)$.

ج- فرض شود که $Y_m = inc\,(Y_{m-1})$.

چ- فرض شود که $C_m = D_m \oplus (e_K(Y_m))|_r$.

ح- فرض شود که $T = (G(H, A, C_1||C_2||\dots||C_m) \oplus e_K(Y_0))|_t$.

خروجی حاصل از فرآیند بالا یعنی نسخه رمزگذاری اصالت‌سنجی شده از D باید رشته بیت زیر باشد:

$$C = C_1 \,||\, C_2 \,||\, \dots \,||\, C_m \,||\, T$$

یعنی رشته‌ای از $(m-1)n+r+t$ بیت، که C دقیقاً حاوی t بیت بیشتر از D است (اگرچه ضروری است که متغیر آغازین S که طولی متغیر دارد، و داده رمزگذاری اصالت‌سنجی شده A که طولی متغیر دارد نیز به گیرنده منتقل شود).

۱۱-۷ رویه رمزگشایی

گیرنده برای رمزگشایی و تصدیق رشته رمزگذاری اصالت‌سنجی شده C و تصدیق داده رمزگذاری اصالت‌سنجی شده افزونه A باید گام‌های زیر را بردارد.

الف- اگر طول C کمتر از t است، توقف و در خروجی نامعتبر نمایش‌داده‌شود.

ب- فرض شود اعداد صحیح منحصربه‌فرد m و r طوری تعریف شده‌اند که $len(C) = (m-1)n+r+t$ که $0 < r \leq n$. C به دنباله‌ای از بلوک‌های $C_1, C_2, \dots, C_m, T$ به شکلی که در ادامه می‌آید افراز شود. فرض شود که C_1 شامل n بیت اول C باشد، C_2، حاوی n بیت بعدی باشد و الی‌آخر، تا C_m که r بیت بعدی C را در بر دارد. در انتها فرض شود T، آخرین t بیت از C را داشته باشد.

پ- فرض شود که $H = e_K(0^{128})$.

ت- اگر $len(S) = 96$ باشد فرض شود که $Y_0 = S \,||\, 0^{31} \,||\, 1$ در غیر این صورت فرض شود که

$$Y_0 = G(H, \{\}, S)$$

ث- فرض شود که $T' = (G(H, A, C_1||C_2||\dots||C_m) \oplus e_K(Y_0))|_t$.

ج- اگر $T \neq T'$ توقف و در خروجی نامعتبر نمایش‌داده‌شود.

چ- برای $i = 1, 2, \dots, m-1$ گام‌های زیر برداشته شود:

۱- فرض شود که $Y_i = inc(Y_{i-1})$؛

۲- فرض شود که $D_i = C_i e_K(Y_i)$.

ح- فرض شود که $Y_m = inc(Y_{m-1})$.

خ- فرض شود که $D_m = C_m(e_K(Y_m))|_r$.

د- در خروجی D و داده اصالت‌سنجی شده افزونه A نمایش‌داده‌شود.

پیوست الف
(اطلاعاتی)
راهنمایی برای استفاده از سازوکارها

الف-۱ مقدمه

هدف این پیوست فراهم‌کردن راهنمایی برای استفاده از سازوکارهای تعریف‌شده در این استاندارد ملی است. استفاده از هر سازوکار نیازمند انتخاب پارامترهای مختص به سازوکار است. توصیه‌های مرتبط با انتخاب پارامترها در بخش‌های الف-۳ تا الف-۸ آمده است. در ادامه این قسمت، توصیه‌هایی با توجه به الزامات قابل‌اعمال در تمام سازوکارهای این استاندارد ارائه شده است (به بند ۵ مراجعه شود).

همه سازوکارها نیازمند انتخاب رمز بلوکی از بین رمز بلوک‌های استانداردشده در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷هستند. طول بلوک ($\mathbf{n}$) رمز بلوک باید حداقل ۶۴ باشد و در صورت امکان استفاده از رمز بلوکی با $\mathbf{n = 128}$ توصیه می‌شود. استفاده از رمز بلوکی با $\mathbf{n = 128}$ برای سازوکارهای ۲، ۳ و ۶ اجباری است.

همه سازوکارها همچنین نیازمند این هستند که فرستنده و گیرنده، داده محافظت‌شده کلید محرمانه K را به اشتراک‌گذارند. این کلید تنها باید توسط این دو طرف و احتمالاً توسط طرف‌های سومی[1] که به این منظور، مورد اعتماد فرستنده و گیرنده هستند، شناخته شده باشد. راه‌های زیادی برای ایجاد کلید وجود دارد، اما استفاده از سازوکار ایجاد کلید، مشخص‌شده در ISO/IEC 11770-2 یا استاندارد ملی ایران شماره ۳-۱۰۸۲۲، سال ۱۳۸۷ توصیه می‌شود.

هر شش سازوکار، نیازمند انتخاب طول برچسب هستند. انتخاب این پارامتر، درجه اطمینان گیرنده به یکپارچگی و مبدأ پیام محافظت‌شده را تحت تأثیر قرار می‌دهد. برای جزئیات بیشتر به استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰ مراجعه کنید.

الف-۲ انتخاب سازوکار

گمان می‌رود که همه سازوکارهای این استاندارد درجه بالایی از امنیت را فراهم سازند، اگرچه بعضی از این سازوکارها برای کاربردهای خاص، از بقیه مناسب‌تر هستند. هنگام انتخاب یک سازوکار، واقعیت‌هایی که در جدول ۱ داده شده‌اند و مواردی که در زیر مشخص شده‌اند باید مورد توجه قرار گیرند.

1- Third Parties

جدول الف-۱: ویژگی‌های سازوکارها

شماره سازوکار	۱	۲	۳	۴	۵	۶
تعداد تقریبی عملیات رمز بلوک لازم برای رمزگذاری یک پیام q بیتی	q/n	12[q/n]	2q/n	2q/n	بستگی به روش‌های رمزگذاری و MAC استفاده‌شده دارد	q/n
نیاز احتمالی به مجوزها[1]	بله	خیر	خیر	خیر	بستگی به روش‌های رمزگذاری و MAC استفاده‌شده دارد	خیر
طراحی‌شده به طور خاص برای استفاده با پیام‌های کوتاه	خیر	بله	خیر	خیر	خیر	خیر
طول پیام باید قبل از شروع رمزگذاری مشخص باشد	خیر	خیر	بله	خیر	خیر	خیر
متغیر آغازین نیاز است	بله	خیر	بله	بله	بله	بله
از پیش استاندارد شده است	خیر	بله	بله	خیر	خیر	بله

الف- سازوکارهای سه و چهار روش‌هایی برای ترکیب رمزگذاری بلوکی در حالت CTR (به استاندارد ملی ایران شماره ۹۶۰۰، سال ۱۳۸۶مراجعه شود) با کد اصالت‌سنجی پیام است.

ب- سازوکار پنج روشی برای ترکیب روش‌های استاندارد رمزگذاری و محاسبه MAC فراهم می‌کند. اگر پیاده‌سازی چنین کارکردهایی از پیش در دسترس باشد، سازوکار پنج ممکن است دارای بعضی مزایای پیاده‌سازی باشد.

پ- سازوکار شش برای پیاده‌سازی با سخت‌افزارهایی با گذرداد[2] بالا مناسب است، چرا که می‌تواند بدون تأخیر[3] خط‌لوله[4] پیاده‌سازی شود

الف-۳ سازوکار ۱(OCB 2.0)

این سازوکار نیازمند انتخاب پارامتر طول برچسب t که ($t \leq n$)است. انتخاب طول برچسب t بستگی به محیطی دارد که سازوکار باید در آن استفاده شود. هرچند، درصورتی‌که دلایل قوی برای انتخاب گزینه دیگر نباشد، استفاده از $t \geq 64$ پیشنهاد شده است.

1- Licence
2- High-Throughput
3- Stall
4- Pipeline

الف-۴ سازوکار ۲ (پوشش کلید)

این سازوکار نیازمند این است که رمز بلوک مورد استفاده دارای $n = 128$ باشد. استفاده از رمز بلوکی با این ویژگی که در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷ مشخص‌شده، اجباری است (به قسمت ۵ مراجعه شود).

الف-۵ سازوکار ۳ (CCM)

این سازوکار نیازمند این است که رمز بلوک مورد استفاده دارای $n = 128$ باشد. استفاده از رمز بلوکی با این ویژگی که در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷ مشخص‌شده، اجباری است (به قسمت ۵ مراجعه شود).

این سازوکار نیازمند انتخاب پارامتر طول برچسب t (از بین مجموعه $\{32, 48, 64, 80, 96, 112, 128\}$) است. انتخاب طول برچسب t بستگی به محیطی دارد که سازوکار باید در آن استفاده شود. هرچند، درصورتی‌که دلایل قوی برای انتخاب گزینه دیگر نباشد، استفاده از $t \geq 64$ پیشنهاد شده است.

این سازوکار نیازمند انتخاب طول w (به‌صورت هشتایی) از فیلد پیام (از مجموعه$\{2, 3, 4, 5,6,7,8\}$) است. انتخاب طول هشتایی فیلد طول پیام w نیز به محیطی که سازوکار باید در آن استفاده شود بستگی دارد. انتخاب طول هشتایی، سطح امنیتی را که توسط این سازوکار فراهم می‌شود، تحت تأثیر قرار نمی‌دهد. مقادیر بزرگ‌تر w طول پیام بزرگ‌تر را فراهم می‌کنند و درعین‌حال طول باقی‌مانده متغیر آغازین را کاهش می‌دهند. بااین‌وجود حتی اگر w با بیش‌ترین مقدار ممکن انتخاب شود، یعنی $w = 8$ باشد، ۵۶ بیت از متغیر آغازین به‌منظور اطمینان از به‌کارگیری متغیرهای آغازین مختلف برای هر پیام، می‌تواند استفاده شود که برای بیشتر کاربردهای عملی و نه همه ، باید کافی باشد. برای اکثر کاربردها، مقدار $w = 4$، که حداکثر طول پیام 2^{32} معادل تقریباً هشتایی 4×10^9 را میسر می‌سازد، به نظر می‌رسد کافی باشد.

الف-۶ سازوکار چهار(EAX)

این سازوکار نیازمند انتخاب پارامتر طول برچسب t است که ($t \leq n$). انتخاب طول برچسب t بستگی به محیطی دارد که سازوکار باید در آن استفاده شود. هرچند درصورتی‌که دلایل قوی برای انتخاب گزینه دیگر نباشد، استفاده از $t \geq 64$ پیشنهاد شده است.

الف-۷ سازوکار پنج (رمزگذاری سپس MAC)

این سازوکار نیازمند انتخاب حالت عملیات و روش محاسبه MAC است. امنیتی که به‌وسیله طرح‌واره‌ی رمزگذاری اصالت‌سنجی شده فراهم می‌شود بستگی به امنیت اولیه اساسی[1] دارد.

صرف نظر از حالت رمزگذاری انتخاب‌شده، استفاده از متغیر آغازین یکنواخت به طور تصادفی انتخاب‌شده از مجموعه متغیرهای آغازین ممکن به شدت توصیه می‌شود. اگر این توصیه پیروی نشود، نتیجه Bellare و

1- Underlying primitive

Namprempre (به یادآوری بند ۱۰-۱ مراجعه شود) خواهد شد. علاوه بر این، در برخی شرایط، امکان حمله وجود دارد. در این ارتباط توجه داشته باشید که، برای حالت CBC، پیوست ب-۲-۱ استاندارد ISO / IEC 10116 بیان می‌کند که «متغیر آغازین آماری منحصر به فرد به طور تصادفی انتخاب‌شده توصیه می شود».

انتخاب فن MAC باید زمینه استفاده از فن رمزگذاری اصالت‌سنجی‌شده را ئر نظر گیرد و توصیه‌های ارائه‌شده در ISO/IEC 9797 باید به دقت پیروی شود. به طور خاص، اگر رمز بلوکی MAC بر اساس ISO/IEC 9797-1 انتخاب شده است،: (الف) اگر طول پیام ثابت است، تنها باید از الگوریتم MAC 1 استفاده شود و (ب) روش لایه گذاری ۱تنها اگر طول پیام ثابت است باید مورد استفاده قرار گیرد.

الف-۸ سازوکار شش (GCM)

این سازوکار نیازمند این است که رمز بلوک مورد استفاده دارای $n = 128$ باشد. استفاده از رمز بلوکی با این ویژگی که در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷مشخص‌شده، اجباری است (به قسمت ۵ مراجعه شود).

متغیر آغازین S با طول متغیر باید طوری انتخاب شود که $1 \leq \text{len}(S) \leq 2^{64}$. این نیازمندی که متغیرهای آغازین هرگز نباید در طول دوره زندگی[1] یک کلید استفاده مجدد شوند، برای امنیت این سازوکار حیاتی است.

طول برچسب t باید طوری انتخاب شود که t مضربی از ۸ باشد و شرط $96 \leq t \leq 128$ را برآورده کند(t=32 و t=64 نیز برای بعضی از کاربردهای خاص مجاز هستند، هرچند این گزینه‌ها بهتر است با دقت بالایی استفاده شوند. راهنمای تفصیلی استفاده از این طول برچسب‌ها در پیوست C از [۸] آمده است).

رشته داده‌ایD که سازوکار رمزگذاری اصالت‌سنجی شده باید به آن اعمال شود باید شرط $\text{len}(D) \leq 2^{39} - 256$ را داشته باشد و رشته داده اصالت‌سنجی شده افزونه A باید شرط $len(A) \leq 2^{64}$ را برآورده کند. مجموع تعداد بلوک‌های داده و بلوک‌های داده اصالت‌سنجی شده افزونه که سازوکار CGM باید به آن اعمال شود، برای یک کلید ثابت K باید حداکثر 2^{64} باشد. همچنین مجموع فراخوانی‌های رویه رمزگذاری برای هر کلید باید حداکثر 2^{32} باشد، مگر آنکه برای هر استفاده از آن کلید $\text{len}(S) = 96$ باشد.

1- Lifetime

پیوست ب
(اطلاعاتی)
مثال‌ها

ب-۱ مقدمه

این پیوست شامل مثال‌های کارکرده از عملیات سازوکارهای مشخص‌شده در این استاندارد ملی است.

ب-۲ سازوکار یک (OCB 2.0)

پنج مثال زیر از سه‌تایی‌های پیام(D)، متن‌رمزگذاری شده (C)، و برچسب (T) همگی با استفاده از رمز بلوک AES، در هر مورد با استفاده از $t = 128$ تولید شده‌اند. مثال‌ها با استفاده از نشانه‌گذاری شانزده‌تایی ارائه‌شده‌اند. برای هر یک از این پنج مثال، کلید K و متغیر آغازین S یکسانی که در زیر مشخص شده‌اند، به‌کار گرفته شده است.

K: 000102030405060708090A0B0C0D0E0F
S: 000102030405060708090A0B0C0D0E0F

D_1: 0001020304050607
C_1: C636B3A868F429BB
T_1: A45F5FDEA5C088D1D7C8BE37CABC8C5C

D_2: 000102030405060708090A0B0C0D0E0F
C_2: 52E48F5D19FE2D9869F0C4A4B3D2BE57
T_2: F7EE49AE7AA5B5E6645DB6B3966136F9

D_3: 000102030405060708090A0B0C0D0E0F
1011121314151617
C_3: F75D6BC8B4DC8D66B836A2B08B32A636
CC579E145D323BEB
T_3: A1A50F822819D6E0A216784AC24AC84C

D_4: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
C_4: F75D6BC8B4DC8D66B836A2B08B32A636
CEC3C555037571709DA25E1BB0421A27
T_4: 09CA6C73F0B5C6C5FD587122D75F2AA3

D_5: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
2021222324252627

C_5: F75D6BC8B4DC8D66B836A2B08B32A636
9F1CD3C5228D79FD6C267F5F6AA7B231
C7DFB9D59951AE9C

T_5: 9DB0CDF880F73E3E10D4EB3217766688

ب-۳ سازوکار دو (پوشش کلید)

مثال‌های عملیات این سازوکار با رمز بلوک AES در [۱۱] آورده شده است.

ب-۴ سازوکار سه (CCM)

شش مثال زیر از سه‌تایی‌های پیام(D_i)، متن‌رمزگذاری شده (C_i)، و برچسب (T_i) همگی با استفاده از رمز بلوک AES، در هر مورد با استفاده از $t = 128$ و $w = 2$ تولید شده‌اند(بنابراین S باید ۱۰۴ بیت داشته باشد). مثال-ها با استفاده از نشانه‌گذاری شانزده‌تایی ارائه شده‌اند. برای هر یک از این پنج مثال کلید K و متغیر آغازین S یکسانی که در زیر مشخص شده‌اند، به‌کار گرفته شده است.

K: 000102030405060708090A0B0C0D0E0F
S: 000102030405060708090A0B0C

D_1: رشته تهی

C_1: رشته تهی

T_1: 54C92FE45510D6B3B0D46EAC2FEE8E63

D_2: 0001020304050607
C_2: 1635B68B570CFC85
T_2: 2734A0447531C02916CF8B9A494C3AD1

D_3: 000102030405060708090A0B0C0D0E0F
C_3: 1635B68B570CFC85529E39AC913910D7
T_3: C7C5C394B685B08B3F00DCD81256F0D0

D_4: 000102030405060708090A0B0C0D0E0F
1011121314151617
C_4: 1635B68B570CFC85529E39AC913910D7
F3111631623867F1
T_4: BB85D5BEEA595F573A9B4733D3E04887

D_5: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
C_5: 1635B68B570CFC85529E39AC913910D7
F3111631623867F134E6E441904FD504
T_5: C80A98AAFDFF79C23FB4D775A71C29D0

D_6: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
2021222324252627
C_6: 1635B68B570CFC85529E39AC913910D7
F3111631623867F134E6E441904FD504

F5746D6BF189815F
T_6: 1A6F75C612B703E25E47260BABCCB06E

یادآوری- مثال‌های بیشتری از اجرای این سازوکار با رمز بلوک AES در [۱۲] آمده است.

ب-۵ سازوکار چهار(EAX)

شش مثال زیر از سه‌تایی‌های پیام(D_i)، متن‌رمزگذاری شده (C_i)، و برچسب (T_i) همگی با استفاده از رمز بلوک AES، در هر مورد با استفاده از $t = 128$ تولید شده‌اند. مثال‌ها با استفاده از نشانه‌گذاری شانزده‌تایی ارائه‌شده‌اند. برای هر یک از این پنج مثال کلید K و متغیر آغازین S یکسانی که در زیر مشخص شده‌اند، به‌کار گرفته شده است.

K: 000102030405060708090A0B0C0D0E0F
S: 000102030405060708090A0B0C0D0E0F

D_1: رشته تهی

C_1: رشته تهی

T_1: 1CE10D3EFFD4CADBE2E44B58D60AB9EC

D_2: 0001020304050607
C_2: 29D878D1A3BE857B
T_2: 9E1F336E2D9058EE57BF181EDF49395B

D_3: 000102030405060708090A0B0C0D0E0F
C_3: 29D878D1A3BE857B6FB8C8EA5950A778
T_3: BD55E38C169E77135C2AE42309004C04

D_4: 000102030405060708090A0B0C0D0E0F
1011121314151617
C_4: 29D878D1A3BE857B6FB8C8EA5950A778
331FBF2CCF33986F
T_4: 7E72C073D72CB70D1129C56FA0794573

D_5: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
C_5: 29D878D1A3BE857B6FB8C8EA5950A778
331FBF2CCF33986F35E8CF121DCB30BC
T_5: EF07F23F26E1DC3BEEFF83B18A9E2687

D_6: 000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
2021222324252627
C_6: 29D878D1A3BE857B6FB8C8EA5950A778
331FBF2CCF33986F35E8CF121DCB30BC
5C87F59B057A40E9
T_6: A0FA15E39A14811AE5AC0E7353C2BAB6

یادآوری- مثال‌های بیشتر از عملیات این سازوکار با رمز بلوک AES در [۱۳] آمده است.

ب-۶ سازوکار پنج (رمزگذاری سپس MAC)

خواننده به استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰ و استاندارد ملی ایران شماره ۹۶۰۰، سال ۱۳۸۶ ارجاع داده می‌شود.

ب-۷ سازوکار شش (GCM)

دو مثال زیر از سه‌تایی‌های پیام(D_i)، متن‌رمزگذاری شده (C_i)، و برچسب (T_i) همگی با استفاده از رمز بلوک AES، در هر مورد با استفاده از $t = 128$ و داده اصالت‌سنجی شده افزونه که شامل رشته تهی است، تولیدشده‌اند. مثال‌ها با استفاده از نشانه‌گذاری شانزده‌تایی ارائه شده‌اند. برای هر یک از این مثال‌ها کلید K و متغیر آغازین S یکسانی که در زیر مشخص شده‌اند، به‌کار گرفته شده است.

K: 00000000000000000000000000000000
S: 000000000000000000000000

D_1: رشته تهی

C_1: رشته تهی

T_1: 58e2fccefa7e3061367f1d57a4e7455a

D_2: 00000000000000000000000000000000
C_2: 0388dace60b6a392f328c2b971b2fe78
T_2: ab6e47d42cec13bdf53a67b21257bddf

یادآوری- مثال‌های بیشتر از عملیات این سازوکار با رمز بلوک AES در مرجع [۸] آمده است.

پیوست پ
(الزامی)
پیمانه ASN.1

پ-۱ تعریف صوری

```
AuthenticatedEncryption {
iso(1) standard(0) authenticated-encryption(19772) asn1-module(0)
authenticated-encryption-mechanisms(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER
AuthenticatedEncryptionMechanism ALGORITHM ::= {
ae-mechanism1 |
ae-mechanism2 |
ae-mechanism3 |
ae-mechanism4 |
ae-mechanism5 |
ae-mechanism6
}
-- Synonyms --
is19772 OID ::= { iso(1) standard(0) authenticated-encryption(19772) }
mechanism OID ::= { is19772 mechanisms(1) }
ae-mechanism1 OID ::= { mechanism 1 }
ae-mechanism2 OID ::= { mechanism 2 }
ae-mechanism3 OID ::= { mechanism 3 }
ae-mechanism4 OID ::= { mechanism 4 }
ae-mechanism5 OID ::= { mechanism 5 }
ae-mechanism6 OID ::= { mechanism 6 }
END -- AuthenticatedEncryption --
```

پ-۲ استفاده از شناسه‌های شی پَسین

هر یک از سازوکارهای اصالت‌سنجی که در این استاندارد مشخص شده‌اند از یک الگوریتم رمزگذاری بلوکی استفاده می‌کنند و در مورد سازوکار پنج، حالت عملیات متناظر و الگوریتم MAC نیز استفاده می‌شوند. بنابراین، مجاز است شناسه شی سازوکار رمزگذاری اصالت‌سنجی شده که با یکی از شناسه‌های الگوریتم سازوکار رمزگذاری بلوکی که در استاندارد ملی ایران شماره ۳-۱۰۸۲۴، سال ۱۳۸۷ آمده است و پارامترهای متناظر، دنبال شود.در مورد سازوکار پنج، شناسه الگوریتم حالت عملیات رمز بلوک انتخاب‌شده (استاندارد ملی ایران شماره ۹۶۰۰، سال ۱۳۸۶) و الگوریتم MAC (از استاندارد ملی ایران شماره ۱-۹۷۹۷، سال ۱۳۹۰) نیز مجازند که فراهم شوند.

کتاب‌نامه

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

[2] M. Bellare and C. Namprempre, 'Authenticated encryption: Relations among notions and analysis ofthe generic composition paradigm'. In: T. Okamoto (ed.), Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings. Lecture Notes in Computer Science 1976, Springer-Verlag (2000) pp. 531-545.

[3] M. Bellare, P. Rogaway and D. Wagner, 'The EAX mode of operation'. In: B. K. Roy, W. Meier (eds.): Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. Lecture Notes in Computer Science 3017, Springer-Verlag (2004) pp.389-407.

[4] ISO/IEC 10118 (all parts), Information technology — Security techniques — Hash-functions

[5] ISO/IEC 11770 (all parts), Information technology — Security techniques — Key management

[6] ISO/IEC 18033-1:2005, Information technology — Security techniques — Encryption algorithms — Part 1: General

[7] T. Krovetz and P. Rogaway, The OCB Authenticated-Encryption Algorithm, IETF draft draft-krovetzocb- 00.txt, March 2005

[8] National Institute of Standards and Technology, NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. November 2007.

[9] National Institute of Standards and Technology, AES Key Wrap Specification. NIST, November 2001

[10] National Institute of Standards and Technology, NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode For Authentication and Confidentiality. May 2004

[11] J. Schaad and R. Housley, RFC 3394: Advanced Encryption Standard (AES): Key Wrap Algorithm. IETF, September 2002

[12] D. Whiting, R. Housley and N. Ferguson, RFC 3610: Counter with CBC-MAC (CCM). IETF, September 2003