ISIRI
10824-1
1st. edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۰۸۲۴-۱
چاپ اول

فن‌آوری اطلاعات –
فنون امنیتی الگوریتم‌های رمزنگاری –
قسمت اول : کلیات

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

ICS:35.040

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

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

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

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سا زمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، مؤسسهٔ استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می کند .ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1 - International organization for Standardization
2 - International Electro technical Commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات - فنون امنیتی - الگوریتم‌های رمزنگاری -- قسمت اول : کلیات »

رئیس:	**سمت و/ یا نمایندگی**
حسینی خیاط ، سعید	عضو هیات علمی دانشکده مهندسی
(دکترای مهندسی برق)	دانشگاه فردوسی مشهد
دبیر:	
خانیکی ، رضا	اداره کل استاندارد و تحقیقات صنعتی
(لیسانس مهندسی برق - مخابرات)	خراسان رضوی
اعضاء: (اسامی به ترتیب حروف الفبا)	
اثنی عشری ، امیر مهدی	موسسه تحقیقات و فن آوری پارس
(لیسانس مهندسی برق - کنترل)	
ارومیه‌چی‌ها ، محمدعلی	شرکت صنایع الکترونیک زعیم
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
رضایی ، امید	شرکت مهندسی ایمن رایانه شرق
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
سهی زاده ابیانه ، محمد رضا	شرکت صنایع الکترونیک زعیم
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
صادق اقبالی ، سامان	گروه مهندسین فن‌آوری نوین ۵۲
(لیسانس مهندسی برق - مخابرات)	
طوماریان ، سهیلا	مؤسسهٔ استاندارد و تحقیقات صنعتی
(لیسانس مهندسی برق- الکترونیک)	ایران

فرزاد ، پویان
(فوق لیسانس ریاضی‌کاربردی)
گروه مهندسین فن‌آوری نوین ۵۲

میرمطهری ، نوید
(فوق لیسانس مهندسی برق- مخابرات)
اداره مخابرات و ارتباطات رادیویی
آستان قدس رضوی

فهرست مندرجات

پیش گفتار

استاندارد " فن‌آوری اطلاعات - فنون امنیتی - الگوریتم‌های رمزنگاری -- قسمت اول : کلیات " که پیش نویس آن درکمیسیون های مربوط توسط (مؤسسهٔ استاندارد و تحقیقات صنعتی ایران) تهیه و تدوین شده و در پنجاه و چهارمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۸/۱۲ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

منابع و مآخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

1- ISO/IEC 18033-1:2005, 1st Ed.: Information technology - Security techniques - Encryption algorithms - Part 1: General

۲ - کلیه واژگان مصوب فرهنگستان علوم, سایت اینترنتی فرهنگستان زبان و ادبیات پارسی

http://www.persianacademy.ir/

مقدمه

مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴، سیستم‌های رمزنگاری[1] (سیستم‌های رمزگذاری[2]) را جهت تامین محرمانگی داده مشخص می‌کند. الگوریتم‌های رمزنگاری در مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴ با هدف ترویج استفاده از آنها به عنوان بازتابی از جدیدترین فن‌آوری‌های موجود در فنون رمزنگاری ذکرشده‌اند.

هدف اصلی از فنون رمزنگاری (به‌رمزدرآوردن[3])، حفاظت از محرمانگی داده‌های ذخیره شده یا ارسال شده است. برای تولید داده رمزنگاری‌شده، یک الگوریتم رمزنگاری بر روی داده (که اغلب متن خام یا متن اصلی نامیده می‌شود) اعمال‌می‌شود و به این فرایند رمزنگاری گفته‌می‌شود. توصیه می‌شود که الگوریتم رمزنگاری به گونه‌ای طراحی شود که متن رمزشده هیچگونه اطلاعاتی درباره متن خام، احتمالا بجز طول آن، را مشخص ننماید. همراه با هر الگوریتم رمزنگاری یک الگوریتم رمزگشایی متناظر نیز وجود دارد که متن رمزشده را دوباره به متن اصلی تبدیل می‌کند.

الگوریتم‌های رمزگذاری همراه با یک کلید کار می‌کنند. در یک الگوریتم رمزگذاری متقارن، یک کلید برای هر دو الگوریتم رمزنگاری و رمزگشایی مورد استفاده قرار می‌گیرد. در یک الگوریتم رمزگذاری نامتقارن، از دو کلید متفاوت اما مرتبط برای رمزنگاری و رمزگشایی استفاده می‌شود. استاندارد ISO/IEC 18033-2 به الگوریتم‌های رمزگذاری نامتقارن و استانداردهای ISO/IEC 18033-3 و استاندارد ملی ایران به شماره ۱۰۸۲۴-۴ به دو طبقه[4] متفاوت از الگوریتم‌های رمزگذاری متقارن که با نام‌های الگوریتم رمزگذاری قطعه‌ای و الگوریتم رمزگذاری جریانی شناخته می‌شوند، اختصاص داده شده‌اند.

1- Encryption systems

2- Cipher

این واژه در قالب مفهوم کلی رمزگذاری به عبارت‌های الگوریتم رمزگذاری و سیستم رمزگذاری اشاره دارد. در برخی موارد این واژه به معنی متن‌رمزشده نیز می‌باشد.

3- Encipherment

4- Class

فن‌آوری اطلاعات - فنون امنیتی - الگوریتم‌های رمزنگاری -- قسمت اول : کلیات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، گردآوری تعاریف مورد استفاده در قسمت‌های بعدی این مجموعه استاندارد است. در این استاندارد، ماهیت رمزنگاری معرفی شده و جنبه‌های عمومی استفاده از آن و خصوصیات آن شرح داده‌شده‌اند. معیارهای استفاده شده برای انتخاب الگوریتم‌ها در قسمت‌های بعدی مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴، در پیوست الف ذکر شده است.

۲ اصطلاحات و تعاریف

در این سند، اصطلاحات و تعاریف زیر بکار برده می‌شوند.

۲-۱ سیستم رمزگذاری نامتقارن[1]

اصطلاح جایگزین برای سیستم رمزنگاری نامتقارن.

۲-۲ فن رمزنگاری نامتقارن[2]

یک فن رمزنگاری که از دو تبدیل مرتبط با هم استفاده می‌کند، تبدیل عمومی (تعریف شده توسط یک کلید عمومی) و تبدیل خصوصی (تعریف شده توسط یک کلید خصوصی). این دو تبدیل دارای این خصوصیت هستند که با در اختیار داشتن تبدیل عمومی، دستیابی به تبدیل خصوصی از لحاظ محاسباتی غیرعملی است.

[ISO/IEC 11770-1:1996]

۲-۳ سیستم به‌رمزدرآوردن نامتقارن[3]

اصطلاح جایگزین برای سیستم رمزنگاری نامتقارن.

۲-۴ سیستم رمزنگاری نامتقارن[4]

یک سیستم مبتنی‌بر فنون رمزنگاری نامتقارن است که تبدیل عمومی آن برای رمزنگاری و تبدیل خصوصی آن برای رمزگشایی مورد استفاده قرار می‌گیرد.

[ISO/IEC 9798-1:1997]

1- Asymmetric cipher
2- Asymmetric cryptographic technique
3- Asymmetric encipherment system
4- Asymmetric encryption system

۲-۵ جفت کلید نامتقارن[1]

یک جفت کلید مرتبط است که کلید خصوصی، تبدیل خصوصی و کلید عمومی، تبدیل عمومی را تعیین می‌کند.
[ISO/IEC 9798-1:1997]

۲-۶ قطعه[2]

رشته‌ای از بیت‌ها با طول مشخص.

۲-۷ سیستم رمزگذاری قطعه‌ای[3]

سیستم رمزنگاری متقارن با این خصوصیت که الگوریتم رمزنگاری بر روی یک قطعه از متن خام اعمال شده، به عبارت دیگر رشته ای از بیت‌ها با طول مشخص؛ و یک قطعه از متن رمزشده را نتیجه می‌دهد.

۲-۸ سیستم رمزگذاری

اصطلاح جایگزین برای سیستم به‌رمزدرآوردن.

۲-۹ متن رمز شده[4]

داده ای که با هدف مخفی کردن محتویات آن، تغییر شکل داده شده است.
[استاندارد ملی ایران به شماره ۹۶۰۰]

۲-۱۰ متن اصلی[5]

اصطلاح جایگزین برای متن خام.

۲-۱۱ رمزبرداری[6]

اصطلاح جایگزین برای رمزگشایی.

۲-۱۲ الگوریتم رمزبرداری[7]

اصطلاح جایگزین برای الگوریتم رمزگشایی.

۲-۱۳ رمزگشایی[8]

برگشت عملیات به‌رمزدرآوردن متناظر.

1- Asymmetric key pair
2- Block
3- Block cipher
4- Ciphertext
5- Cleartext
6- Decipherment
7- Decipherment algorithm
8- Decryption

[ISO/IEC 11770-1:1996]

۲-۱۴ الگوریتم رمزگشایی[1]

فرآیندی که متن رمز شده را به متن اصلی تبدیل می‌کند.

۲-۱۵ به رمزدرآوردن

اصطلاح جایگزین برای رمزنگاری.

۲-۱۶ الگوریتم به‌رمزدرآوردن[2]

اصطلاح جایگزین برای الگوریتم رمزنگاری.

۲-۱۷ سیستم به‌رمزدرآوردن[3]

اصطلاح جایگزین برای سیستم رمزنگاری.

۲-۱۸ رمزنگاری[4]

تبدیل (برگشت پذیر) داده با استفاده از یک الگوریتم رمزنگاری جهت تولید متن رمزشده؛ به عبارت دیگر مخفی کردن محتوای اطلاعات داده.
[ISO/IEC 9797-1]

۲-۱۹ الگوریتم رمزنگاری[5]

فرآیندی که متن خام را به متن رمز شده تبدیل می‌کند.

۲-۲۰ سیستم رمزنگاری[6]

فن رمزنگاری مورد استفاده برای حفاظت از محرمانگی داده است که از یک فرآیند سه جزئی تشکیل شده است: یک الگوریتم رمزنگاری، یک الگوریتم رمزگشایی و یک روش برای تولید کلید.

۲-۲۱ کلید[7]

دنباله‌ای از نمادها که تبدیل رمزنگاری داده را کنترل می‌کند. (مانند رمزگذاری و رمزگشایی).
[ISO/IEC 11770-1:1996]

1- Decryption algorithm
2- Encipherment algorithm
3- Encipherment system
4- Encryption
5- Encryption algorithm
6- Encryption system
7- Key

۲-۲۲ رشته کلید[1]

رشته‌ای شبه تصادفی از نمادها است، که تلاش می‌شود تا محرمانه نگاه داشته شود و توسط الگوریتم‌های رمزنگاری و رمزگشایی مربوط به یک رمز دنباله‌ای مورد استفاده قرار می‌گیرد. اگر بخشی از رشته کلید در اختیار حمله کننده قرار گیرد، باید استنباط کردن اطلاعاتی درباره سایر بخش‌های رشته کلید برای حمله کننده از لحاظ محاسباتی غیرعملی باشد.

۲-۲۳ رمزگذاری قطعه‌ای n- بیتی[2]

رمزگذاری قطعه‌ای با این خصوصیت که طول قطعات متن خام و متن رمزی n-بیت است.
[استاندارد ملی ایران به شماره ۹۶۰۰]

۲-۲۴ متن خام[3]

اطلاعات رمزنگاری نشده.
[استاندارد ملی ایران به شماره ۹۶۰۰]

۲-۲۵ کلید خصوصی[4]

کلیدی از زوج کلید نامتقارن یک نهاد که توصیه می‌شود تنها توسط همان نهاد مورد استفاده قرار گیرد.
[ISO/IEC 11770-1:1996]

یادآوری- توصیه می‌شود کلید خصوصی به طور معمول افشا نشود.

۲-۲۶ کلید عمومی[5]

کلیدی از زوج کلید نامتقارن یک نهاد که می‌تواند در اختیار عموم قرار داده شود.
[ISO/IEC 11770-1:1996]

۲-۲۷ کلید محرمانه[6]

کلیدی که به همراه فنون رمزنگاری متقارن، توسط مجموعه‌ای مشخص از نهادها مورد استفاده قرار می‌گیرد.
[ISO/IEC 11770-3:1999]

۲-۲۸ رمزگذاری جریانی خود همزمان[7]

رمزگذاری جریانی با این خصوصیت که نمادهای رشته کلید، بصورت تابعی از یک کلید محرمانه و تعداد ثابتی از بیت‌های متن رمزی قبلی تولید می‌شوند.

1- Keystream
2- N-bit block cipher
3- Plaintext
4- Private key
5- Public key
6- Secret key
7- Self-synchronous stream cipher

۲-۲۹ رمزگذاری جریانی همزمان[1]

رمزگذاری جریانی با این خصوصیت که نمادهای رشته کلید، بصورت تابعی از یک کلید محرمانه تولید می-شوند و از متن خام و متن رمزی مستقل هستند.

۲-۳۰ رمزگذاری جریانی[2]

سیستم رمزنگاری متقارن[3] با این خصوصیت که الگوریتم رمزنگاری، در هر لحظه دنباله‌ای از نمادهای متن خام و دنباله‌ای از نمادهای رشته کلید را با استفاده از یک تابع معکوس‌پذیر بصورت نماد به نماد ترکیب می کند. دو نوع الگوریتم رمزگذاری جریانی وجود دارند: الگوریتم‌های رمزگذاری جریانی همزمان و الگوریتم‌های رمزگذاری جریانی خود همزمان، که با توجه به شیوه مورد استفاده برای بدست آوردن رشته کلید شناسایی می‌شوند.

۲-۳۱ رمزگذاری متقارن[4]

اصطلاح جایگزین برای سیستم رمزنگاری متقارن.

۲-۳۲ فن رمزنگاری متقارن[5]

یک فن رمزنگاری که در آن برای تبدیل داده هم در مبدا و هم مقصد از یک کلید محرمانه یکسان استفاده می‌شود. بدون اطلاع از کلید محرمانه، محاسبه کردن تبدیل انجام شده در مبدا و مقصد از لحاظ محاسباتی غیرعملی است.

یادآوری- متن‌های رمزشده متقارن و کدهای احراز اصالت پیام (MACs) [6]، مثال‌هایی از فنون رمزنگاری متقارن هستند. در یک الگوریتم رمزگذاری‌متقارن، برای رمزنگاری و رمزگشایی داده از یک کلید محرمانه یکسان استفاده می‌شود. در یک طرح MAC برای تولید و بررسی درستی یا نادرستی کدهای احراز اصالت پیام از کلید محرمانه یکسان استفاده می‌شود.

۲-۳۳ سیستم به‌رمزدرآوردن متقارن[7]

اصطلاح جایگزین برای سیستم رمزنگاری متقارن.

۲-۳۴ سیستم رمزنگاری متقارن

سیستم رمزنگاری مبتنی‌بر فنون رمزنگاری متقارن است که برای الگوریتم‌های رمزنگاری و رمزگشایی، از یک کلید محرمانه یکسان استفاده می‌کند.

1- Synchronous stream cipher
2- Stream cipher
2- Symmetric encryption system
4- Symmetric cipher
5- Symmetric cryptographic technique
6- Message Authentication Codes
7- Symmetric encipherment system

۳ ماهیت رمزنگاری

۳-۱ هدف از رمزنگاری

هدف اصلی بکارگیری سیستم‌های رمزنگاری (یا رمزگذاری) حفاظت از محرمانگی داده‌های ذخیره شده یا ارسال شده است. الگوریتم‌های رمزنگاری جهت دستیابی به این هدف، متن خام را به متن رمزشده تبدیل می‌کنند و بدین‌ترتیب دستیابی به هرگونه اطلاعات درباره محتویات متن خام بدون استفاده از کلید رمزگشایی از لحاظ محاسباتی غیرعملی است. با این وجود عموماً طول متن خام توسط رمزنگاری از دید پنهان نمی‌شود زیرا معمولاً طول متن رمزشده برابر و یا کمی بیشتر از طول متن خام متناظر است.

مساله مهمی که باید به آن توجه شود این است که رمزنگاری همیشه - به خودی خود - از تمامیت[1] یا اصالت[2] داده حفاظت نمی‌کند. در بسیاری از موارد این امکان وجود دارد که بدون دانستن کلید، متن‌رمزشده را بصورتی تغییرداد که اثرات قابل‌پیش‌بینی در متن‌خام بازیابی‌شده بوجودآید. برای اطمینان از تمامیت و اصالت داده، اغلب استفاده از روش‌های تکمیلی مانند روش‌هایی که در استانداردهای ISO/IEC 9796، ISO/IEC 9797، ISO/IEC 14888، ISO/IEC 15946-2، ISO/IEC 15946-4 و استاندارد بین‌المللی آتی ISO/IEC 19772 شرح داده شده‌اند، نیز ضروری است.

۳-۲ رمزگذاری متقارن و نامتقارن

هر الگوریتم رمزگذاری به همراه یک کلید، وظیفه خود را انجام می‌دهد.

در یک رمزگذاری متقارن از یک کلید محرمانه در الگوریتم‌های رمزنگاری و رمزگشایی استفاده می‌شود. دانستن کلید محرمانه برای انجام دادن هر دو عملیات رمزنگاری و رمزگشایی الزامی است، بنابراین لازم است که کلید محرمانه تنها در اختیار طرف‌هایی قرارگیرد که مجاز به دسترسی به داده‌هایی هستند که کلید برای رمزنگاری آنها بکار رفته است.

در یک رمزگذاری نامتقارن از کلیدهای متفاوت و در عین حال مرتبط برای رمزنگاری و رمزگشایی استفاده می‌شود. بنابراین کلیدها در مجموعه‌های دوتایی هماهنگ تولید می‌شوند، یکی از کلیدها به عنوان کلید رمزنگاری و کلید دیگر به عنوان کلید رمزگشایی مورد استفاده قرار می‌گیرند. حتی با دانستن کلید رمزنگاری، دستیابی به هرگونه اطلاعاتی درباره متن خام از روی متن رمزشده متناظر، از لحاظ محاسباتی غیرعملی فرض می شود. در بسیاری از موارد این امکان وجود دارد که کلید رمزنگاری را در اختیار عموم قرار داد، در اینصورت به کلید رمزنگاری، کلید عمومی گفته می‌شود. در عوض کلید رمزگشایی تنها دارای یک مالک بوده و محرمانه نگاه داشته می‌شود (در اینصورت به کلید رمزگشایی، کلید خصوصی گفته می‌شود). هر شخصی که از کلید رمزنگاری عمومی آگاه باشد می‌تواند داده‌ها را برای ارسال به شخصی که کلید رمزگشایی را در اختیار دارد، رمزنگاری کند بدین‌ترتیب تنها شخص دارنده کلید خصوصی می‌تواند داده‌ها را رمزگشایی نماید.

1- Integrity of data
2- Origin of data

یادآوری- یک الگوریتم رمزگذاری نامتقارن شامل عملیاتی است که نسبت به یک الگوریتم رمزگذاری متقارن، دارای پیچیدگی محاسباتی بسیار بیشتری است و بطور معمول از الگوریتم‌های رمزگذاری نامتقارن برای رمزنگاری داده‌هایی با حجم بالا استفاده نمی‌شود؛ در عوض این الگوریتم‌ها برای رمزنگاری کلیدهای محرمانه نشست (کلیدهایی که در الگوریتم‌های رمزگذاری متقارن مورد استفاده قرار می گیرند) بکار گرفته می‌شوند. به هر حال تعدادی از الگوریتم‌های رمزگذاری نامتقارن که در استاندارد ISO/IEC 18033-2 شرح داده شده‌اند، به گونه‌ای طراحی شده‌اند که برای رمزنگاری داده‌هایی با حجم بالا نیز مناسب می‌باشند.

استاندارد ISO/IEC 18033-2 به الگوریتم‌های رمزگذاری نامتقارن اختصاص یافته است. استانداردهای ISO/IEC 18033-3 و استاندارد ملی ایران به شماره ۴-۱۰۸۲۴ به دو نوع مختلف از الگوریتم‌های رمزگذاری متقارن به نام‌های الگوریتم‌های رمزگذاری قطعه‌ای و الگوریتم‌های رمزگذاری جریانی، اختصاص یافته‌اند.

۳-۳ مدیریت کلید

همه روش‌های رمزنگاری با تکیه بر مدیریت کلیدهای رمزنگاری مورد استفاده قرار می‌گیرند. تمامی الگوریتم‌های رمزگذاری، متقارن و یا نامتقارن، الزام دارند که طرف‌های استفاده کننده از الگوریتم رمزگذاری به کلیدهای ضروری دسترسی داشته باشند. این امر موجب افزایش نیاز به مساله مدیریت کلید - شامل تولید، توزیع و مدیریت مستمر کلیدها - می‌شود. یک چهارچوب کلی برای مدیریت کلید در استاندارد ISO/IEC 11770-1 ارائه شده است.

مساله مدیریت کلید برحسب اینکه کلیدها مربوط به الگوریتم‌های رمزگذاری متقارن یا نامتقارن هستند، متفاوت است. برای الگوریتم‌های رمزگذاری متقارن ضروری است که کلیدهای محرمانه توسط جفت‌ها (یا گروه‌های بزرگ) تولید شده و به اشتراک گذاشته شود. برای الگوریتم‌های رمزگذاری نامتقارن ضروری است که تولید جفت کلیدها و توزیع کلیدهای عمومی به گونه‌ای انجام شود که اصلیت[1] آنها تضمین شود.

روش‌های برقرار کردن کلیدهای محرمانه اشتراکی با استفاده از روش‌های رمزنگاری متقارن در استاندارد ISO/IEC 11770-2 مشخص شده‌اند. روش‌های برقرار کردن کلیدهای محرمانه اشتراکی با استفاده از روش-های رمزنگاری نامتقارن در استاندارد ISO/IEC 11770-3 مشخص شده‌اند؛ در استاندارد بین‌المللی اخیر همچنین روش‌هایی برای توزیع قابل اطمینان کلیدهای عمومی - مربوط به روش‌های رمزنگاری نامتقارن - مشخص شده‌اند.

۴ کاربرد و خصوصیات رمزنگاری

۴-۱ رمزگذاری نامتقارن

الگوریتم رمزنگاری مورد استفاده برای رمزگذاری نامتقارن، نگاشتی از مجموعه پیام‌های متن‌خام مجاز (معمولا به شکل مجموعه‌ای از رشته بیت‌ها) به مجموعه پیام‌های متن رمزشده (باز هم معمولا به شکل مجموعه‌ای از رشته بیت‌ها) را تعریف می‌کند. مجموعه پیام‌های مجاز و مجموعه متن رمزشده، به الگوریتم رمزگذاری و جفت کلید انتخابی وابسته هستند.

1- Authenticity

در رمزگذاری نامتقارن، الگوریتم رمزنگاری به کلید عمومی وابسته است، درحالیکه رمزگشایی به کلید خصوصی بستگی دارد. بنابراین ضمن اینکه قطعه متن رمزشده متناظر با یک متن خام ممکن است به سادگی محاسبه شود، برای هر شخصی بجز صاحب کلید خصوصی، استنباط کردن قطعه متن خام متناظر با یک قطعه متن رمزشده انتخابی، باید عملی نباشد. در هر حال اگر یک شنودکننده غیر مجاز[1] متن رمزشده، کلید عمومی مورد استفاده برای تهیه متن رمزشده را در اختیار داشته باشد و همچنین بداند که متن خام از بین مجموعه‌ای کوچک از احتمالات انتخاب شده است، قادر خواهد بود تا متن خام را با انجام جستجوی کامل روی همه متن‌های خام محتمل استنباط کند.

در نتیجه و در راستای دستیابی به یک سطح امنیت مطلوب، آمیختن داده‌های تصادفی در فرآیند رمزنگاری به گونه‌ای که قطعه متن رمزشده متناظر با قطعه متن خام داده شده قابل پیش‌بینی نباشد، ضروری است. روش‌های جزئی درباره چگونگی آمیختن داده‌های تصادفی در استاندارد ISO/IEC 18033-2 تشریح شده‌اند.

۴-۲ رمزگذاری قطعه‌ای

یک الگوریتم رمزگذاری قطعه‌ای، یک الگوریتم رمزگذاری متقارن است با این خصوصیت که الگوریتم رمزنگاری بر روی قطعه‌هایی از متن خام اعمال شده، به عبارت دیگر رشته‌هایی از بیت‌ها با طول مشخص؛ و قطعه‌هایی از متن رمزشده را نتیجه می‌دهد. هر کلید رمزگذاری قطعه‌ای، یک نگاشت معکوس پذیر خاص از قطعه‌های متن خام به قطعه های متن رمز شده را تعریف می‌کند (و یک نگاشت معکوس متناظر برای رمزگشایی مورد استفاده قرار می‌گیرد). چنانچه قطعه‌های متن خام و قطعه‌های متن رمزشده همگی قطعه-هایی از n رقم دودویی باشند - که معمولا همینطور است - آنگاه هرکلید به سادگی یک جایگشت[2] روی مجموعه تمامی قطعه‌های n- بیتی تعریف می‌کند.

۴-۲-۱ حالت‌های عملیاتی

روش‌های بسیاری برای بکارگیری یک الگوریتم رمزگذاری قطعه‌ای n- بیتی برای به‌رمزدرآوردن متن خام وجود دارد؛ این روش‌ها با نام حالت‌های عملیاتی الگوریتم‌های رمزگذاری قطعه‌ای نامیده می‌شوند. حالت‌های عملیاتی در استاندارد ملی ایران به شماره ۹۶۰۰ تعریف شده‌اند. اگر تعداد بیت‌ها در متن خام برابر با n باشد، آنگاه رمزنگاری به سادگی و با اعمال فرآیند رمزنگاری روی قطعه انجام می‌شود. در هر حال برای متن خام با طول دلخواه، بکارگیری یک روش پیچیده تر ضروری است. به این دلیل و به دلایل دیگر، غالبا استفاده از یکی دیگر از حالت‌های عملیاتی تعریف شده در استاندارد ملی ایران به شماره ۹۶۰۰ ضروری است.

۴-۲-۲ کدهای احراز اصالت پیام (MACs)

اگرچه رمزنگاری تمامیت داده را تامین نمی‌کند، می‌توان یک الگوریتم رمزگذاری قطعه‌ای را طبق یک شیوه تعریف شده خاص برای تامین وظیفه حفاظت از تمامیت داده مورد استفاده قرار داد. در حالت خاص، استفاده از یک الگوریتم رمزگذاری قطعه‌ای برای محاسبه کد احراز اصالت پیام (MAC) برای یک رشته از بیت‌ها،

2- Interceptor
1- Permutation

امکان‌پذیر است. این کد احراز اصالت پیام می‌تواند برای حفاظت از تمامیت و اصالت رشته بیت مورد استفاده قرار گیرد. راه‌های دستیابی به این هدف در استاندارد ISO/IEC 9797-1 مشخص شده‌اند. توجه کنید که گاهی استفاده از یک الگوریتم رمزگذاری قطعه‌ای برای رمزنگاری و نیز محاسبه یک کد احراز اصالت پیام روی یک متن خام، مطلوب می باشد. در این مواقع، عموما بکارگیری دو کلید محرمانه متفاوت - یک کلید برای رمزنگاری و دیگری برای محاسبه کد احراز اصالت پیام - ضروری است.

یادآوری- اگر ترکیبی خاص از کد احراز اصالت پیام و رمزنگاری، بصورت خاص امکان استفاده از کلید محرمانه یکسان را فراهم سازد، آنگاه نیازی به دو کلید مجزا نخواهد بود.

۴-۳ رمزگذاری جریانی

یک الگوریتم رمزگذاری جریانی همواره بر اساس یک مولد رشته کلید پایه‌گذاری می‌شود، به‌عبارت‌دیگر یک تابع که زمانی که یک کلید محرمانه (و یا احتمالا متن رمزشده قبلی) به عنوان ورودی به آن داده می‌شود، دنباله‌ای از نمادها - که به نام رشته کلید شناخته می‌شود - را در خروجی تولید می‌کند. این دنباله برای رمزنگاری متن خام مورد استفاده قرار می‌گیرد، بدین منظور دنباله کلید با استفاده از یک تابع معکوس‌پذیر (مانند عمل یای انحصاری بیتی[1]) بصورت یک نماد دریک‌زمان با دنباله نمادهای متن خام ترکیب می‌شود.
بطور معمول، اگر از همین کلید بیش از یک بار برای مقدار دهی اولیه مولد کلید استفاده شود، آنگاه رشته کلیدهای یکسانی ایجاد خواهند شد. اگر از یک رشته کلید مشابه جهت رمزنگاری بیش از یک متن خام استفاده شود، آنگاه این خطر وجود دارد که شنود کننده این متن‌های رمزشده، قادر به استنباط اطلاعاتی درباره هر دو متن خام باشد. در نتیجه، ضروری است که تمهیداتی اندیشیده شود تا برای رمزنگاری هر متن خام، یک رشته کلید متفاوت مورد استفاده قرار گیرد. این مباحث کلیدی در استاندارد ملی ایران به شماره ۴-۱۰۸۲۴ به صورت کامل تشریح شده‌اند.
الگوریتم‌های رمزگذاری جریانی همیشه حفاظت از تمامیت متن‌خام را تامین نمی‌کنند. در مواردی که عمل رمزنگاریِ الگوریتم‌رمزگذاری‌جریانی شامل جمع پیمانه‌ای بیتی در مبنای ۲ بین متن‌خام و رشته کلید است، تغییر یک بیت در متن‌رمزشده موجب تغییر یک بیت در متن‌خام بازیابی شده‌می‌شود. همچنین، اینگونه الگوریتم‌های‌رمزگذاری‌جریانی همواره طول دقیق متن‌خام را فاش می‌کنند.

۵ شناسه شیء

مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴ نامی یکتا (یک شناسه شیء OSI[2]) را به هر الگوریتم‌رمز مشخص‌شده، اختصاص می‌دهد. در کاربردهایی که در آنها از شناسه‌های شیء استفاده می‌شود، شناسه‌های شئ مشخص‌شده در مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴، بر سایر شناسه‌های شئ مجاز موجود برای الگوریتم‌ها ارجحیت دارند.

1- Bit-wise exclusive-or operation
2- Open System Interconnection

پیوست الف
(اطلاعاتی)

معیارهای انتخاب الگوریتم‌های رمزگذاری در مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴

الگوریتم‌های رمزگذاری ذکر شده در قسمت‌های بعدی مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴ از بین تعداد زیادی از روش‌های منتشر شده و مورد استفاده، انتخاب شده‌اند. مستثنی نمودن الگوریتم‌های رمزگذاری خاص بدین معنی نیست که این روش‌ها ناامن هستند. الگوریتم‌های رمزگذاری مشخص شده، مجموعه‌ای کوچک از روش‌های انتخابی را طبق معیارهای زیر نمایش می‌دهند (ترتیب نمایش معیارها دارای اهمیت نیست).

ارزیابی‌ها با توجه به جنبه‌های رمزگذاری زیر انجام شده‌اند.

۱- امنیت الگوریتم رمزگذاری، به‌عبارت‌دیگر الگوریتم‌های انتخاب شده باید در برابر حملات تحلیلی مقاوم باشند. برای حصول این شرط، وجود یک اثبات برای امنیت - مانند یک استدلال مهم برای جانبداری از یک الگوریتم رمزگذاری - با استناد به مدل‌امنیتی و فرضیات اثبات، مورد توجه قرارگرفته است. ماهیت ارزیابی‌ها دارای اهمیت بسیار است، خصوصا آن دسته از ارزیابی‌ها که توسط سازمان‌های ارزیابی‌کننده مشهور هدایت می شوند.

۲- کارایی الگوریتم رمزگذاری روی تعدادی از بسترهای گوناگون متداول. این بند نه تنها شامل مباحثی چون کارایی زمان و فضا است بلکه به این نکته نیز توجه شده است که آیا الگوریتم رمزگذاری دارای ویژگی‌هایی است که آن را نسبت به سایر روش‌ها ممتاز می‌سازد یا خیر.

۳- ماهیت هرگونه مباحث مربوط به اخذ مجوز که الگوریتم رمزگذاری را تحت تاثیر قرار می‌دهد.

۴- بلوغ الگوریتم رمزگذاری. بلوغ الگوریتم رمزگذاری با توجه به مواردی چون وسعت دامنه استفاده از الگوریتم، گسترده بودن تحلیل‌های منتشر شده و سطح شکست الگوریتم رمزگذاری ارزیابی می‌شود.

۵- درجه‌ای که از سوی یک سازمان شناخته شده (مانند سازمان استاندارد[1]، یک آژانس امنیتی دولتی یا ...) به الگوریتم رمزگذاری تنفیذ شده‌است یا تنفیذ درجه توسط چنین سازمانی دردست‌بررسی یا تجزیه‌وتحلیل است.

۶- سطح پذیرش فعلی الگوریتم رمزگذاری. در صورتی که سایر ملاحظات باعث صرف‌نظر کردن از این مشخصه نشوند، الگوریتم‌های رمزگذاری متداول - که به آنها استانداردهای عملی[2] نیز گفته می‌شود - به سایر الگوریتم‌هایی که کمتر مورد استفاده قرار می‌گیرند، ترجیح داده می‌شوند.

۷- در حالت کلی توصیه می‌شود که تعداد الگوریتم‌های رمزگذاری استانداردشده در هر قسمت از مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۴ تا حد امکان کم باشد. دو استثنا برای این قاعده وجود دارد.

1- Standard body
2- De facto Standards

الف) هنگامیکه دو الگوریتم رمزگذاری دارای ویژگی‌های متفاوتی باشند، مانند الگوریتم‌های رمزگذاری قطعه‌ای n- بیتی که دارای مقادیر n متفاوت هستند یا الگوریتم‌های رمزگذاری که الزامات پیاده‌سازی آنها تا حد زیادی از نظر حجم محاسبات و فضا با یکدیگر متفاوت هستند، و هر دو مجموعه ویژگی از نظر عملی دارای اهمیت می‌باشند، الگوریتم‌های رمزگذاری از هر دو نوع احتمالا استانداردسازی خواهند شد.
ب) عموماً در اختیار داشتن الگوریتم‌های رمزگذاری استاندارد بر پایه قواعد بنیادی متفاوت مطلوب است، بدین‌ترتیب که اگر یک الگوریتم رمزگذاری در برابر حملات تحلیل‌رمز آسیب‌پذیر شد، سایر الگوریتم‌های رمزگذاری شانس خوبی برای ایمن ماندن خواهند داشت.

کتابنامه

۱- استاندارد ملی ایران ۹۶۰۰ : سال ۱۳۸۶، فن آوری اطلاعات - روش‌های امنیتی - حالت‌های عملیاتی یک الگوریتم رمزنگاری قطعه‌ای n بیتی

2- ISO/IEC 9796 (all parts), Information technology - Security techniques - Digital signature schemes giving message recovery

3- ISO/IEC 9797 (all parts), Information technology - Security techniques - Message Authentication Codes (MACs)

4- ISO/IEC 9798-1:1997, Information technology - Security techniques - Entity authentication - Part 1: General

5- ISO/IEC 10118-2:2000, Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher

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

7- ISO/IEC 14888 (all parts), Information technology - Security techniques - Digital signatures with appendix

8- ISO/IEC 15946-2, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures

9- ISO/IEC 15946-4, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery

10- ISO/IEC 19772, Information technology - Security techniques - Authenticated encryption mechanisms

11- Federal Information Processing Standards Publications (FIPS PUBS)