INSO
10824-1
1st. Revision
2017
Identical with
18033-1: ISO/IEC
2015

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

استاندارد ملی ایران
۱۰۸۲۴-۱
تجدیدنظر اول
۱۳۹۵

فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۱: کلیات

Information technology- Security techniques- Encryption algorithms– Part 1: General

ICS: 35.030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج- ایران

تلفن: ۸-۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.gov.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No. 2592 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.gov.ir

Website: http://www.isiri.gov.ir

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 می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند 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 بین‌المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات 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 می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی 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 سیستم های 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، گواهی‌نامه تایید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. 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- الگوریتم‌های رمزگذاری- قسمت ۱: کلیات»

«تجدیدنظر اول»

رئیس:	**سمت و/یا محل اشتغال:**
نامجو، احسان (دکترای مخابرات)	هیأت علمی دانشگاه شهید چمران اهواز
دبیر:	
آرین‌نژاد، حسین (کارشناسی مهندسی برق- الکترونیک)	کارشناس تدوین اداره کل استاندارد خوزستان
اعضا: (اسامی به ترتیب حروف الفبا)	
خادم، حامد (کارشناسی مهندسی فناوری اطلاعات)	کارشناس فناوری اطلاعات اداره کل استاندارد خوزستان
خدابخشی، مونا (کارشناسی ارشد مهندسی برق- قدرت)	شرکت ایزی ارتباط پارس
داوودزاده، سیدمجتبی (کارشناسی مهندسی برق- الکترونیک)	اداره کل تنظیم مقررات و ارتباطات رادیویی
دهقانیان، یحیی (کارشناسی ارشد مهندسی برق – مخابرات)	انجمن رمز ایران (آفتا)
رفیعی، مهناز (دکترای کامپیوتر- سخت افزار)	هیأت علمی دانشگاه آزاد اسلامی واحد رامهرمز
رضازاده، آرشین (کارشناسی ارشد مهندسی کامپیوتر)	هیأت علمی دانشگاه شهید چمران اهواز
شهاوند، طیبه (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس ارشد- معاونت فناوری اطلاعات دادگستری خوزستان
عنصری‌نیا، سعید (کارشناسی مهندسی کامپیوتر- سخت افزار)	مشاور فنی- شرکت ملی مناطق نفت‌خیز جنوب

اعضا: (اسامی به ترتیب حروف الفبا)	**سمت و/یا محل اشتغال:**
فرهانی‌پور، مبین (کارشناسی ارشد مهندسی برق- مخابرات)	کارشناس فنی- صدا و سیما آبادان
موجبی، محمود (کارشناسی ارشد مهندسی مخابرات- رمز)	سازمان ملی فناوری اطلاعات ایران
مهتدی، محمد (کارشناسی مهندسی برق- الکترونیک)	اداره کل تنظیم مقررات و ارتباطات رادیویی
مولوی، اردشیر (کارشناسی مهندسی برق- مخابرات)	کارشناس سوئیچ- شرکت ارتباطات زیرساخت

ویراستار:

ترابی، مهرنوش (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس استاندارد

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۱: کلیات» که نخستین‌بار در سال ۱۳۸۷ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تأیید کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره‌شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ برای نخستین بار مورد تجدیدنظر قرار گرفت و در چهارصد و هشتاد و دومین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۱۲/۱۸ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ هم‌گامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهد 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 تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۴: سال ۱۳۸۷ می‌شود.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 18033-1: 2015, Information technology- Security techniques- Encryption algorithms- Part 1: General

مقدمه

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران به شمارهٔ ۱۰۸۲۴ است.

سایر قسمت‌های این مجموعه عبارتند از:

- ISO/IEC 18033-2: 2015, Information technology- Security techniques- Encryption algorithms- Part 2: Asymmetric ciphers

– استاندارد ملی ایران شمارهٔ ۳-۱۸۰۳۳: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزنگاری- قسمت ۳: رمزهای قالبی

– استاندارد ملی ایران شمارهٔ ۴-۱۸۰۳۳: سال ۱۳۸۷، فناوری اطلاعات- فنون امنیتی الگوریتم‌های رمزنگاری- قسمت ۴: رمزگذاری جریانی

- ISO/IEC 18033-5: 2015, Information technology- Security techniques- Encryption algorithms- Part 5: Identity-based ciphers

این مجموعه استاندارد ملی سامانه‌های رمزگذاری (رمزهایی) را برای هدف محرمانگی داده‌ها مشخص می‌کند. هدف قرارگیری رمزها در این استاندارد ملی، ترویج استفاده از آن‌ها به عنوان به‌روزترین فناوری در فنون رمزگذاری می‌باشد.

هدف اصلی فنون رمزگذاری حفاظت از محرمانگی داده‌های ذخیره‌شده یا داده‌های مخابره‌شده است. یک الگوریتم رمزگذاری، به داده‌ها (اغلب متن اصلی یا متن آشکار نامیده می‌شود) اعمال می‌شود تا داده‌های رمزگذاری‌شده حاصل شود (یا متن رمز)، این فرایند رمزگذاری نامیده می‌شود. بهتر است الگوریتم‌های رمزگذاری به شکلی طراحی شوند که هیچ‌گونه اطلاعاتی از متن رمز در رابطه با متن اصلی مگر احتمالا طول آن حاصل نشود. همراه با هر الگوریتم رمزگذاری یک الگوریتم رمزگشایی نیز وجود دارد، که متن رمز را به متن اصلی اولیه برمی‌گرداند.

رمزها همراه با یک کلید عمل می‌کنند. در رمز نامتقارن، کلیدهایی متفاوت ولی مرتبط به هم برای رمزگذاری و رمزگشایی استفاده می‌شوند. در این مجموعه استاندارد ملی، استاندارد ISO/IEC 18033-2 و استاندارد ISO/IEC 18033-5 به دو طبقه متفاوت از رمزهای نامتقارن اختصاص دارند که رمزهای نامتقارن مرسوم (یا صرفا رمزهای نامتقارن) و رمزهای شناسه‌مبنا معروفند. استانداردهای ISO/IEC 18033-3 و ISO/IEC 18033-4 به دو طبقه متفاوت از رمزهای متقارن اختصاص دارند که به رمزهای قالبی و رمزهای جریانی معروفند.

فناوری اطلاعات- فنون امنیتی- الگوریتم‌های رمزگذاری- قسمت ۱: کلیات

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعریف اصطلاحات مورد استفاده در قسمت‌های بعدی این مجموعه استاندارد است. اهمیت رمزگذاری تعریف‌شده و برخی ازجنبه‌های عمومی استفاده و خصوصیات آن توصیف می‌شود. معیارهای مورد استفاده جهت گزینش الگوریتم‌هایی که در سایر قسمت‌های این استاندارد مشخص می‌شوند، در پیوست الف و ب تعیین می‌شود.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات با تعاریف زیر به‌کار می‌رود:

۲-۱

رمز نامتقارن

asymmetric cipher

اصطلاحی جایگزین برای سامانه رمزگذاری نامتقارن است.

۲-۲

فن رمزنگاشتی نامتقارن

asymmetric cryptographic technique

نوعی فن رمزنگاشتی که از دو تبدیل وابسته به هم استفاده می‌کند، یک تبدیل عمومی (تعریف‌شده توسط کلید عمومی) ویک تبدیل خصوصی (تعریف‌شده توسط کلید خصوصی) می‌باشد.

یادآوری- دو تابع تبدیل دارای این ویژگی هستند که با معین بودن تبدیل عمومی، استنتاج تبدیل خصوصی از نظر محاسباتی غیرعملی است.

[منبع: زیربند ۲-۱ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۲: سال ۱۳۹۲]

۲-۳

سامانه رمزگذاری نامتقارن

asymmetric encipherment system

اصطلاحی جایگزین برای سامانه رمزگذاری نامتقارن است.

۴-۲

سامانه رمزگذاری نامتقارن

asymmetric encryption system

سامانه‌ای مبتنی بر فنون رمزنگاشتی نامتقارن است که تبدیل عمومی آن برای رمزگذاری و تبدیل خصوصی آن برای رمزگشایی استفاده می‌شود.

[منبع: زیربند۳-۲ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۵: سال ۱۳۹۱]

۵-۲

زوج کلید نامتقارن

asymmetric key pair

زوج کلیدی وابسته به هم در فن رمزنگاشتی نامتقارن بوده که کلید خصوصی تبدیل خصوصی و کلید عمومی تبدیل عمومی را تعریف می‌کند.

۶-۲

حمله

attack

الگوریتمی که محاسباتی را انجام داده و برای رمزگذاری و/یا رمزگشایی متون منتخب وفقی با یک کلید مخفی، پرسمانی در الگوریتم رمزگذاری اجرا می‌کند، با این هدف که متن اصلی نامعلوم را برای یک متن رمز معین بازیابی نماید که ممکن است متن رمز به‌طور منتخب وفقی انتخاب شده، اما پرسمان رمزگشایی برای آن صادر نشده باشد یا با این هدف که کلید رمز را بازیابی نماید.

۷-۲

ارزش حمله

attack cost

نسبت متوسط پیچیدگی الگوریتم حمله است که بر حسب تعداد دفعات فراخوانی الگوریتم رمزگذاری توسط حمله به احتمال موفقیت حمله اندازه‌گیری می‌شود.

یادآوری- با استفاده از نشان‌گذاری تعریف‌شده در زیربند ۳-۱ ارزش حمله معادل با نسبت W/P می‌باشد.

۸-۲

قالب

block

رشته‌ای از بیت‌ها با طولی معین است.

۹-۲

رمز قالبی

block cipher

سامانه رمزگذاری متقارن با این خصوصیت که الگوریتم رمزگذاری بر روی قالبی از متن اصلی عمل می‌کند، یعنی برروی رشته‌ای از بیت‌ها با طولی معین، تا قالبی از متن رمز تولید نماید.

۱۰-۲

رمز

cipher

اصطلاح جایگزین برای سامانه رمزگذاری است.

۱۱-۲

متن رمز

ciphertext

داده‌ای که جهت مخفی نمودن محتویاتش تغییر شکل یافته است.

[منبع: زیربند ۳-۳ استاندارد ملی ایران شمارهٔ ۹۶۰۰: سال ۱۳۸۶]

۱۲-۲

متن آشکار

cleartext

اصطلاحی جایگزین برای متن اصلی است.

۱۳-۲

حمله تحلیل رمز

cryptanalytic attack

حمله‌ای برعلیه رمز با استفاده از خصوصیات آن می‌باشد.

یادآوری ۱- هر حمله تحلیل رمز دارای مدل حمله خاص خود است، بعضی از مدل‌ها ممکن است در پیاده‌سازی‌های خاص قابل اجرا یا غیرقابل اجرا باشند. نظر به این‌که زمینه به‌کارگیری رمز برای طراح آن نامعلوم است، هنگام ارزیابی امنیت یک الگوریتم، همه مدل‌های تک کلیدی، مورد ملاحظه قرار می‌گیرند.

یادآوری ۲- حملات تحلیل رمز شامل پیاده‌سازی حملات خاص مانند حمله تحلیل کانال جانبی نیستند.

۲-۱۴

رمزبرداری

decipherment

اصطلاحی جایگزین برای رمزگشایی است.

۲-۱۵

الگوریتم رمزبرداری

decipherment algorithm

اصطلاحی جایگزین برای الگوریتم رمزگشایی است.

۲-۱۶

رمزگشایی

decryption

معکوس عمل رمزگذاری متناظر است.

[منبع: زیربند ۲-۶ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۲: سال ۱۳۹۲]

۲-۱۷

الگوریتم رمزگشایی

decryption algorithm

فرایندی که متن رمز را به متن اصلی تبدیل می‌کند.

۲-۱۸

رمزگذاری

encipherment

اصطلاحی جایگزین برای رمزگذاری است.

۲-۱۹

الگوریتم رمزگذاری

encipherment algorithm

اصطلاحی جایگزین برای الگوریتم رمزگذاری است.

۲-۲۰

سامانه رمزگذاری

encipherment system

اصطلاحی جایگزین برای سامانه رمزگذاری است.

۲-۲۱

رمزگذاری

encryption

تبدیل (معکوس‌پذیر) داده‌ها توسط یک الگوریتم رمزنگاشتی جهت تولید متن رمز یعنی جهت مخفی نمودن محتوای اطلاعات داده‌ها می‌باشد.

[منبع: زیربند ۳-۶ استاندارد ملی ایران شمارهٔ ۱-۹۷۹۷: سال ۱۳۹۱]

۲-۲۲

الگوریتم رمزگذاری

encryption algorithm

فرایندی که متن اصلی را به متن رمز تبدیل می‌کند.

۲-۲۳

سامانه رمزگذاری

encryption system

فنی رمزنگاشتی که برای محافظت از محرمانگی داده‌ها استفاده می‌شود و از سه فرایند جزئی تشکیل شده است که شامل الگوریتم رمزگذاری، الگوریتم رمزگشایی و روشی برای تولید کلیدها می‌باشد.

۲-۲۴

حمله عام

generic attack

حمله‌ای برعلیه رمز که متکی به ساختار رمز نبوده و می‌تواند جهت بازیابی کلید رمز یا متن اصلی استفاده شود.

۲-۲۵

رمز شناسه‌مبنا

identity-based cipher

اصطلاحی جایگزین برای سامانه رمزگذاری شناسه‌مبنا است.

۲-۲۶

سامانه رمزگذاری شناسه‌مبنا

identity-based encryption system

رمزی نامتقارن که در آن الگوریتم رمزگذاری رشته‌ای دلخواه را به عنوان کلید عمومی اتخاذ می‌کند.

۲-۲۷

کلید

key

دنباله‌ای از نمادها که عملیات تبدیل رمزنگاشتی (مانند رمزگذاری و رمزبرداری) را کنترل می‌کند.

[منبع: زیربند ۲-۱۲ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۲: سال ۱۳۹۲]

۲-۲۸

کلید جریانی

keystream

دنباله‌ای شبه‌تصادفی از نمادها با قید محرمانه بودن که توسط الگوریتم‌های رمزگذاری و رمزگشایی یک رمز جریانی استفاده می‌شود.

یادآوری- اگر بخشی از کلید جریانی توسط مهاجم کشف شود باید استنباط کردن اطلاعاتی درباره مابقی کلید جریانی برای مهاجم از لحاظ محاسباتی غیرعملی باشد.

۲-۲۹

رمز قالبی n بیتی

***n*-bit block cipher**

رمزی قالبی با این خصوصیت است که طول قالب‌های متن اصلی و متن رمز n بیت است.

[منبع: زیربند ۳-۱۰ استاندارد ملی ایران شمارهٔ ۱-۹۷۹۷: سال ۱۳۹۱]

۲-۳۰

متن اصلی

plaintext

اطلاعات رمزگذاری نشده است.

[منبع: زیربند ۳-۱۱ استاندارد ملی ایران شمارهٔ ۱-۹۷۹۷: سال ۱۳۹۱]

۲-۳۱

کلید خصوصی

private key

کلیدی از زوج کلید نامتقارن یک هستار که توصیه می‌شود صرفا توسط همان هستار استفاده شود.

یادآوری- توصیه می‌شود کلید خصوصی به شیوه معمول اعلام نشود.

[منبع: زیربند ۲-۳۵ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۲: سال ۱۳۹۲]

۲-۳۲

کلید عمومی

public key

کلیدی از زوج کلید نامتقارن یک هستار با امکان علنی شدن است.

[منبع: زیربند ۲-۳۶ استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۲: سال ۱۳۹۲]

۲-۳۳

کلید مخفی

secret key

کلیدی که در فنون رمزنگاشتی متقارن توسط مجموعه‌ای مشخص از هستارها استفاده می‌شود.

[منبع: زیربند ۲ -۳۵ استاندارد ملی ایران شمارهٔ ۳-۱۰۸۲۲: سال ۱۳۹۰]

۲-۳۴

قدرت امنیتی

security strength

عددی وابسته به حجم کار (مثلا تعداد عملیات) که جهت شکست یک الگوریتم یا سامانه رمزنگاشتی نیاز است.

یادآوری ۱- در بازیابی کلید رمز، قدرت امنیتی n بیتی به این معناست که حجم کار مورد نیاز جهت شکست سامانه رمز معادل با 2^n بار اجرای سامانه رمز است. برای اطلاعات بیشتر در رابطه با کاربرد قدرت امنیتی جهت انتخاب الگوریتم‌های رمزنگاشتی برای این مجموعه استاندارد ملی به زیربند ۱-۴ پیوست پ رجوع شود.

یادآوری ۲- در استاندارد ISO/IEC 29192 قدرت امنیتی برحسب بیت مشخص شده است، مثلا ۸۰، ۱۱۲، ۱۲۸، ۱۹۲ یا ۲۵۶.

۲-۳۵

رمز جریانی خود هم‌زمان

self-synchronous stream cipher

رمزی جریانی با این خصوصیت که نمادهای کلید جریانی به صورت تابعی از یک کلید مخفی و تعداد ثابتی از بیت‌های متن رمز قبلی تولید می‌شوند.

۲-۳۶

رمز جریانی

stream cipher

سامانه رمزگذاری متقارن با این خصوصیت که الگوریتم رمزگذاری، دنباله‌ای از نمادهای متن خام و دنباله‌ای از نمادهای کلید جریانی را با استفاده از یک تابع معکوس‌پذیر، نماد به نماد ترکیب می‌کند.

یادآوری- دونوع رمز جریانی قابل شناخت است. رمزهای جریانی هم‌زمان و رمزهای جریانی خود هم‌زمان، که باتوجه به روش مورد استفاده برای دریافت کلید جریانی تفکیک می‌شوند.

۲-۳۷

رمز متقارن

symmetric cipher

اصطلاحی جایگزین برای سامانه رمزگذاری متقارن است.

۲-۳۸

فن رمزنگاشتی متقارن

symmetric cryptographic technique

فنی رمزنگاشتی که از یک کلید مخفی یکسان برای هردو تبدیل صادرکننده[1] و گیرنده استفاده می‌کند.

یادآوری- بدون اطلاع از کلید مخفی، محاسبه کردن هریک از تبدیل‌های صادرکننده و گیرنده پیام از لحاظ محاسباتی غیرعملی است.

۲-۳۹

سامانه رمزگذاری متقارن

symmetric encipherment system

اصطلاحی جایگزین برای سامانه رمزگذاری متقارن است.

1- Originator

۲-۴۰

سامانه رمزگذاری متقارن

symmetric encryption system

سامانه رمزگذاری مبتنی بر فنون رمزنگاشتی متقارن است.

۲-۴۱

رمز جریانی هم‌زمان

synchronous stream cipher

رمزی جریانی با این خصوصیت که نمادهای کلید جریانی بر حسب تابعی از کلید مخفی و احتمالا یک بـردار مقداردهی اولیه مستقل از متن اصلی و متن رمز تولید می‌شوند.

۳ نمادها و کوته نوشت‌ها

این بند فهرستی از نمادها و کوته نوشت‌های لازم را برای درک و/یا کاربرد بهتر استاندارد ارائه می‌دهد.

۳-۱ نمادها

n عدد صحیح

P احتمال موفقیت یک حمله برعلیه یک الگوریتم رمزنگاشتی

W حجم کار یا پیچیدگی یک حمله که بر حسب تعداد دفعات فراخوانی الگـوریتم رمزنگاشـتی محاسـبه می‌شود.

۳-۲ کوته نوشت‌ها

این بند فهرستی از نمادها و کوته نوشت‌های لازم را برای درک و/یا کاربرد بهتر استاندارد ارائه می‌دهد.

ECB	Electronic Codebook	کتاب‌کد الکترونیکی
MAC	Message Authentication Code	کد احراز اصالت پیام
SC	Sub Committee	کمیته فرعی
SD	Standing Document	سند معتبر
WG	Working Group	کارگروه

۴ ماهیت رمزگذاری

۴-۱ هدف از رمزگذاری

هدف اصلی سامانه‌های رمزگذاری حفاظت از محرمانگی داده‌های ذخیره‌شده یا مخابره‌شده است. این هدف توسط الگوریتم‌های رمزگذاری با تبدیل متن اصلی به متن رمز انجام می‌شود، که دست‌یابی به هرگونه اطلاعاتی در رابطه با محتوای متن اصلی از طریق متن رمز از لحاظ محاسباتی غیرعملی است، مگر آن‌که کلید رمزگشایی معلوم باشد. البته در بسیاری موارد، طول متن اصلی توسط رمزگذاری پنهان نمی‌شود، زیرا طول متن رمز معمولا برابر و یا کمی بیشتر از طول متن اصلی متناظر است.

لازم به ذکر است که رمزگذاری به تنهایی، همیشه قادر به محافظت از یکپارچگی یا اصالت داده‌ها نیست. در بسیاری موارد ممکن است دستکاری نمودن متن رمز، بدون در اختیار داشتن کلید، با اثرات قابل پیش‌بینی بر متن اصلی همراه باشد. غالبا به منظور اطمینان از یکپارچگی و اصالت داده‌ها، باید فنونی اضافی همانند فنون توصیف‌شده در استانداردهای ISO/IEC 9796، ISO/IEC 9797، ISO/IEC 14888، ISO/IEC 19772، ISO/IEC 29192 استفاده شود.

۴-۲ سامانه‌های رمز متقارن و نامتقارن

عملکرد رمزها وابسته به کلید است.

- در رمز متقارن، از یک کلید مخفی یکسان، به همراه هر دو الگوریتم رمزگذاری و رمزگشایی استفاده می‌شود. اطلاع از کلید مذکور برای انجام رمزگذاری و رمزگشایی ضروری است، از این رو اطلاع از کلید مخفی باید محدود به طرفینی باشد که مجازند به اطلاعات مورد رمزگذاری توسط آن دسترسی داشته باشند.

- در رمز نامتقارن، کلیدهایی متفاوت اما مرتبط به هم برای رمزگذاری و رمزگشایی استفاده می‌شوند. بنابراین کلیدها به فرم زوج‌های قابل تطبیق تولید می‌شوند، که یکی از زوج کلیدها کلید رمزگذاری و دیگری کلید رمزگشایی است. فرض بر این است که حتی با اطلاع از کلید رمزگذاری، یافتن هرگونه اطلاعاتی در رابطه با محتوای متن اصلی ازطریق متن رمز متناظر، از نظر محاسباتی غیرعملی است. فاش نمودن کلید رمزگذاری در اغلب موارد مجاز است، از این رو به کلید رمزگذاری اغلب کلید عمومی اطلاق می‌گردد، درصورتی که کلید رمزگشایی متناظر معمولا فقط یک مالک دارد و محرمانه می‌ماند و از این جهت کلید خصوصی نامیده می‌شود. هر شخصی که کلید عمومی رمزگذاری را در اختیار داشته باشد قادر به رمزگذاری داده‌های مقرر برای دارنده کلید خصوصی متناظر با آن می‌باشد، درحالی‌که صرفا دارنده کلید خصوصی رمزگشایی قادر به رمزگشایی داده‌های رمزشده است.

یادآوری- در اغلب موارد رمز نامتقارن شامل عملیات پیچیده محاسباتی بسیار بیشتری نسبت به یک رمزمتقارن است و معمولا این نوع رمزها برای رمزگذاری حجم وسیعی از داده‌ها استفاده نمی‌شوند بلکه صرفا جهت رمزگذاری کلیدهای نشست

مخفی (جهت استفاده آتی در رمزهای متقارن) به‌کار می‌آیند. البته بعضی از رمزهای نامتقارنی که در استاندارد ISO/IEC 18033-2 تعیین شده، به شکلی طراحی شده‌اند، که برای رمزگذاری حجم وسیعی از داده‌ها مناسب باشند.

استاندارد ISO/IEC 18033-2 و استاندارد ISO/IEC 18033-5 به دو طبقه از رمزهای نامتقارن متفاوت اختصاص دارند که به رمزهای نامتقارن مرسوم (یا صرفا رمزهای نامتقارن) و رمزهای شناسه‌مبنا معروفند. استاندارد ISO/IEC 18033-3 و استاندارد ISO/IEC 18033-4 به دو گروه از رمزهای متقارن متفاوت اختصاص دارند که به رمزهای قالبی و رمزهای جریانی معروفند.

۴-۳ مدیریت کلید

استفاده از انواع رمزنگاری، متکی به مدیریت کلیدهای رمزنگاشتی است. برای کلیه رمزها اعم از متقارن و نامتقارن ضروری است که طرف‌های استفاده کننده از رمز به کلیدهای ضروری دسترسی داشته باشند. چنین امری منجر به ضرورت مدیریت کلید می‌شود که شامل، تولید، توزیع و مدیریت مداوم کلیدها می‌شود. در استاندارد ISO/IEC 11770-1 چارچوبی جامع برای مدیریت کلید ارائه می‌شود.

مسئله مدیریت کلید بسته به این‌که کلیدها مربوط به رمز متقارن یا نامتقارن هستند، متفاوت است. در رمزهای متقارن مراتب تولید و به اشتراک‌گذاری کلیدها باید توسط جفت (یا چندین گروه از) هستارها انجام شود. در رمزهای نامتقارن تولید زوج کلیدها و انتشار کلیدهای عمومی باید به شکلی باشد که اعتبار آن‌ها تضمین شود. در رمز شناسه‌مبنا، کلید عمومی رشته داده‌ای دلخواه است که معمولا از بخشی از اطلاعات عمومی مربوط به رمزگشا انتخاب می‌شود.

در استاندارد ISO/IEC 11770-2 روش‌هایی برای برقرارکردن کلیدهای مخفی مشترک با استفاده از فنون رمزنگاشتی متقارن شرح داده شده است. در استاندارد ISO/IEC 11770-3، روش‌هایی برای برقرارکردن کلیدهای مخفی مشترک با استفاده از فنون رمزنگاشتی نامتقارن تعیین شده است. هم‌چنین فنونی جهت توزیع مطمئن کلیدهای عمومی برای فنون رمزنگاشتی نامتقارن توصیف شده است.

۵ استفاده و خصوصیات رمزگذاری

۵-۱ رمزهای نامتقارن

الگوریتم رمزگذاری برای رمز نامتقارن، نگاشتی از مجموعه مجاز پیام‌های متن اصلی (معمولا مجموعه رشته‌های بیتی) به مجموعه‌ای از پیام‌های متن رمز (معمولا مجموعه رشته‌های بیتی) مشخص می‌کند. مجموعه مجاز پیام‌های متن اصلی و متن رمز وابسته به انتخاب رمز و زوج کلید است.

در رمز نامتقارن الگوریتم رمزگذاری به یک کلید عمومی وابسته است، در حالی که رمزگشایی به کلید خصوصی وابسته است. بنابراین، ضمن این‌که ممکن است محاسبه قالب متن رمز متناظر با یک قالب متن اصلی منتخب به سادگی انجام شود، استنتاج یک قطعه متن خام متناظر با یک قطعه متن رمز منتخب، نباید

برای شخصی غیر از دارنده کلید خصوصی عملی باشد. البته اگر یک نفوذگر به متن رمز، از کلید عمومی مورد استفاده برای تولید آن آگاه باشد و هم‌چنین مطلع باشد که متن خام از میان مجموعه حالاتی اندک تشکیل شده است آن‌گاه ممکن است استنتاج متن خام برای نفوذگر از طریق جستجوی فراگیر کلیه متون ساده احتمالی امکان‌پذیر باشد.

به این دلیل و به منظور دست‌یابی به سطح امنیتی رضایت‌بخش، در فرایند رمزگذاری باید داده‌های تصادفی آمیخته شود تا پیش بینی قطعه رمز متناظر با یک قطعه متن خام امکان‌پذیر نباشد. در استاندارد ISO/IEC 18033-2 فنونی جهت آمیختن داده‌های تصادفی به تفصیل شرح داده می‌شود.

۵-۲ رمزهای قالبی

۵-۲-۱ کلیات

رمز قالبی، رمزی متقارن است با این خصوصیت که به منظور تولید قالب‌های متن رمز، الگوریتم رمزگذاری بر روی قالب‌های متن اصلی، یعنی رشته بیت‌هایی با طول معین، عمل می‌کند. هرکلید در رمز قالبی، نگاشتی معکوس‌پذیر و منحصربه فرد، از قالب‌های متن اصلی به قالب‌های متن رمز مشخص می‌کند (و نگاشت معکوس متناظر مورد استفاده برای رمزگشایی). اگر طبق معمول همه قالب‌های متن رمز و متن خام قالب‌هایی متشکل از n رقم دودویی باشند، آن‌گاه در واقع هر کلید، جایگشتی برروی مجموعه تمامی قالب‌های n بیتی تعیین می‌کند.

استفاده از رمزهای قالبی به شیوه‌هایی متعدد امکان‌پذیر است. دو کاربرد از مهم‌ترین کاربردها در زیربند ۵-۲-۲ و زیربند ۵-۲-۳ توصیف شده‌اند، اما کارکردهایی دیگر نظیر توابع درهم‌ساز (به استاندارد ISO/IEC 10118-2 رجوع شود) و مولدهای اعداد تصادفی (به استاندارد ISO/IEC 18031 رجوع شود) وجود دارد.

۵-۲-۲ مودهای کارکرد

استفاده از یک رمز قالبی n بیتی برای رمزگذاری متن اصلی به روش‌هایی متعدد امکان‌پذیر است. این قبیل روش‌ها مودهای عملیات رمزهای قالبی نامیده می‌شوند. مودهای عملیات در استاندارد ISO/IEC 10116 تعیین می‌شوند. اگر تعداد بیت‌ها در متن اصلی تصادفا n بیت باشد، آن‌گاه رمزگذاری به‌سادگی با اعمال فرایند رمزگذاری به این قالب امکان‌پذیر است. این مود رمزگذاری کتاب‌کد الکترونیکی (ECB) نامیده می‌شود. اما برای متن اصلی با طول دلخواه، باید راهکاری پیچیده‌تر به کار رود. از این رو و با توجه به دلایل دیگر اغلب باید یکی دیگر از مودهای عملیاتی تعیین‌شده در استاندارد ISO/IEC 10116 استفاده شود.

۵-۲-۳ کدهای احراز اصالت پیام (MACs)

اگرچه رمزگذاری، منجر به یکپارچگی داده‌ها نمی‌شود، استفاده از یک رمز قالبی که با شیوه‌ای خاص تعریف شده است، جهت ایفای نقش حفاظت از یکپارچگی داده‌ها امکان‌پذیر است. به ویژه استفاده از یک رمز قالبی جهت محاسبه یک کد احراز اصالت پیام (MAC) برای یک جریان بیتی امکان‌پذیر است. استفاده از این MAC جهت تامین یکپارچگی و حفاظت از رشته بیتی امکان‌پذیر است.

در استاندارد ISO/IEC 9797-1 شیوه‌هایی برای دست‌یابی به این امرتعیین می‌شود. لازم به یادآوری است که گاهی مطلوبست از یک رمز قالبی به شکلی هم‌زمان جهت رمزگذاری و محاسبه یک MAC برای متن اصلی استفاده کرد. عموما در چنین حالتی باید از دو کلید مخفی، یک کلید برای رمزگذاری و یک کلید برای محاسبه MAC، استفاده کرد. به عنوان جایگزین، در استاندارد ISO/IEC 19772 فنونی برای رمزگذاری همراه با احراز اصالت پیام مشخص می‌شوند که هم‌زمان محرمانگی و حفاظت از یکپارچگی داده‌ها را صرفا با یک کلید مخفی تامین می‌کنند.

۵-۳ رمزهای جریانی

یک رمز جریانی بنا به تعریف مبتنی بر یک مولد کلید جریانی است یعنی تابعی که با دریافت یک کلید مخفی (و احتمالا متن رمز قبلی) به عنوان ورودی، دنباله‌ای از نمادها که کلید جریانی نامیده می‌شوند را خروجی می‌دهد. این دنباله برای رمزگذاری متن اصلی با استفاده از ترکیب آن با دنباله‌ای از نمادهای متن اصلی به شکل نماد به نماد توسط یک تابع معکوس‌پذیر استفاده می‌شود (مثلا عملیات بیتی یای انحصاری[1])

معمولا اگر بیش از یک بار از یک بردار مقداردهی اولیه و کلیدی یکسان برای مقداردهی اولیه مولد کلید جریانی استفاده شود، آنگاه کلید جریانی یکسان حاصل می‌شود. اگر کلید جریانی یکسانی برای رمزگذاری بیش از یک متن اصلی استفاده شود، آن گاه خطر استنباط اطلاعاتی در رابطه با هر دو متن اصلی، توسط نفوذگری به متون رمز حاصل‌شده، امکان‌پذیر است. در نتیجه باید شیوه‌هایی تدارک دیده شود که جهت رمزگذاری هر متن اصلی از کلیدهای جریانی متفاوت استفاده شود. این قبیل مسائل مرتبط با کلیدسازی در استاندارد ISO/IEC 18033-4 با جزییاتی بیشتر مطرح می‌شوند.

رمزهای جریانی فقط در صورتی از یکپارچگی متن اصلی حفاظت می‌کنند که از فنون خاص قالب‌بندی متن اصلی استفاده شود. در حالتی که عملیات رمزگذاری رمز جریانی شامل عملیات بیتی یای انحصاری باشد، تغییر یک بیت از متن رمز منجر به تغییر یک بیت در متن اصلی بازیابی‌شده می‌شود. هم‌چنین، این قبیل رمزهای جریانی همیشه طول دقیق متن اصلی را فاش می‌کنند.

1- Exclusive-or

۵-۴ سازوکارهای شناسه‌مبنا

فن رمزگذاری شناسه‌مبنا، یک سازوکار رمزگذاری نامتقارن است که در آن استفاده از یک رشته دلخواه به عنوان کلید عمومی‌مجاز است. رمزگذار با استفاده از رشته‌ای به عنوان کلید عمومی که به سادگی قابل شناسایی است (مثلا یک رایانامه)، بدون نیاز به دسترسی به یک گواهی کلید عمومی، به شکلی مطمئن آن را احراز و تصدیق کند. در بعضی مواقع مثلا با افزودن تاریخ یا مهر زمانی[1] در کلید عمومی همراه با شناساگری برای دارنده آن ممکن است بتوان ترتیبی داد تا کلید عمومی عمر کوتاهی داشته باشد. در چنین حالتی، برخلاف حالتی که از گواهی‌نامه کلید عمومی استفاده می‌شود، ضرورتی به وجود سازوکاری مجزا برای ابطال کلیدهای عمومی نیست. (به استاندارد ISO/IEC 11770-3 رجوع شود). نظر به این‌که در رمزگذاری شناسه‌مبنا گواهی‌نامه های کلید عمومی ضروری نبوده و هم‌چنین نیازی به سازوکار ابطال نیز نمی‌باشد، نسبت به فنون رمزگذاری نامتقارن مبتنی بر گواهی‌نامه مزیت‌های قابل‌توجه عملی دارد.

استفاده از رمزگذاری شناسه‌مبنا، شامل شخص ثالث معتمد خاص، به عنوان مولد کلید خصوصی است. این هستار، مسئول تولید کلید خصوصی کاربران منحصر به فرد است. درنتیجه این شخص ثالث ابزار رمزگشایی کلیه پیام‌های مقرر برای موکلین خود را در اختیار دارد. ممکن است این خصوصیت همیشه مطلوب نباشد، در چنین حالتی توصیه می‌شود فن رمزگذاری نامتقارن مبتنی بر گواهی‌نامه طبق استاندارد ISO/IEC 18033-2 استفاده شود.

۶ شناسه‌های شیء[2]

این استاندارد ملی نامی منحصر به فرد (یک شناسه شی OSI) برای هر الگوریتم مشخص تعیین می‌کند. در کاربردهایی که در آن‌ها از شناسه‌های شی استفاده می‌شود، استفاده از شناسه‌های شی‌ای که در این استاندارد مشخص شده است برای الگوریتم‌های مرتبط باید بر دیگر شناسه‌های شیء، در صورت وجود، اولویت داشته باشند.

1- Timestamp

2- Object identifiers

پیوست الف

(الزامی)

معیارهای ارائه [1]رمزها برای قرارگیری احتمالی در این استاندارد

الف-۱ راهنمایی‌های مورد استفاده برای ارزیابی الگوریتم‌های رمزگذاری

رمزهای قرارگرفته در قسمت‌های بعدی این استاندارد، از میان تعداد زیادی از فنون منتشرشده و در حال استفاده انتخاب شده‌اند. عدم پذیرش رمزهایی خاص به معنی ناامن بودن این فنون نیست. رمزهای مشخص‌شده بیان‌گر مجموعه‌ای کوچک از فنونی هستند که طبق معیارهای زیر انتخاب شده‌اند (که ترتیب نمایش معیارها فاقد اهمیت می‌باشد).

ارزیابی‌ها نسبت به جنبه‌هایی از رمز صورت می‌گیرد که در زیر ارائه شده‌اند.

الف- *امنیت* رمز، یعنی الگوریتم‌های منتخب باید نسبت به حملات تحلیل رمز مقاوم باشند. وجود سندی برای امنیت، بسته به مدل امنیتی و فرضیات سند، به عنوان دلیلی قابل‌توجه به نفع رمز در نظر گرفته می‌شود. ماهیت هرگونه ارزیابی نیز از اهمیت زیادی برخوردار است، به ویژه ارزیابی‌هایی که توسط سازمان‌های ارزیابی مشهور انجام می‌شوند.

ب- *عملکرد* رمز بر طیفی از پلتفرم‌های معمول. چنین موردی نه تنها شامل مسائلی هم‌چون بازدهی زمانی و فضا است، بلکه شامل این مورد نیز می‌باشد که آیا رمز دارای مشخصاتی است که نسبت به سایر فنون برتری دارد یا خیر.

پ – ماهیت هرنوع *صادرکننده گواهی‌نامه* که رمز را تحت تاثیر قرار می‌دهد.

ت- *بلوغ* رمز. ارزیابی *بلوغ* رمز بر حسب میزان وسعت استفاده، انتشار هرگونه تجزیه و تحلیل آن و میزان بررسی هر رمز صورت می‌گیرد.

ث- درجه‌ای که رمز توسط یک سازمان معتبر (مثلا یک نهاد استاندارد، یک آژانس امنیتی دولتی و غیره) *تایید می‌شود*، یا درجه‌ای که یک رمز جهت تایید توسط این قبیل نهادها تحت بازرسی و/یا تجزیه و تحلیل می‌باشد.

ج- *سطح پذیرش رمز در بازار*. رمزهایی که به وسعت مورد پذیرش بازار هستند باید بر فنون کمتر استفاده شده مقدم باشند مگر این‌که ملاحظاتی دیگر سبب لغو این چنین مصوبه‌ای شوند.

1- Inclusion

چ – در حالت کلی توصیه می‌شود، *تعداد* رمزهای مورد استانداردسازی در هر قسمت از این مجموعه استاندارد تا حد امکان کم باشد. سه استثنا برای این اصل وجود دارد.

- در حالتی که دو رمز دارای مشخصاتی متفاوت باشند، مثلا رمزهای قالبی n بیتی با مقادیر متفاوت n یا رمزهایی که الزامات پیاده‌سازی محاسباتی و فضای بسیار متفاوتی دارند و در عین حال هردو مجموعه مشخصات از نظر عملی دارای اهمیت باشند، استانداردسازی هر دو نوع رمز قابل‌قبول است.
- عموما مطلوب است رمزهایی استاندارد مبتنی بر اصول اساسی متفاوت موجود باشد که اگر یک رمز در برابر حملات تحلیل رمز آسیب‌پذیر باشد، رمز دیگر شانس بالایی برای امن ماندن داشته باشد.
- عموما مطلوب است رمزهای استاندارد مبتنی بر بیش از یک مسئله محاسباتی دشوار موجود باشد. مثلا مسئله تجزیه به عوامل صحیح، یا مسئله لگاریتم گسسته با مجموعه‌های متنوع، شامل گروه‌های ضربی میدان متناهی و مجموعه نقاط روی خم بیضوی در یک میدان متناهی.

ح- فرایندی را که SC 27 هنگام تصمیم‌گیری در رابطه با قرارگیری یک رمز جدید در این مجموعه استاندارد مورد پیروی قرار می‌دهد در WG 2 SD 5 قابل دسترسی است.

الف-۲ توانایی حملات وارد بر الگوریتم‌های رمزگذاری

هنگام تصمیم‌گیری در رابطه با امکان لحاظ نمودن یک الگوریتم رمزگذاری برای قرارگیری در سایر قسمت‌های این استاندارد، میزان اثربخشی حملات معلوم تحلیل رمز بر الگوریتم‌های رمزگذاری، دارای اهمیت اساسی است.

در این پیوست مقایسه ارزش یک حمله تحلیل رمز خاص با مدل و هدف معین نسبت به بهترین حمله عام باید تعیین کند که آیا حمله به عنوان شکست الگوریتم رمزگذاری طبقه‌بندی می‌شود یا خیر. اگر ارزش حمله بیشتر یا معادل با ارزش بهترین حمله متناظر عام باشد، حمله تحلیل رمز نباید شکست الگوریتم رمزگذاری به حساب آید. اگر ارزش حمله برای مدل و هدف مقرر کمتر از ارزش بهترین حمله متناظر عام باشد، آن‌گاه حمله تحلیل رمز باید شکست الگوریتم رمزگذاری به حساب آید. برای آشنایی با تعریف اصطلاح حمله به زیربند ۲-۶ این استاندارد ملی رجوع شود.

در این پیوست، پیاده‌سازی حملات خاص نباید لحاظ شود.

یادآوری- برای پیشینه اطلاعاتی حملات به پیوست پ رجوع شود.

الف-۳ حداقل معیارهای شایستگی برای ارائه رمزهای جدید

معیارهای مقرر در این بند برای ارائه رمزهایی درنظر گرفته‌شده که هنوز در قسمت‌های بعدی این استاندارد قرارنگرفته‌اند. برای ملاحظه یک رمز جهت قرارگیری در قسمت‌های بعدی این استاندارد، رمز باید با الزامات زیر مطابقت داشته باشد:

الف- حداقل طول کلید: برای الگوریتم‌های رمزگذاری متقارن، الگوریتم رمزگذاری باید کلیدی با حداقل طول ۱۲۸ بیت را تدارک ببیند. برای الگوریتم‌های نامتقارن، غالبا طول کلید از نظر بیتی طولانی‌تر است، اما نگاشت آن به طول کلید متقارن معادل، امکان‌پذیر است. در این حالت، الگوریتم نامتقارن باید طول کلید معادلی با حداقل طول ۱۲۸ بیت تدارک ببیند.

یادآوری- جهت اطلاعات بیشتر در رابطه با طول کلید معادل رمزهای متقارن و نامتقارن، به سند معتبر ۱۲ از کمیته JTC 1/SC 27 (SC 27 SD 12) با آدرس اینترنتی http://www.jtc1sc27.din.de/sbe/SD12 رجوع شود.

ب- نتایج تحلیل رمزهای شناخته‌شده: هیچ حمله شناخته‌شده تحلیل رمز نباید قادر به شکستن الگوریتم رمزگذاری طبق زیربند ۱-۴ پیوست پ باشد.

مثال: رمزی با کلیدی به طول ۲۵۶ بیت ارائه می‌شود. حمله‌ی تحلیل رمزی برای رمز موجود است. پیچیدگی کلید برای این حمله تحلیل رمز $۲^{۲۵۰}$ و احتمال موفقیت یک می‌باشد. هم‌چنین این حمله از بهترین حمله عام با مدل و هدف یکسان سریع‌تر است. در این حالت رمز از نظر معیارهای بند الف این پیوست قبول می‌شود اما از نظر معیارهای بند ب این پیوست مردود است و بنابراین جهت قرارگیری احتمالی مورد ملاحظه قرار نمی‌گیرد.

پ- حوزه عمومی: توصیف رمز باید حداقل برای یک دوره سه ساله در حوزه عموم منتشر شده باشد. انتشارات قابل قبول شامل موارد زیر بوده ولی صرفا محدود به موارد زیر نیست:

۱- کنفرانس‌ها و سمینارهای IACR:

- Asiacrypt, Crypto, Eurocrypt
- International workshop on Fast Software Encryption (FSE)
- International workshop on Cryptographic Hardware and Embedded Systems (CHES)
- Conference on Practice and Theory in Public Key Cryptography (PKC)

۲- کنفرانس‌های سالیانه IEEE:

- Symposium on Security and Privacy
- Symposium on the Foundations of Computer Science (FOCS)

۳- کنفرانس‌های سالیانه ACM:

- Symposium on Theory of Computing (ACM-STOC)
- Computer and Communication Security (ACM-CCS)

۴- کنفرانس‌های بین‌المللی مشهور با پیشینه‌ای بیش از ۱۵ سال با شرح اقدامات موجود

- USENIX Security
- European Symposium on Research in Computer Security (ESORICS)
- Australasian Conference on Information Security and Privacy (ACISP)
- Financial Cryptography and Data Security (FC)
- International Conference on Information Security and Cryptography (ICISC)
- Selected Areas in Cryptography (SAC)

۵- انتشارات مشهورکه حداقل سامانه‌های دادگان و برنامه نویسی منطقی (DBLP)[1] به آن‌ها ارجاع داده):

الف – ACM

- Journal of the ACM
- Communications of the ACM

ب – Elsevier

- Computer Communications
- Information and Computation
- Journal of Computer and System Sciences (JCSS)
- Journal of Discrete Algorithms

پ – IEEE

- IEEE Transactions on Information Theory
- IEEE Transactions on Computers
- IEEE Security and Privacy

ت- IEICE

- IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences
- IEICE Transactions on Information and Systems

ث-SIAM

- SIAM Journal on Computing

1- DataBase Systems and Logic Programming

ج- Springer

- Combinatorica
- Cryptography and Communications
- Designs, Codes and Cryptography
- Journal of Cryptology
- International Journal of Information Security,

۶- استانداردهای دیگر

الف- انتشارات رسمی به عنوان استاندارد به زبان انگلیسی توسط یک سازمان استانداردسازی رسمی که توسط عموم قابل دسترسی است.

۷- یک مسابقه بین‌المللی که صرفا دارای هدفی جهت انتخاب یک الگوریتم رمزگذاری جدید از نوعی خاص (هم‌چون رمز قالبی، رمز جریانی، رمز نامتقارن) است، که حداقل به مدت دو سال در حال اجرا باشد و تحلیل‌ها و وقایع آن در دسترس عموم باشد. بهتر است نسخه دستکاری نشده الگوریتم حداقل به مدت سه سال قبل از ارائه به این مجموعه استاندارد، در دسترس عموم باشد.

ت- تحلیل رمز: یک سامانه رمز قبل از قرارگیری در این مجموعه استاندارد، باید دارای مقاله‌های تحلیل رمز منتشرشده در مجله‌های بررسی دقیق یا کنفرانس‌هایی هم‌چون موارد ارائه‌شده در زیربند پ بند الف- ۳ پیوست الف این استاندارد ملی باشد.

ث- پذیرش صنعت: برای کاربردهای تجاری که از سامانه رمز استفاده می‌کنند و گسترش احتمالی استفاده کاربردها به شکل بین‌المللی باید مدرکی قوی ارائه شود.

ج- عملکرد: برای سطوح امنیتی پیش تعیین‌شده (هم‌چون طول کلید)، اندازه‌گیری عملکرد با استفاده از معیارهای‌متری[1] متنوع، هم‌چون bits/cycle یا bits/watt عملی می‌شود. برای ادعای این‌که سامانه رمز عملکردی بهتر نسبت به سامانه‌های رمز موجود از نظر معیارهای‌متری مرتبط با کاربردهای در نظر گرفته‌شده ارائه می‌کند باید مدارکی مستدل فراهم شود، ضمنا سامانه رمز باید حداقل سطح امنیتی مشابه با سامانه‌های رمز استانداردشده موجود داشته باشد.

1- Metrics

پیوست ب

(الزامی)

معیارهایی برای حذف رمزهای موجود در این استاندارد

اگر امنیت یک رمز در برابر روش‌های ابداعی نوین حملات تحلیل رمز قابل تضمین نباشد آن‌گاه الگوریتم‌های رمزگذاری استانداردشده موجود در قسمت‌های بعدی مجموعه استاندارد ملی ایران شمارهٔ ۱۸۰۳۳ مشمول حذف از این مجموعه استاندارد می‌شوند در نتیجه امنیت الگوریتم‌های رمزگذاری در عمل پس از آن قابل تضمین نیست. استانداردهای موجود به منظور تضمین صحت و کارایی به طور مرتب بازنگری می‌شوند. در بازنگری، آخرین تحلیل‌های رمز منتشرشده برای الگوریتم‌های رمزگذاری معرفی‌شده در این استاندارد ملی لحاظ می‌شوند. جهت ارزیابی آخرین فنون تحلیل رمز، از مراحل اجرایی مورد توصیف در SC ۲۷ پیروی می‌شود.

فاکتورهایی که در طی ارزیابی چگونگی تحت تاثیر قرار گرفتن الگوریتم‌های رمزگذاری معرفی‌شده در این مجموعه استاندارد ملی توسط فنون جدید تحلیل رمزلحاظ می‌شوند به شرح زیر می‌باشد:

الف- صحت تحلیل رمزها. فنون‌نوین تحلیل رمز در انجمن‌هایی بسیار متنوع اعلام می‌شوند. گاهی تحلیل رمزهای انتشار یافته در رابطه با توان امنیتی یا پیچیدگی حمله رمزنگاشتی مبالغه‌آمیز است. علاوه بر این الگویی که حمله رمزنگاشتی مبنی بر آن پیشنهاد می‌شود عاملی مهم در تعیین اعتبار حمله است. قبل از ارزیابی اثر یک فن جدید بر الگوریتم‌های منتشرشده، باید در رابطه با معتبر بودن تحلیل رمز اجماع نظر صورت گیرد.

ب- قابلیت اجرای تحلیل‌های رمز در عمل. اهمیت برخی نتایج تحلیل‌های رمز از جنبه نظری بوده و لزوما قابل اعمال به تمامی الگوریتم رمزگذاری نیست. هم‌چنین ممکن است که تحلیل رمزهای یک رمز منجر به حمله نظری بر یک الگوریتم رمزگذاری شود اما به دلیل الگوی حمله یا به دلیل پیچیدگی حمله عملی نباشد. اگر حمله‌ای عملی باشد، ممکن است برای کاربران الگوریتم رمزگذاری خطراتی تلویحی داشته باشد و حذف الگوریتم رمزگذاری از این مجموعه استاندارد ملی لحاظ می‌شود.

پ- تاثیر بر فراورده‌های الگوریتم رمزگذاری در صنعت. هنگامی که حذف یک الگوریتم مورد ملاحظه قرار می‌گیرد، توصیه می‌شود همراه با گزارش ضعف الگوریتم رمزگذاری تاثیر آن بر صنعت نیز کاملا به حساب آورده شود به ویژه اگر از نظر عملی ضعف الگوریتم جدی نباشد.

بسته به پیامد بازنگری، اگر یک الگوریتم خطرات عملی برای کاربران نشان دهد، ممکن است از این مجموعه استاندارد ملی حذف شود. اگر الگوریتمی حذف نشود و امنیت آن تحت تاثیر آخرین فنون علنی‌شده تحلیل رمز نباشد، آنگاه اطلاعات بیشتر در رابطه با تاثیر این فنون بر سطح امنیت الگوریتم در سند شمارهٔ ۱۲ SC ۲۷ (SC 27 SD 12) قابل دسترسی بوده که به شکل رایگان در http://www.jtc1sc27.din.de/sbe/SD12 قابل دست‌یابی است.

پیوست پ

(الزامی)

حملات برعلیه الگوریتم‌های رمزگذاری

پ-۱ تحلیل رمز الگوریتم‌های رمزگذاری

پ-۱-۱ مدل‌ها و اهداف حمله

تحلیل رمز فرایندی است که بوسیله آن یک الگوریتم رمزگذاری جهت تعیین میزان قدرت آن نسبت به فاش شدن اطلاعات درمورد متن اصلی نامعلوم و/یا کلید نامعلوم تحلیل می‌شود. تحلیل رمز شامل مدلی برای تعیین میزان دسترسی مهاجم به منظور پرسمان الگوریتم رمزگذاری، یک الگوریتم حمله که متن اصلی/ متن رمز را به عنوان ورودی دریافت و متن اصلی نامعلوم و یا کلید نامعلوم را خروجی می‌دهد و دارای هدفی جهت بازیابی متن اصلی نامعلوم یا کلید نامعلوم است.

مدل‌های معمول شامل موارد زیر است:

- مهاجم صرفا به متن رمز دسترسی دارد.
- مهاجم به بخش‌هایی از متون اصلی معلوم و متون رمز متناظر دسترسی دارد.
- مهاجم قادر به پرسمان الگوریتم رمزگذاری با متون اصلی منتخب جهت دست‌یابی به متون رمز با کلیدی نامعلوم می‌باشد.
- مهاجم قادر به پرسمان الگوریتم رمزگذاری با متون اصلی منتخب و پرسمان الگوریتم رمزگشایی با متون رمز منتخب جهت دست‌یابی به متون رمز متناظر (متون اصلی به ترتیب) با یک کلید نامعلوم است.
- - مهاجم قادر به پرسمان الگوریتم رمزگذاری و/ یا الگوریتم رمزگشایی با متون منتخب به‌واسطه کلیدهایی متفاوت می‌باشد که این کلیدها رابطه‌ای معلوم یا منتخب با کلید نامعلوم دارند.

مدل‌هایی که در آن‌ها صرفا یک کلید استفاده می‌شود مجموعه‌های تک کلیدی نامیده می‌شوند، در حالی که آخرین مدل از موارد فهرست‌شده فوق در مجموعه کلید مرتبط قرار می‌گیرد. در این پیوست، صرفا مدل‌های مجموعه تک کلیدی مورد ملاحظه قرار می‌گیرند، که دارای یکی از دو هدف حمله می‌باشند (بازیابی متن اصلی نامعلوم، یا یک کلید نامعلوم). مهاجم مجاز به پرسمان الگوریتم رمزگذاری یا رمزگشایی با متون منتخب اصلی یا متون رمز با کلید نامعلوم جهت دست‌یابی به متون رمز یا متون اصلی متناظر است. اگر هدف بازیابی کلید رمزگذاری نامعلوم است، هیچ محدودیتی برای پرسمان‌ها وجود ندارد. اگر هدف بازیابی متن اصلی از متن رمز نامعلوم است، محدودیتی در این مدل اعمال می‌شود که به موجب آن، مهاجم مجاز به

پرسمان الگوریتم برای رمزگشایی متن رمزی که در اختیار دارد نیست، اما مجاز به پرسمان الگوریتم رمزگذاری برای رمزگشایی هر متن رمز منتخب دیگر می‌باشد.

یادآوری- دو نوع پرسمان در این مدل‌ها امکان‌پذیر است، نوعی که در آن پرسمان الگوریتم رمزگذاری در مرحله اکتساب داده‌ها انجام شده سپس داده‌ها توسط الگوریتم حمله پردازش می‌شوند و نوع دیگر که، پرسمان‌ها مطابق با خروجی الگوریتم حمله تطبیق داده می‌شوند. نوع دوم حملات متن اصلی یا متن رمز منتخب وفقی[1] نامیده می‌شوند که احتمالا قوی‌ترین مجموعه مدل تک کلیدی است.

پ-۱-۲ حملات عام

حمله عام حمله‌ای قابل‌اعمال به الگوریتم‌های رمزگذاری است که به ساختار الگوریتم‌ها وابسته نیست. یک نمونه حمله عام حمله جستجوی فراگیر کلید است. مهاجم با دراختیار داشتن یک جفت متن اصلی متن رمز، با آزمودن هر کلید محتمل متن اصلی را رمزگذاری می‌کند و متن رمز حاصل‌شده را با متن رمزی که در اختیار دارد مقایسه می‌کند. اگر دو متن رمز مطابقت داشته باشند، کلید استفاده‌شده یک کاندید محتمل است. یک نمونه حمله عام دیگر حمله واژه‌نامه‌ای است. مهاجم برای کلیدی ثابت واژه‌نامه کاملی از جفت‌های متن اصلی/ متن رمز را تخمین اولیه می‌زند. مهاجم با در اختیار داشتن یک متن رمز نامعلوم، واژه نامه را به منظور امکان دربرداشتن متن رمز بررسی می‌کند. در صورت وجود متن رمز، مهاجم متن اصلی متناظر را از واژه نامه استخراج می‌کند.

پ-۱-۳ ارزش حمله

پیچیدگی حملات تحلیل رمز با تعداد دفعات فراخوانی الگوریتم رمزگذاری نسبت به حملات عام به قاعده درمی‌آید[2]. این قاعده در مواردی که مدل نیازمند فراخوانی الگوریتم رمزگذاری است می‌تواند ساده باشد اما ممکن است در مواردی که حمله شامل محاسبات برون‌خطی پیچیده بی نیاز به پرسمان است (مثل حملات جبری) دشوار شود که در این مورد پیچیدگی الگوریتم حمله صرفا قابل تخمین است.

پیچیدگی حمله تحلیل رمز با نماد W نشان داده می‌شود و عددی به شکل ۲^k است که معادل میانگین پیچیدگی حمله بر حسب تعداد دفعات فرخوانی الگوریتم رمزگذاری است.

بعضی از حملات وارد بر الگوریتم‌های رمزگذاری فرضی هستند یعنی در تمامی موارد موفقیت‌آمیز نیستند. احتمال موفقیت یک حمله با P نشان داده می‌شود که P مقداری مثبت بین صفر و یک است.

ارزش حمله با نسبت W/P تعریف می‌شود. مثلا برای حمله جستجوی فراگیر، اگر P=۱ و $W = ۲^{n-1}$ باشند که در آن n طول کلید بر حسب بیت است آن‌گاه $W/P = ۲^{n-1}$. اگر نسبت W/P برای یک حمله تحلیل رمز

1- Adaptively
2- Normalized

خاص بزرگتر از 2^{n-1}باشد آنگاه بر اساس این پیوست حمله رمزنگاشتی کندتر از حمله جستجوی فراگیر پنداشته می‌شود.

پ-۱-۴ اثر حملات تحلیل رمز

بررسی قدرت امنیتی الگوریتم رمزگذاری، رویکرد سنتی جهت تعیین این‌که آیا یک حمله تحلیل رمز منجربه شکست یک الگوریتم می‌شود می‌باشد. رویکرد سنتی کلیه مدل‌های محتمل حمله قابل مقایسه با حملات عام را مورد ملاحظه قرار نمی‌دهد، هم‌چنین احتمال موفقیت حمله را نیز درنظر نمی‌گیرد. در این پیوست هنگام ملاحظه الگوریتم‌های رمزگذاری برای امکان گنجایش در سایر قسمت‌های این مجموعه استاندارد، راهکار زیر استفاده می‌شود.

برای یک مدل و هدف حمله خاص، یک حمله عام علیه الگوریتم رمزگذاری وجود دارد. برای یک حمله تحلیل رمز معین علیه یک الگوریتم رمزگذاری خاص، احتمالی برای موفقیت حمله وجود دارد. ارزش حمله، با استفاده از پیچیدگی حمله قابل محاسبه است.

پ-۲ حملات کانال جانبی بر الگوریتم‌های رمزگذاری

حملاتی دیگر بر الگوریتم‌های رمزگذاری وجود دارد که مستقیما به جنبه‌های نظری الگوریتم رمزگذاری وابسته نیست، بلکه بیشتر به جنبه‌های پیاده‌سازی وابسته است. عموما این حملات، حملات کانال جانبی نامیده می‌شوند.

حملات کانال جانبی شامل موارد زیر است:

- تجزیه و تحلیل توان
- تجزیه و تحلیل زمانی
- تجزیه و تحلیل عیب

تجزیه و تحلیل توان به منظور استخراج اطلاعاتی در مورد محاسبات در حال انجام درون الگوریتم رمزگذاری، به محاسبه توان مصرفی می‌پردازد. تجزیه و تحلیل زمانی، جهت تعیین اطلاعاتی در مورد محاسبات در حال انجام درون الگوریتم رمزگذاری، تفاوت‌های زمانی حین اجرای الگوریتم رمزگذاری را اندازه می‌گیرد. تجزیه و تحلیل عیب، عیب‌هایی به الگوریتم رمزگذاری حین اجرا تحمیل می‌کند و سپس خصوصیات گسترش عیب، جهت سنجش و تعیین یک حالت نامعلوم درونی الگوریتم رمزگذاری، یا اطلاعاتی در مورد کلید نامعلوم استفاده می‌شود.

کلیه این حملات به شکلی یکسان برای رمزگشایی به‌کار رفته و خاص پیاده‌سازی هستند. اقدامات متقابل معمولا قابل پیاده‌سازی هستند.

کتاب‌نامه

[۱] استاندارد ملی ایران شمارهٔ ۹۶۰۰: سال ۱۳۸۶، فناوری اطلاعات- روش‌های امنیتی- حالت‌های عملیاتی یک الگوریتم رمزنگاری قطعه‌ای N بیتی

[۲] استاندارد ملی ایران شمارهٔ ۱-۱۰۸۲۵: سال ۱۳۹۲، فناوری اطلاعات- فنون امنیتی- احراز هویت هستار- قسمت ۱: کلیات

[۳] استاندارد ملی ایران شمارهٔ ۱۱۴۹۴ (تمام قسمت‌ها)، فناوری اطلاعات- فنون امنیت امضاهای دیجیتال با پیوست

[۴] استاندارد ملی ایرن شمارهٔ ۱۸۹۱۵، فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها- فرمان پیکربندی جلویی- انتهایی برای NFC-WI(NFC-FEC)

[5] ISO/IEC 9796 (all parts), Information technolog-Security techniques- Digital signature schemes giving message recovery

یادآوری- مجموعه استانداردهای ملی ایران شمارهٔ ۹۷۹۶، فناوری اطلاعات- فنون امنیتی – طرح‌های امضای دیجیتال با قابلیت بازیابی پیام، با استفاده از برخی قسمت‌های استاندارد ISO/IEC 9796 تدوین شده است.

[6] ISO/IEC 9797 (all parts), Information technology–Security techniques–Message Authentication Codes (MACs)

یادآوری- مجموعه استانداردهای ملی ایران شمارهٔ ۱۷۹۱۴، فناوری اطلاعات- فنون امنیتی- کدهای اصالت‌سنجی پیام (MACs)، با استفاده از برخی قسمت‌های استاندارد ISO/IEC 9797 تدوین شده است.

[7] ISO/IEC 10118-2:2000, Information technology- Security techniques- Hash-functions- Part 2: hash-functions using an n-bit block cipher algorithm

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

یادآوری- مجموعه استانداردهای ملی ایران شمارهٔ ۱۰۸۲۲، فناوری اطلاعات- فنون امنیتی- مدیریت کلید، با استفاده از برخی قسمت‌های استاندارد ISO/IEC 11770 تدوین شده است.

[9] ISO/IEC 29192 (all parts), Information technology- Security techniques- Lightweight

یادآوری- مجموعه استانداردهای ملی ایران شمارهٔ ۱۹۲۶۷، فناوری اطلاعات- فنون امنیتی- رمزنگاری سبک، با استفاده از برخی قسمت‌های استاندارد ISO/IEC 29192 تدوین شده است.

[10] Cryptographic algorithms and key lengths (SC 27 SD 12), http://www.jtc1sc27.din.de/sbe/SD12

[11] Introduction and Removal of Cryptographic Techniques (SC 27/WG 2 SD 5), http://www.jtc1sc27.din.de/sbe/wg2sd5