سیستم مدیریت ایزو
www.isomanagement.ir

تماس تلفنی جهت دریافت مشاوره:

۱. مشاور دفتر تهران (آقای محسن ممیز)

۰۹۱۲ ۹۶۳ ۹۳۳۶

۲. مشاور دفتر اصفهان (سرکار خانم لیلا ممیز)

۰۹۱۳ ۳۲۲ ۸۲۵۹

مجموعه **سیستم مدیریت ایزو** با هدف بهبود مستمرعملکرد خود و افزایش رضایت مشتریان سعی بر آن داشته، کلیه استانداردهای ملی و بین المللی را در فضای مجازی نشر داده و اطلاع رسانی کند، که تمام مردم ایران از حقوق اولیه شهروندی خود آگاهی لازم را کسب نمایند و از طرف دیگر کلیه مراکز و کارخانه جات بتوانند به راحتی به استانداردهای مورد نیاز دسترسی داشته باشند.

این موسسه اعلام می دارد در کلیه گرایشهای سیستم های بین المللی ISO پیشگام بوده و کلیه مشاوره های ایزو به صورت رایگان و صدور گواهینامه ها تحت اعتبارات بین المللی سازمان جهانی IAF و تامین صلاحیت ایران می باشد.

هم اکنون سیستم خود را با معیارهای جهانی سازگارکنید...

ISO 9001 14001 18001

CE

GMP GAP 22716

IMS HSE-MS

45001

22000 HACCP

INSO
15713-1
1st Edition
2019
Identical with
ISO IEC 19592-1: 2016

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

استاندارد ملی ایران
۱-۱۵۷۱۳
چاپ اول
۱۳۹۷

فناوری اطلاعات- فنون امنیت- تسهیم راز- قسمت ۱: کلیات

Information technology- Security techniques- Secret sharing- Part 1: General

ICS: 35.030

استاندارد ملی ایران شمارهٔ ۱-۱۵۷۱۳ (چاپ اول): سال ۱۳۹۷

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

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه۱۳۷۱تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشراستانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های 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، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 در کمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود 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 به عنوان تنها رابط[4] کمیسیون کدکس غذایی(CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه 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 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 کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. 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 واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد 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، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4-Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیت- تسهیم راز- قسمت ۱: کلیات»

رئیس:	**سمت و/یا محل اشتغال:**
علیزاده، مجتبی (دکتری مهندسی کامپیوتر- امنیت اطلاعات)	عضو هیات علمی دانشگاه لرستان- مشاور شرکت پایش کیفیت ماهان پیشگام کرمان
دبیر:	
سالار کریمی، هادی (کارشناسی مهندسی تکنولوژی نرم‌افزار)	کارشناس اندازه‌شناسی، اوزان و مقیاس‌ها- اداره کل استاندارد استان کرمان
اعضا: (اسامی به ترتیب حروف الفبا)	
آزادی مطلق، مهدی (دکتری مهندسی کامپیوتر- فناوری اطلاعات)	کارشناس اداره طرح و برنامه رمزنگاری شرکت مدیریت امن الکترونیکی کاشف
بیت‌الهی، محدثه (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	کارشناس امور استاندارد و فناوری اطلاعات- اداره کل استاندارد استان کرمان
جوانمرد، جواد (کارشناسی ارشد مهندسی کامپیوتر- سخت‌افزار)	مدرس- دانشگاه آزاد اسلامی واحد خرم‌آباد
حیدرنژاد، امین (کارشناسی ارشد مهندسی کامپیوتر- فناوری اطلاعات)	عضو مستقل
خدادادی، تورج (دکتری امنیت اطلاعات)	کارشناس- شرکت پایش کیفیت ماهان پیشگام کرمان
خزائی، هما (کارشناسی مهندسی کامپیوتر- فناوری اطلاعات)	کارشناس امور استاندارد- اداره کل استاندارد استان کرمان
دهداری سی‌سخت، علیرضا (کارشناسی ارشد مهندسی کامپیوتر- علوم کامپیوتر)	مدرس- دانشگاه آزاد اسلامی واحد کرمان
شجاع چایی‌کار، سامان (دکتری مهندسی کامپیوتر- امنیت اطلاعات)	پژوهشگر- دانشگاه خواجه نصیرالدین طوسی
عروجی، سید مهدی (کارشناسی ارشد مدیریت فناوری اطلاعات)	سرپرست گروه تدوین استاندارد- سازمان تنظیم مقررات و ارتباطات رادیویی

اعضا: (اسامی به ترتیب حروف الفبا)	**سمت و/یا محل اشتغال:**
عطارپور، سیما (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	کارشناس فناوری اطلاعات- اداره کل استاندارد استان کرمان
کاظمی، رسول (کارشناسی ارشد مهندسی مخابرات- رمز)	کارشناس مرکز میانی عام- مرکز صدور گواهی الکترونیکی وزرات صنعت، معدن و تجارت (ریشه)
کرمی‌زاده، ساسان (دکتری علوم کامپیوتر- پردازش تصویر)	پژوهشگر- پژوهشکده امنیت پژوهشگاه ارتباطات و فناوری اطلاعات
کریمی، شبیر (کارشناسی ارشد مهندسی کامپیوتر- فناوری اطلاعات)	کارشناس- شرکت فنی و مهندسی مهرآفرین
کولیوند، داود (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	کارشناس فناوری اطلاعات- شرکت پایش کیفیت ماهان پیشگام کرمان

ویراستار:

عروجی، سید مهدی (کارشناسی ارشد مدیریت فناوری اطلاعات)	سرپرست گروه تدوین استاندارد- سازمان تنظیم مقررات و ارتباطات رادیویی

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیت- تسهیم راز- قسمت ۱: کلیات» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی/ منطقه‌ای به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در پانصد و نود و هفتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۷/۱۱/۱۵ 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 خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

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 19592-1: 2016, Information technology- Security techniques- Secret sharing- Part 1: General

مقدمه

الگوی تسهیم راز[1] نوعی فن رمزنگاری است که از آن برای حفظ محرمانگی پیام با تقسیم‌بندی آن به بخش‌هایی بنام سهم[2] استفاده می‌شود. الگوی تسهیم راز از دو بخش اصلی تشکیل می‌شود: یک الگوریتم تسهیم پیام[3] برای تقسیم کردن پیام به شُماری سهم و یک الگوریتم بازسازی پیام[4] برای بازسازی پیام با استفاده از همه یا زیرمجموعه‌ای از سهم‌ها.

اُلگوهای تسهیم راز را می‌توان برای ذخیره داده‌ها (برای مثال مقادیر محرمانه و/یا کلیدهای رمزنگاری) به‌طور امن در سیستم‌های توزیع شده[5] استفاده کرد. علاوه بر این، تسهیم راز، یک فن‌آوری اساسی برای محاسبات چند طرفه است[6] که می‌توان از آن برای حفاظت از پردازش داده‌ها در سیستم‌های توزیع شده بهره برد. برای آسان کردن استفاده موثر از این فن‌آوری و حفظ قابلیت همکاری بین قسمت‌های مختلف، مجموعه استاندارد ISO/IEC 19592 (کلیه قسمت‌ها)، به اُلگوهای تسهیم راز و فن‌آوری های مرتبط با آن اختصاص داده شده است.

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران شماره ۱۷۵۱۳ است.

این مجموعه استاندارد شامل موارد زیر است:

– قسمت ۱: کلیات

– Part 2: Fundamental mechanisms

1- Secret sharing scheme
2- Sharing
3- Message sharing algorithm
4- Message reconstruction algorithm
5- Distributed systems
6- Multi-party computation

فناوری اطلاعات- فنون امنیت- تسهیم راز- قسمت ۱: کلیات

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین طرفین مسئول در یک الگوی تسهیم راز، معرفی اصطلاحات و تعاریف مورد استفاده در متن تسهیم راز و خصوصیات و پارامترهای آن است.

مجموعه استاندارد ISO/IEC 19592، الگوی تسهیم راز و خصوصیات آن را تعیین می‌کند.

۲ مراجع الزامی

در این استاندارد مراجع الزامی کاربرد ندارد.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱

ساختار دسترسی

access structure

مجموعهٔ زیرمجموعه‌های تمام سهم-دارندگان[1] (به زیربند ۳-۱۱ مراجعه شود)، $A \subset \{S | S \subset \{1,\ldots,n\}\}$ است به‌طوری‌که برای همه $S,T \in A$، S زیرمجوعه T نبوده و T نیز زیرمجموعه S نباشد و سهم‌های (به زیربند ۳-۱۰ مراجعه شود) نگه داشته شده توسط سهم-دارندگان در مجموعه S، برای بازسازی موفقیت‌آمیز پیام (به زیربند ۳-۴ مراجعه شود) با استفاده از الگوریتم بازسازی[2] (به زیربند ۳-۵ مراجعه شود)، کافی باشد.

۳-۲

ساختار متخاصم (متضاد)

adversary structure

مجموعهٔ زیرمجموعه‌های تمام سهم-دارندگان (به زیربند ۳-۱۱ مراجعه شود)، $D \subset \{S \mid S \subset \{1,...,n\}\}$ است طوری‌که برای هر $S,T \in D$، S زیرمجموعه T نیست و T نیز زیرمجموعه S نیست و سهم‌های سهم-دارندگان (به زیربند ۳-۱۰ مراجعه شود) S، برای بازسازی پیام(به زیربند ۳-۴ مراجعه شود) کافی نیست.

1- Share Holders
2- Message Reconstruction Algorithm

۳-۳

واسط

dealer

طرف اجراکننده الگوریتم تسهیم پیام[1] (به زیربند ۳-۶ مراجعه شود) است.

۴-۳

پیام

message

اطلاعات محرمانه‌ای است که باید حفاظت شوند.

مثال: یک مقدار محرمانه و یا یک کلید رمزنگاری.

۵-۳

الگوریتم بازسازی پیام

message reconstruction algorithm

فرایندی که مجموعهٔ عناصر بازیابی‌پذیر بردار سهم را[2] (به زیربند ۳-۱۳ مراجعه شود) به پیام اولیّه (به زیربند ۳-۴ مراجعه شود) تبدیل می‌کند.

۶-۳

الگوریتم تسهیم پیام

message sharing algorithm

فرایندی که پیام‌ها (به زیربند ۳-۴ مراجعه شود) را به بردار سهم (به زیر بند ۳-۱۳ مراجعه شود) تبدیل می‌کند.

۷-۳

گستره پیام

message space

مجموعه‌ای از پیام‌ها (به زیربند ۳-۴ مراجعه شود) که می‌توان آن‌ها را با استفاده از اُلگوی تسهیم راز (به زیربند ۳-۹ مراجعه شود) به تسهیم گذاشت.

1- Message Sharing Algorithm
2- Share vector

۸-۳

دریافت‌کننده

receiver

طرف اجراکنندهٔ الگوریتم بازسازی پیام[1] (به زیربند ۳-۵ مراجعه شود) است.

۹-۳

تسهیم راز

secret sharing scheme

فنّ رمزنگاشتی‌ای برای حفاظت از محرمانگی پیام (به زیربند ۳-۴ مراجعه شود) با خُرد کردن آن پیام به چندین بخش یا سهم (به زیربند ۳-۱۰ مراجعه شود) است.

یادآوری- از دو فرایند شکل گرفته‌ست: الگوریتم تسهیم پیام و الگوریتم بازسازی پیام:

۱- الگوریتم تسهیم پیام؛

۲- الگوریتم بازسازی پیام.

۱۰-۳

سهم

share

عنصری از بُردار سهم (به زیربند ۳-۱۳ مراجعه شود) است.

۱۱-۳

دارنده سهم

share holder

طرفی که برونداد سهم را با الگوریتم تسهیم پیام (به زیربند ۳-۶ مراجعه شود) را انبار می‌کند.

۱۲-۳

گستره سهم

share space

مجموعه عناصر «اُلگوی تسهیم راز» (به زیربند ۳-۱۳ مراجعه شود) که روی بردار سهم (به زیربند ۳-۹ مراجعه شود) آشکار می‌شوند.

1- Message Reconstruction Algorithm

۱۳-۳

بردار سهم

share vector

بردار پدید آمده از برونداد مقادیر به‌دست آمده از الگوریتم تسهیم پیام (به زیربند ۳-۶ مراجعه شود) است.

۱۴-۳

آستانه

threshold

کمینه شُمار عناصر اصلاح‌نشدهٔ روی بردار سهم (به زیربند ۳-۱۳ مراجعه شود) است که در بازسازی موفقیت‌آمیز پیام به آن‌ها نیاز است.

۴ مدل همه‌پذیر تسهیم راز

۴-۱ گروه‌های درگیر

عملیات «اُلگوی تسهیم راز» سه نقش را در بر دارد:

الف- واسط[1]؛

ب- سهم-دارنده[2]؛

پ- دریافت‌کننده[3]

واسط کسی است که یک «پیام» دارد و الگوریتم تسهیم راز را اجرا می‌کند. پس از اجرای الگوریتم روی پیام برای دستیابی و رسیدن به بردار سهم، واسط سهم‌های روی بردار سهم را میان سهم-دارندگان بخش و پخش می‌کند. شیوه‌ای که برای پخش کردن سهم‌ها میان سهم-دارندگان به‌کار می‌رود، «کاربرد-بنیان» است و (همهٔ قسمت‌های آن) خارج از دامنهٔ کاربرد استاندارد ISO/IEC 15592 هستند.

دریافت‌کننده کسی است که می‌کوشد پیام را بازسازی کند. هنگامی‌که دریافت‌کننده می‌خواهد از پیام آگاه شود، سهم‌های گردآوری‌شده از مجموعهٔ گروه‌های مجاز را به شکل بردار سهم سرهم‌بندی می‌کند تا در «الگوریتم بازسازی پیام» به کار آید. اگر شُمار سهم‌های در دسترس برای بازسازی پیام بسنده باشد، دریافت‌کننده با اجرا کردن الگوریتم بازسازی پیام، از پیام آگاه می‌شود. دریافت‌کننده شاید بخواهد که با گردآوری سهم‌های هر چه بیشتر، بخت خود را در بازسازی موفقیت‌آمیز افزایش دهد. شیوه‌ای که دریافت‌کننده برای گردآوری سهم‌ها از سهم-دارندگان به‌کار می‌برد، «کاربرد-بنیان» است و (همهٔ

1- Dealer
2- Share holder
3- Reciever

قسمت‌های آن) از خارج از دامنهٔ کاربرد استاندارد ISO/IEC 15592 هستند. برای هر گروه می‌تواند بیش از یک «نقش» داشته باشد. میان چند گروه - برای نمونه- هر گروهی شاید پیامی داشته باشد که بخواهد آن را با هـمهٔ گروه‌ها- با خود نیز – سهـیم شود و در چنین الگویی، هر گروه همزمان، هم دریافت‌کننده و هم سهم-دارنده است.

۴-۲ پارامترها

۴-۲-۱ بررسی گذرا

پارامت_رهای زیر در تمام ال_گوهای تسهیم راز ارائه شده در مجموعه استاندارد ISO/IEC 19592 (همه قسمت‌های آن)، به‌کار برده می‌شوند:

الف- گسترهٔ پیام، توصیف‌شده در زیربند ۴-۲-۲؛

ب- گسترهٔ سهم‌دهی، توصیف‌شده در زیربند ۴-۲-۳؛

پ- شمار سهم‌ها، توصیف‌شده در زیربند ۴-۲-۴؛

ت- ساختار دسترسی، توصیف‌شده در زیربند ۴-۲-۵.

۴-۲-۲ گستره پیام[1]

گسترهٔ پیام مجموعه مقدارهای ممکن هر پیام است، به عبارتی یک «راز» که با به‌کارگیری الگوریتم سهم-دهی پیام به تعدادی «سهم» بخش می‌شود. زمانی که اُلگوی سهم‌دهی پیام، دامنه‌ای از گستره‌های امکان-پذیر پیام را در هر «نُمود و پدیداری» ویژه‌ای مجاز می‌شمارد، برای مثال: در پیوند با انواع گوناگون داده؛ گسترهٔ پیام تثبیت خواهد شد و همهٔ کاربران آن اُلگو از جزئیات گسترهٔ پیام آگاهند.

۴-۲-۳ گسترهٔ سهم[2]

گسترهٔ سهم شامل مجموعه اجزائی است که سهم‌های یک پیام از میان آن‌ها انتخاب می‌شوند. الگوریتم سهم‌دهی پیام یک بردار سهم‌دهی را تولید می‌کند که شامل اجزائی از گسترهٔ سهم‌دهی است. برای بسیاری از اُلگوهای سهم‌دهی راز، انتخاب گسترهٔ پیام مستقیماً گسترهٔ سهم را تثبیت می‌کند.

۴-۲-۴ شُمار سهم‌ها

یک اُلگوی سهم‌دهی راز، معمولاً می‌تواند یک پیام ورودی را به شُمار محدودی «سهم» بخش کند. در عمل، اُلگوهایی می‌خواهیم که بتوانند یک پیام را به دو یا چند «سهم» بخش کنند. هر نُمود و پدیداری «اُلگوی

1- Message Space
2- Share space

سهم‌دهی راز»، یک «الگوریتم سهم‌دهی پیام» را تعریف می‌کند که یک «بردار سهم» را با «n» تعداد سهم بیرون می‌دهد.

به طور همانند، هر نُمود و پدیداری اُلگوی سهم‌دهی راز، یک «الگوریتم بازسازی پیام» را تعریف می‌کند که پذیرای یک «بردار سهم» است با شُمار معیّن و کم و زیاد نشدنی از عناصر. باید دانست که برخی اُلگوهای سهم‌دهی راز می‌توانند حتی با «مقدار»هایی از «بردار سهم» که دستکاری شده‌اند یا اصلاً جای‌شان روی بردار سهم خالی است نیز، پیام‌ها را بازسازی کنند.

یادآوری- همواره، نُمود و پدیداری «اُلگوی سهم‌دهی راز»، دامنه‌ای از شُمار ممکنی سهم - با حدّ بالا و پایین معیّن- را اُستوار و ثابت می‌کند؛ برای مثال می‌توان الگوریتم سهم‌دهی پیام را آن‌گونه به‌کار گرفت که همیشه یک «بردار سهم» با «n» سهم بیرون دهد؛ اگرچه -بسته به کاربرد- می‌تواند «t» سهم نیز بیرون دهد چنان که $2 \leq t \leq n$ برقرار باشد.

۴-۲-۵ ساختار دسترسی[1]

عملیات اُلگوی تسهیم راز به طرزی بنیادین به ساختار دسترسی‌اش بستگی دارد. ساختار دسترسی کمینه مجموعهِ زیرمجموعه‌های امکان‌پذیرِ سهم‌ها است که نقشِ «ورودی» الگوریتم بازسازی پیام را بپذیرد تا الگوریتم یادشده بتواند پیام را به گونه‌ای موفقیت‌آمیز بیرون دهد؛ به عبارتی -با فرض در دست داشتن مجموعه‌ای از سهم‌ها- الگوریتم یادشده را می‌توان در بازسازی پیام به کار گرفت، اگر و تنها اگر یک یا بیشتر زیرمجموعهٔ سهم در ساختار دسترسی خود داشته باشد.

برخی اُلگوها، آستانهٔ پیوسته‌ای دارند - مار سهم‌های صحیح که برای باید برای الگوریتم بازسازی پیام فراهم کرد تا به گونه‌ای موفقیت‌آمیز پیام را بازسازی کند. برای نمونه: اگر اُلگوی تسهیم راز از آستانه‌های پیوسته-اش پشتیبانی کند، می‌توان آن‌را چنان به‌کار گرفت که پیام را به n سهم با آستانهٔ k تسهیم کند، چنان که: $2 \leq k \leq n$. در چنین زمینه‌ای، هر سهم k برای تکمیل موفّق الگوریتم بازسازی پیام کافی است. به‌عبارتی، هر یک ساختار دسترسی متشکل از همه زیرمجموعه‌های سهم‌های k و به عبارت دیگر یا همه زیرمجموعه‌هایی هستند که شُمار k عضو دارند.

همچنین «اُلگو» می‌تواند با یک ساختار دسترسی سفارشی، شامل مجموعه‌هایی از طرفین که قادر به بازسازی پیام با ترکیب سهم‌های آن‌ها هستند، به‌کار گرفته شود. برای مثال، برای چهار سهم-دارنده، یک ساختار دسترسی می‌تواند حکم کند که سهم‌های m_1، m_2، m_3، و یا m_1 و m_4 و یا m_2 و m_4 به تنهایی برای بازسازی پیام کافی هستند، که این حکم ساختار دسترسی زیر را نتیجه می‌دهد:

A={{1,2,3},{1,4},{2,4}}

1- Access structure

در این حالت، طرفین ۳ و ۴ یا ۱ و ۲ برای مثال، قادر به بازسازی پیام نیستند، اما کلیه مجموعه‌های طرفین بیان شده در A، هچنین مجموعه‌های مرجع آن‌ها، قادرند پیام را بازسازی کنند. برای این مثال، ساختار متخاصم عبارت است از:

D={{1,2},{1,3},{2,3},{3,4}}

۳-۴ فرایند تسهیم پیام

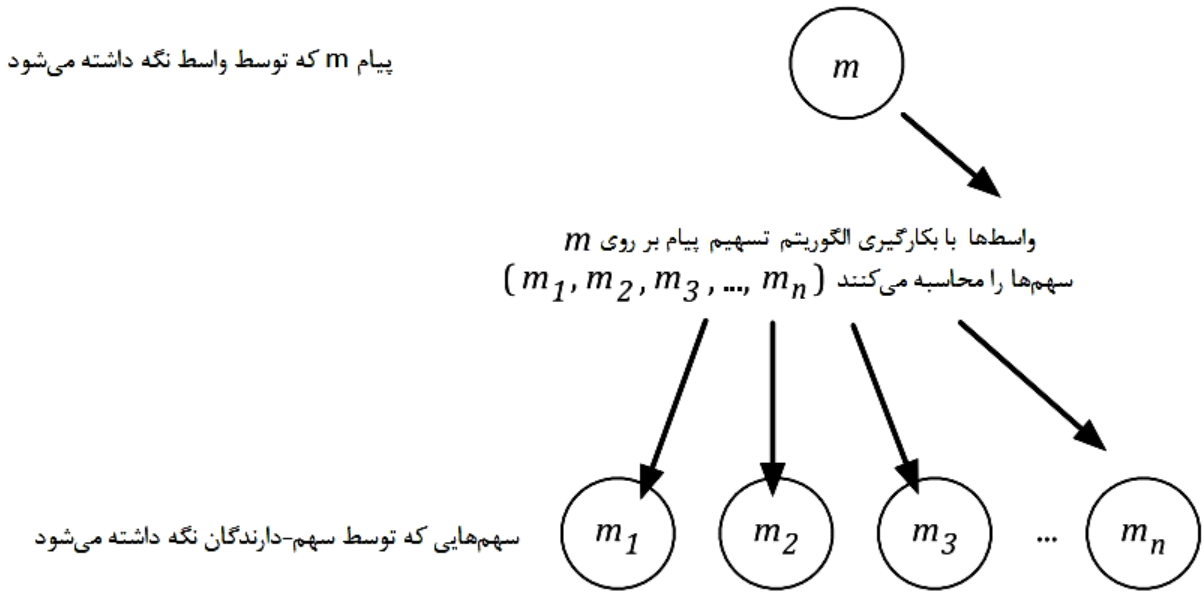
فرایند تسهیم پیام از سه گام زیر تشکیل می‌شود:

الف- واسط با اجرای الگوریتم تسهیم پیام روی پیام، بردارِ سهم ($m_1,m_2,\ldots,m_n$) را تولید می‌کند؛

ب- واسط اجزاء بردارِ سهم را میان سهم-دارندگان توزیع می‌کند؛

پ- سهم-دارندگان، سهم‌ها را به‌صورت امن نگهداری می‌کنند.

شکل ۱ مثالی از فرایند تسهیم پیام را نشان می‌دهد.



شکل ۱- نمونه‌ای از فرایند تسهیم راز

طراح تسهیم راز بهتر است پس از توزیع سهم‌ها، نسخه‌ای از سهم‌های نزد واسط را پاک کند، مگر این‌که نوع خاص کاربرد الگو، این عمل را منع کرده باشد.

۴-۴ فرایند بازسازی پیام

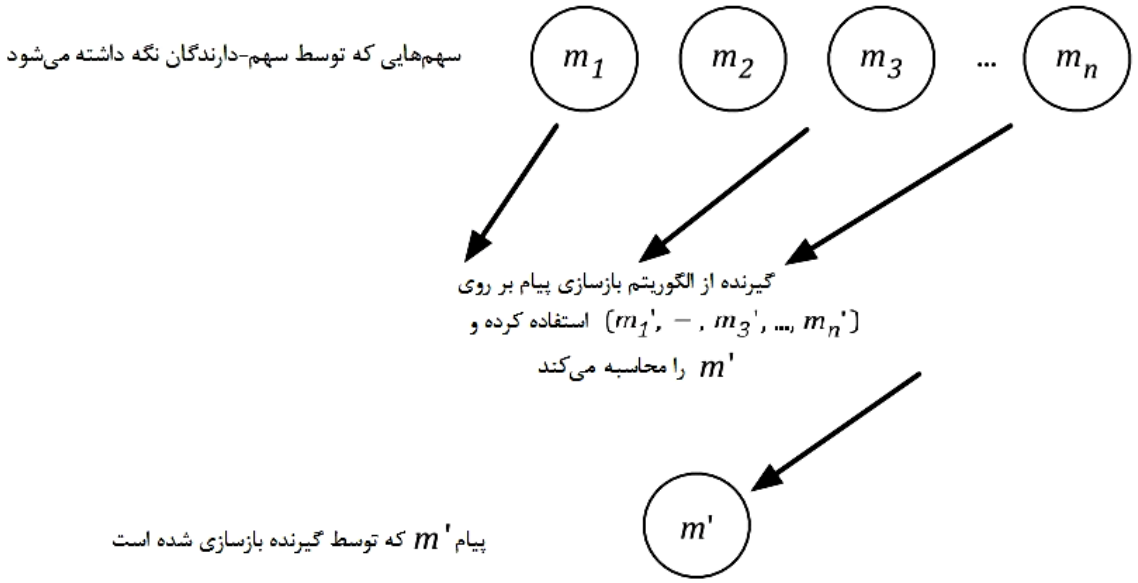
فرایند بازسازی پیام از سه مرحله زیر تشکیل می‌شود:

الف- زیرمجموعه‌ای از سهم-دارندگان راز، سهم خود از پیام m را به گیرنده می‌فرستند؛

ب- گیرنده به‌منظور آموختن پیام، الگوریتم بازسازی پیام را بر روی این سهم‌ها اجرا می‌کند. اگر همه سهم‌های دریافت شده صحیح باشند الگوریتم با موفقیت اجرا می‌شود و گیرنده m' که شکل بازسازی شده پیام m است، را به‌دست می‌آورد. در صورتی که الگوریتم با موفقیت اجرا نشود، گیرنده قادر به بازسازی هیچ بخشی از پیام نخواهد بود و تنها ممکن است طول پیام را به‌دست آورد.

شکل ۲ مثالی از فرایند بازسازی پیام را نشان می‌دهد. در این مثال، گیرنده مقدار m_2' که شکل بازسازی شده m_2 است را دریافت نخواهد کرد. در این مثال فرض شده است که تسهیم راز مورد استفاده، برای بازسازی m نیازی به m_2' ندارد.

یادآوری- در عمل، یک دارنده سهم بدخواه ممکن است به قصد ایجاد اختلال در فرایند بازسازی پیام، مقدار m_i' که برابر با m_i نیست را ارسال نماید. برخی طرح‌واره‌های تسهیم پیام محرمانه قادرند این سهم‌های نادرست را کشف و شناسایی نمایند.



شکل ۲- مثالی از فرایند بازسازی پیام

۵ ویژگی‌های الگوهای تسهیم راز

۵-۱ الزامات بنیادین

۵-۱-۱ بررسی گذرا

دو اصلی که باید در کلیه اُلگوهای تسهیم راز -مطابق با مجموعه استاندارد ISO/IEC 19592 (همه قسمت‌ها)- رعایت شوند، عبارتند از: محرمانگی پیام و قابلیت بازیابی پیام. محرمانگی پیام، از محرمانه ماندن پیام تسهیم‌شده اطمینان حاصل می‌کند و قابلیت بازیابی پیام از در دسترس بودن پیام توسط فرستنده و گیرنده مطمئن می‌شود.

۵-۱-۲ محرمانگی پیام[1]

محرمانگی پیام برای اُلگوی تسهیم پیام بدان معناست که اگر مجموعه‌ای از سهم-دارندگان، زیرمجموعه‌ای از سهم‌ها را که برای بازسازی پیام کافی نیستند، در اختیار داشته باشند، آنگاه این مجموعه از سهم‌دارندگان نخواهند توانست هیچ بخشی را از پیام -مگر در ازای پیام- بازسازی کنند.

یادآوری- برای مثال، کاربری را در نظر بگیرید که با استفاده از اُلگوی تسهیم راز، پروندهٔ محرمانه‌ای را به چندین بخش تقسیم کرده، هر بخش را روی سرور جداگانه‌ای بارگذاری اُلگوی تسهیم به‌کار گرفته شده از سوی کاربر تضمین می‌کند که برای بازسازی این فایل پروندهٔ محرمانه، به کلیه قسمت‌های آن نیاز است. این بدان معناست که برای بازسازی پیام به همگی سرورها نیاز است و هیچ مجموعه ناکاملی از سرورها قادر نخواهند بود هیچ بخشی از پرونده را با استفاده از سهم‌هایی که در اختیار دارند، بازسازی نمایند.

۵-۱-۳ قابل بازیابی بودن پیام[2]

قابل بازیابی بودن پیام برای اُلگوی تسهیم پیام بدان معناست که اگر مجموعه‌ای از سهم-دارندگان، زیرمجموعه‌ای از سهم دارند که برای بازسازی پیام کافی‌اند و می‌توانند با اجرای الگوریتم بازیابی پیام روی این سهم‌ها، پیام اصلی را بازسازی نمایند.

یادآوری- برای مثال سازمانی را در نظر بگیرید که از یک کلید خصوصی[3] حفاظت می‌کند و از آن برای ساخت امضا[4] -با استفاده از اُلگوی تسهیم پیام- استفاده می‌کند؛ اُلگوی یادشده به‌گونه‌ای مقداردهی شده است که به رئیس سازمان اجازه می‌دهد تا تنها با استفاده از سهم‌هایی که دارد، کلید خصوصی را بسازد. افزون بر این، به دو تن از جانشینان روسای سازمان برای ساخت کلید خصوصی و تولید امضای معتبر نیاز است. در این حالت، رئیس سازمان به تنهایی و هر دو جانشین او به‌عنوان افراد تائید شده در نظر گرفته می‌شوند.

۵-۲ الزامات اختیاری

۵-۲-۱ بررسی گذرا

جدا از الزامات اساسی بالا، اُلگوهای تسهیم پیام می‌توانند خصوصیات دیگری را مرتبط با پارامترها و فرآیندهای آن‌ها دارا باشند. نمونه‌ای از این خصوصیات را در زیربندهای ۵-۲-۲ و ۵-۲-۳ می‌توان دید.

۵-۲-۲ همریختی[5]

اُلگوی تسهیم پیام می‌تواند از یک یا چند عملیات همریخت روی مجموعه سهم‌های ممکن پشتیبانی نماید. در اصل عملیات‌های همریخت، به بردارهای سهم امکان می‌دهند که با یکدیگر ترکیب شوند و بردار سهم

1- Message confidentiality
2- Message recoverability
3- Private key
4- Signature
5- Homomorphicity

تازه‌ای شکل دهند به‌گونه‌ای که بردار سهم تازه نتیجه عملیات معنی‌داری روی پیام و/یا پیام‌های اصلی را ارائه می‌دهد.

اُلگوی تسهیم متشکل از n طرف را در نظر بگیرید که دارای گسترهٔ پیام: M، گسترهٔ تسهیم: S الگوریتم تسهیم پیام «*Share*» و الگوریتم بازسازی پیام «*Reconstruct*» است. سپس فرض کنید که $\oplus$ عملیات تعریف شده روی M و $\otimes$ عملیات تعریف شده روی بردارهای سهم مجموعه S_n باشد. «اُلگوی تسهیم پیام» $(\oplus,\otimes)$-همریخت، خواهد بود اگر برای همه پیام‌های $m_1, m_2 \in M$ معادلهٔ زیر برقرار بماند:

$$Reconstruct\ [Share\ (m_1) \otimes Share\ (m_2)] = m_1 \oplus m_2$$

چنین عملیات‌های همریختی برای کاربردهایی همچون محاسبات امن، که در آن یک دستگاه باید یک سری عملیات محاسباتی را روی داده‌ها بدون داشتن مقدار آن‌ها به‌صورت شفاف انجام دهد، مفید خواهد بود.

۵-۲-۳ تصدیق‌پذیری[1]

اگر سهم‌ها خروجی حاصل از اجرای الگوریتم تسهیم پیام، شامل اطلاعات کمکی باشند که به سهم-دارندگان، امکان اثبات صحت سهم‌ها، یعنی: قابل استفاده بودن این سهم‌ها برای بازسازی پیام) را بدهند، اُلگوی تسهیم راز، قابل راستی‌آزمایی است. پیش از بازسازی پیام، هر یک از سهم-دارندگان و یا گیرنده می‌توانند با استفاده از این اطلاعات از صحت سهم‌ها اطمینان حاصل نمایند. روش دیگری که می‌توان از آن برای اثبات صحت یک سهم استفاده کرد، افزودن اطلاعات کمکی به سهم‌ها است که از آن‌ها برای اثبات صحت پیام بازسازی شده (و نه اثبات صحت سهم‌ها) استفاده می‌شود.

۵-۳ ویژگی‌های دیگر

۵-۳-۱ بررسی گذرا

ویژگی‌ها مختلف عملیاتی و امنیتی اُلگوی تسهیم راز را می‌توان با استفاده از موارد بیان شده در زیربندهای ۵-۳-۲ و ۵-۳-۴ اندازه‌گیری کرد.

۵-۳-۲ تضمین‌های محرمانگی[2]

ویژگی محرمانگی پیام اُلگوی تسهیم راز می‌تواند بر اساس فرضیه‌های گوناگونی باشد. برای مثال اُلگوی تسهیم راز از نظر تئوری اطلاعات[3]محرمانه خواهد بو،د اگر محرمانگی پیام را صرف‌نظر از قدرت محاسبه ائتلاف سهم-دارندگان غیرمجاز که می‌کوشند به پیام اصلی دست یابند، حفظ نماید. به‌طور مشابه اُلگوی

1- Verifiability
2- Confidentiality guarantees
3- Informational theory

تسهیم راز از نظر محاسباتی محرمانه خواهد بود اگر محرمانگی آن در برابر طرفین تأیید نشده، با قدرت محاسباتی محدود، تضمین شده باشد.

علاوه بر این، چندین سطح محرمانگی در تئوری اطلاعات تمایزپذیرند. اگر هیچ‌گونه اطلاعاتی دربارهٔ پیام مطلقاً افشاء نشود، محرمانگی کامل است. با این وجود، اُلگوی تسهیم محرمانه اطلاعات ممکن است محرمانگی کمتری را فراهم آورد؛ بدین معنا که ائتلافِ گروه‌های غیرمجاز بتواند تعداد غیر صفری از بیت‌های پیام با ترکیب سهم‌های خود با یکدیگر به شیوه مشخصی باشند.

۵-۳-۳ پیچیدگی[1]

پیچیدگی یک الگوریتم در اُلگوی تسهیم راز، عبارت است از تعداد واحدهای عملیاتی مورد نیاز برای اجرای آن الگوریتم. پیچیدگی الگوریتم را جداگانه برای هر الگوریتم مرتبط با اُلگوی سهم تعیین می‌شود.

۵-۳-۴ نرخ اطلاعات[2]

نرخ اطلاعات، یک ویژگی از اُلگوی تسهیم راز است که بیانگر نسبت اندازه پیام به حداکثر اندازه سهم برای آن پیام است. اگر پیام و سهم به یک اندازه باشند، نرخ اطلاعات برابر با ۱ خواهد بود و اُلگوی تسهیم راز ایده‌ال خوانده می‌شود.

اُلگوهای امنِ محاسباتی تسهیم راز، برای نمونه: اُلگوهای گوناگون رمپ هستند که نرخ اطلاعات آن‌ها بزرگتر از ۱ است. زیرا اندازه پیام بزرگتر از هر یک از تسهیم‌ها به تنهایی است.

1- Complexity
2- Information rate