



انجمن رمز ایران
Iranian Society of Cryptology

مجموعه واژه‌های مصوب

گروه واژه‌گزینی انجمن رمز ایران

(کارگروه واژه‌گزینی رمزشناسی فرهنگستان)

در فرهنگستان زبان و ادب فارسی

شهریورماه ۱۴۰۲

فرهنگستان زبان و ادب فارسی

به نام خدا

پیش گفتار

یکی از فعالیت‌های مهم و اثرگذار انجمن رمز ایران، تشکیل کارگروه واژه‌گزینی به منظور معادل‌یابی فارسی برای واژه‌های انگلیسی مطرح در متون علمی حوزه رمزشناسی و افتا بوده‌است. تدوین و انتشار ویرایش اول «واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات (افتا)» در سال ۱۳۹۰ و ویرایش دوم آن در سال ۱۳۹۴ از جمله فعالیت‌های این کارگروه بوده که فعالیت خود را از سال ۱۳۸۷ آغاز کرده‌است. علاوه بر این، از سال ۱۳۸۹، بر مبنای تفاهم‌نامه همکاری با فرهنگستان زبان و ادب فارسی، کارگروه رمزشناسی در این فرهنگستان تشکیل شد و بر طبق اصول و ضوابط فرهنگستان، کار واژه‌گزینی حوزه رمزشناسی و افتا به صورت مستمر ادامه یافت. تلاش‌های این کارگروه تاکنون به تصویب حدود ۶۰۰ واژه از سوی فرهنگستان زبان و ادب فارسی انجامیده است که در دفاتر مختلف «فرهنگ واژه‌های مصوب فرهنگستان» منتشر شده‌اند.

بر خود لازم می‌دانم از اعضای محترم کارگروه، سرکار خانم دکتر ترانه اقلیدس، آقایان مهندس حبیب رستمی، دکترهادی شهریار شاه‌حسینی، دکترجواد شیخ‌زادگان، سرکار خانم سمانه ملک‌خانی، نماینده محترم فرهنگستان، سرکار خانم دکتر مهشید دلاور، عضو سابق کارگروه، آقای محمدرضا حسینی نماینده قبلی فرهنگستان و نیز آقایان دکتر محمدرضا عارف، دکتر محمود سلماسی‌زاده و دکتر رسول جلیلی، رؤسای محترم فعلی و پیشین انجمن رمز ایران، آقای دکتر غلامعلی حداد عادل، ریاست محترم فرهنگستان زبان و ادب فارسی، سرکار خانم دکتر نسرين پرویزی، معاون محترم گروه واژه‌گزینی فرهنگستان و مجموعه مدیران و کارشناسان انجمن رمز ایران و فرهنگستان زبان و ادب فارسی که با حمایت و پشتیبانی خود، انجام و استمرار این فعالیت و تهیه این مجموعه ارزشمند را ممکن ساختند، صمیمانه سپاس‌گزاری نمایم. اینک با توجه به درخواست استادان، دانشجویان، پژوهشگران و فعالان حوزه افتا نسخه اولیه مجموعه واژه‌های مصوب این کارگروه در اختیار عموم علاقه‌مندان قرار می‌گیرد. نسخه نهایی پس از بازبینی و ویرایش مجدد در آینده نزدیک، چاپ و منتشر خواهد شد.

در پایان از کلیه صاحب‌نظران گرامی تقاضا می‌شود، دیدگاه‌های ارزشمند اصلاحی خود را به دبیرخانه انجمن منعکس نمایند تا در ادامه کار مورد استفاده قرار گیرد.

جواد مهاجری

شهریور ۱۴۰۲

واژه‌های مصوب

واژه بیگانه	معادل فارسی	تعریف
A		
access control	واپایش دسترسی	فرایندی امنیتی که در آن از منابع مشترک در برابر دسترسی غیرمجاز محافظت می‌شود
accountability	بی‌گیری پذیری	امکان ردگیری منحصر به فرد فعالیت‌های یک هستار
accreditation authority syn. authorizing official	مقام مجازشناسی	مأموری رسمی با اختیارات قانونی، برای تعیین سطح پذیرفتنی از مخاطراتی که ممکن است متوجه سرمایه یا کارکنان یا عملیات در یک سامانه اطلاعاتی باشد.
active adversary	مهاجم فعال	مهاجمی که علاوه بر شنود اطلاعات طرفین پروتکل، امکان تخطی از اجرای درست پروتکل را نیز داراست
active cheater	فریب‌دهنده فعال	هستاری که به منظور فریبکاری، یک پروتکل در حال اجرا را مختل می‌کند
active cryptanalysis	تحلیل رمز فعال	نوعی تحلیل رمز مبتنی بر تغییر پیام ارسالی یا ارسال مجدد آن یا حتی وارد کردن پیام‌های جدید موردنظر تحلیل‌گر
active eavesdropper	شنودگر فعال	شنودگری که علاوه بر شنود می‌تواند فعالیت‌هایی نظیر جایگزینی متن رمز شده یا بازارسال (retransmit) آن در هر زمان دیگر یا وارد کردن متن جدید را انجام دهد
active penetration test	آزمون نفوذ فعال	

واژه بیگانه	معادل فارسی	تعریف
		آزمونی برای کاوش مرزهای محدوده هدف و بررسی ضعف‌های امنیتی در محیط هدف، شامل آزمون‌های دارای عمق نفوذ بیشتر در قیاس با آزمون‌های نفوذ غیرفعال، با بهره‌گیری از ضعف‌های امنیتی ذاتی موجود در فناوری محیط هدف، خطاهای طراحی یا ضعف‌های موجود در پیکربندی
active wiretapping	خط‌شوند فعال	نوعی شنود خط برای تغییر داده‌های در حال مبادله با تأثیر بر جریان آن‌ها
adaptive adversary syn. dynamic adversary	مهاجم وقتی مت: مهاجم پویا	مهاجمی که در طول اجرای یک پروتکل تصمیم می‌گیرد که کدامیک از نهادهای شرکت کننده در پروتکل را به عنوان نهاد تسخیر شده انتخاب کند
adaptive chosen ciphertext attack	حمله با متن رمز منتخب وقتی	نوعی حمله با متن رمز منتخب که در آن مهاجم قادر است ورودی به تابع رمزبندی را براساس متن‌های رمز منتخب پیشین انتخاب کند
adaptive chosen message attack	حمله با پیام منتخب وقتی	نوعی حمله به طرح‌های امضا که در آن مهاجم به کمک امضاهای دریافتی بر روی تعدادی پیام منتخب اقدام به جعل امضا بر روی پیام مورد نظر کند
adaptive chosen plaintext attack	حمله با متن اصلی منتخب وقتی	نوعی حمله با متن اصلی منتخب که در آن مهاجم قادر است ورودی به تابع رمزگذاری را براساس متن‌های اصلی منتخب پیشین و متن‌های رمز متناظر با آنها انتخاب کند
adversarial attack	حمله خصمانه	حمله‌ای که از طریق فضای تولید و تبادل اطلاعات صورت می‌گیرد و اهدافی مانند فروپاشیدن، ناکارآمدسازی، تخریب یا واپایش بدخواهانه یک محیط/ زیرساخت محاسباتی یا تخریب درستی داده‌ها یا سرقت اطلاعات مورد واپایش را دنبال می‌کند

واژه بیگانه	معادل فارسی	تعریف
algebraic attack syn. algebraic cryptanalysis	حمله جبری مت: تحلیل رمز جبری	حمله‌ای که بر پایه حل معادلات جبری مستخرج از سامانه رمز انجام می‌شود
algebraic cryptanalysis syn. algebraic attack	تحلیل رمز جبری مت: حمله جبری	حمله‌ای که بر پایه حل معادلات جبری مستخرج از سامانه رمز انجام می‌شود
algebraic immunity degree	درجه ایمنی جبری	به ازای یک تابع بولی f برابر است با حداقل درجه جبری توابع پوچ ساز f یا $1 + f$ که به صورت زیر بیان می‌شود:
all-or-nothing disclosure of secret	افشای راز همه یا هیچ	نوعی طرح افشای راز که در آن کاربری، که تعدادی راز در اختیار دارد، مایل است یکی از آنها را برای کاربر دوم افشا کند بدون آنکه به او اجازه دهد در مورد بیش از یک راز اطلاعاتی کسب کند؛ از طرف دیگر کاربر دوم نیز مایل نیست که کاربر اول آگاه شود که وی مایل به دریافت کدام یک از رازهاست؛ در این طرح افشا به محض دریافت اطلاعات توسط کاربر دوم وی فرصت خود را برای کسب هرگونه اطلاعاتی درباره سایر رازها از دست خواهد داد
all-or-nothing encryption	رمزگذاری همه یا هیچ	نوعی رمزگذاری که در آن رمزگشایی بخشی از پیام بدون رمزگشایی کل آن ممکن نیست
almost-perfect zero-knowledge syn.: statistical zero-knowledge proof	اثبات ناتراوای تقریباً کامل، اثبات دانش صفر تقریباً کامل مت. اثبات ناتراوای آماری، اثبات دانش صفر آماری	اثباتی که در آن، برخلاف حالت‌های کلی اثبات ناتراوا، توزیع مکالمات واقعی با توزیع مکالمات شبیه‌سازی شده از نظر آماری تمایزناپذیر است؛ یعنی فاصله آماری میان توزیع‌ها ناچیز است
anonymity	گمنامی	غیرقابل تشخیص بودن از سایر هستارها در یک ویژگی مشخص
anonymizer	گمنام‌ساز	ابزاری که ردگیری فعالیت‌ها را در اینترنت ناممکن می‌سازد
arbiter PUF	تابع فیزیکی تکثیرناپذیر انتخاب‌گر /	

تفت انتخاب‌گر

نوعی تابع فیزیکی تکثیرناپذیر که بر اساس تفاوت ذاتی زمان‌بندی دو مسیر متقارن منتهی به یک بیت خروجی مدار عمل می‌کند

asymmetric cryptography
syn. public-key cryptography

رمزنگاری نامتقارن
مت. رمزنگاری با کلید عمومی

روش برای رمزگذاری پیام که در آن از کلید عمومی و کلید مخفی استفاده می‌شود: کلید عمومی برای رمزگذاری و کلید مخفی برای رمزگشایی

asymmetric watermarking
syn.: public-key watermarking

ته‌نقش‌گذاری نامتقارن
مت. ته‌نقش‌گذاری کلید عمومی

نوعی روش ته‌نقش‌گذاری که در آن فرستنده ته‌نقش را با استفاده از کلید خصوصی (مشابه تولید امضای دیجیتال) ایجاد می‌کند و هر هستار کدگشا که به کلید عمومی متناظر دسترسی داشته باشد می‌تواند ته‌نقش مربوط را آشکار و بازشناسی کند

asymptotic security

امنیت مجانبی

نوعی امنیت برای یک طرح رمزنگاشتی که در آن احتمال موفقیت هر مهاجم زمان‌چندجمله‌ای احتمالاتی برای شکستن طرح در بهترین حالت ناچیز باشد؛ مجانبی بودن امنیت به دلیل وابستگی امنیت به رفتار طرح برای مقادیری از پارامتر امنیتی است که به اندازه کافی، متناظر با طول کلید، بزرگ باشند

atomicity

تفکیک‌ناپذیری

syn. atomicity property

مت. ویژگی تفکیک‌ناپذیری

یکی از ویژگی‌های پرداخت‌های الکترونیکی که به کاربر امکان می‌دهد چند عمل را به صورت منطقی به یکدیگر چنان مرتبط سازد که یا همه آن عملیات اجرا شود یا هیچ‌یک از آنها اجرا نشود

atomicity property
syn. atomicity

ویژگی تفکیک‌ناپذیری

مت: تفکیک‌ناپذیری

یکی از ویژگی‌های پرداخت‌های الکترونیکی که به کاربر امکان می‌دهد چند عمل را به صورت منطقی به یکدیگر چنان مرتبط سازد که یا همه آن عملیات اجرا شود یا هیچ‌یک از آنها اجرا نشود

attribute certificate

گواهی ویژگی

گواهی رقمی‌ای برای تأیید ویژگی‌های مشخص یک کاربر که توسط یک نهاد ثالث رسمی مورداعتماد امضا شده است

attribute-based access control

واپایش دسترسی ویژگی‌بنیاد

واپایش دسترسی‌ای که براساس ویژگی‌های کاربر انجام می‌شود

واژه بیگانه	معادل فارسی	تعریف
attribute-based authorization	مجازشناسی ویژگی‌بنیاد	فرایندی ساختاریافته که بر مبنای ویژگی‌های کاربران و داده‌ها و سامانه‌ها و خدمات، چگونگی دسترسی یک کاربر به داده‌ها و سامانه‌ها و خدمات را تعیین می‌کند
attribute-based encryption	رمزگذاری ویژگی‌بنیاد	نوعی رمزگذاری با این هدف که تنها افرادی که حائز شرایط یا ویژگی‌های خاصی هستند، قادر به رمزگشایی متن رمز باشند
attributes authority	مرجع تأیید ویژگی	هستاری رسمی با اختیار و ارسی ویژگی‌های متناسب به یک هویت
attributes management	مدیریت ویژگی‌ها	زیرمجموعه مدیریت داده‌های مجازشناسی (management authorization data) که بر مبنای آن ویژگی‌ها متناظر با هستارهای موجود در یک محیط هستند
audio steganography	نهان‌نگاری صوتی	جا دادن پیغام محرمانه در نشانه‌های صوتی رقمی
auditability	ممیزی‌پذیری	امکان بازدید مستقیم از فعالیت‌های یک سامانه برای پایش سامانه و تشخیص تخطی‌های امنیتی به منظور ارائه پیشنهاد در اصلاح نظارت‌ها و روندها و سیاست‌ها
authenticated encryption (AE)	رمزگذاری احراز اصالت شده مت. رمزگذاری اصالت‌سنجی شده	راهکاری جدید برای تأمین همزمان محرمانگی و احراز اصالت که در مقایسه با راهکار گذشته، که حاصل ترکیب مستقیم روش‌های رمزگذاری و احراز اصالت بود، بسیار سریع‌تر و کارا تر است.
authenticated encryption with associated data (AEAD)	رمزگذاری احراز اصالت شده با داده‌های همراه مت. رمزگذاری اصالت‌سنجی شده با داده‌های همراه	رمزگذاری احراز اصالت شده با داده‌های همراه

واژه بیگانه	معادل فارسی	تعریف
		نوعی طرح رمزگذاری احراز اصالت شده که در آن داده‌های کمکی، بدون رمزگذاری، احراز اصالت می‌شوند
authenticated key exchange	تبادل کلید احراز اصالت شده مت. تبادل کلید اصالت‌سنجی شده	
		نوعی طرح رمزنگاشتی دونهادی که در آن طرفین ارتباط، در ضمن احراز اصالت یکدیگر، یک کلید مخفی را محاسبه می‌کنند و به اشتراک می‌گذارند
authentication	احراز اصالت مت. اصالت‌سنجی	
		اقدامی امنیتی شامل واریسی شناسه و تعیین اعتبار مبدأ و منشأ و محتوای پیام
authentication authority	مرجع احراز اصالت مت. مرجع اصالت‌سنجی	
		نهادی که تسهیلات لازم برای احراز اصالت یک هستار را از طریق تأمین شواهد و مستندات لازم یا ارائه سازوکارهای احراز اصالت فراهم می‌کند
authentication mode	شیوه احراز اصالت مت. شیوه اصالت‌سنجی	
		روشی برای بکارگیری رمز قالبی که به اطمینان از اصالت و یکپارچگی داده‌ها منجر می‌شود
authentication period	دوره احراز اصالت مت. دوره اصالت‌سنجی	
		بیشینه‌زمان قابل قبول بین فرایند احراز اصالت اولیه و فرایندهای احراز اصالت بعدی، در طی زمان یک نشست واحد یا در طی زمانی که دسترسی به داده‌ها امکان‌پذیر است
authentication provider	نشان‌بخش اصالت	
		نهادی که مسئولیت احراز اصالت اولیه یک هستار و تخصیص یک نمودافزار را، که نشان‌دهنده انجام احراز اصالت اولیه است، بر عهده دارد
authentication tag	برچسب احراز اصالت مت. برچسب اصالت‌سنجی	
		رشته‌ای از بیت‌های متناظر با یک داده، برای تضمین اصالت آن داده
authenticator	اصالت‌نشان	
		ابزاری برای تأیید هویت یک کاربر یا فرایند یا افزاره

واژه بیگانه	معادل فارسی	تعریف
authenticity	اصالت	اصیل بودن و برخورداری از قابلیت واریسی پذیری و اعتماد که نتیجه آن اطمینان از درستی یک پیام و مبدأ پیام و انتقال آن است
authorization	مجازشناسی	تصمیمی مدیریتی و رسمی از سوی یک مدیر ارشد سازمان، برای مجاز کردن عملیات یک سامانه اطلاعاتی و پذیرش صریح مخاطرات آن، در مورد عملیات و دارایی‌های سازمان یا افراد، براساس مجموعه‌ای از واپایش‌های امنیتی توافق شده
authorization algebra	جبر مجازشناسی	مجموعه‌ای از قواعد و روال‌های مورد استفاده در زیرساخت‌های ساده‌شده کلید عمومی که امکان صدور مجوز و واپایش دسترسی را فراهم می‌سازند
authorization architecture	معماری مجازشناسی	مجموعه‌ای از مؤلفه‌ها و داده‌ها که اخذ و اجرای تصمیمات مجازشناسی را ممکن می‌سازد
authorization boundary	محدوده مجازشناسی	همه مؤلفه‌های یک سامانه اطلاعاتی که یک مقام مجازشناسی می‌تواند آنها را مجاز سازد، بی‌آن که سایر سامانه‌های مجاز متصل به آن را در برگیرند
authorization management	مدیریت مجازشناسی	مدیریت تخصیص مجوز به افراد یا هستارها برای انجام یک کار یا اداره یک سازمان مشخص
authorization policy	خط‌مشی مجازشناسی	خط‌مشی‌ای مرتبط با داده‌های مجازشناسی برای اتخاذ تصمیم‌های مجازشناسی که توسط یک مرجع تصمیم‌گیری ارائه می‌شود
authorizer	مجازشناس	هستاری که خط‌مشی مرجع مجازشناسی را تعیین می‌کند
authorizing official syn. accreditation authority	مقام مجازشناسی	

واژه بیگانه	معادل فارسی	تعریف
		مأموری رسمی با اختیارات قانونی، برای تعیین سطح پذیرفتنی از مخاطراتی که ممکن است متوجه سرمایه یا کارکنان یا عملیات در یک سامانه اطلاعاتی باشد
auto-key	خود کلید	نوعی کلید که با استفاده از متن اصلی به دست می آید
auto-key cipher	رمز خود کلید	رمزی که در آن از متن اصلی یا دنباله کلید اجرایی برای تولید کلید استفاده می کنند
avalanche criterion	معیار بهمنی	معیاری برای ارزیابی رمزهای قالبی که براساس آن لازم است با تغییر یک بیت ورودی به خوارزمی / الگوریتم رمز به طور متوسط نیمی از بیت های خروجی آن تغییر کند
avalanche effect	اثر بهمنی	اثری که در آن با تغییر یک بیت در کلید یا در متن اصلی تغییر فاحشی در متن رمز ایجاد شود
B		
backward secrecy	رازمانی پس سو	خصوصیتی که بنا بر آن لو رفتن کلید نشست های پیشین باعث نمی شود که امنیت نشست کنونی به خطر بیفتد
balance property	ویژگی توازن	برابری شمار صفرها و یک ها در یک دوره تناوب از یک دنباله دودویی متناهی به طول بیشینه
bi-deniable encryption	رمز گذاری دوسوانکارپذیر	نوعی رمز گذاری که در آن هر دو طرف ارتباط، یعنی فرستنده و گیرنده، قادر به انکار پیام دریافتی خود باشند
bigram syn. digraph	دونویسه	یک زوج مرتب متشکل از حروف (نویسه ها) در متن رمز
bilinear Diffie-Hellman problem	مسئله دیفی - هلمن دوخطی	مسئله محاسبه $\hat{e}(p, p)^{abc}$ با در اختیار داشتن چهارتایی (p, ap, bp, cp) و با این فرض که G_1 و G_2 دو گروه دوری از مرتبه عدد اول q و \hat{e} یک نگاشت دو خطی از $G_1 \times G_2$ به G_1 مولدی برای G_1 باشد

واژه بیگانه	معادل فارسی	تعریف
binding	تراست	۱ فرایند ایجاد تناظر بین دو عنصر اطلاعاتی مرتبط. ۲. تأیید ارتباط شناسه یک هستار با کلید عمومی آن توسط یک نهاد مورد اعتماد
bipartite substitution syn. digraphic substitution	جانیشینی دوبخشی	نوعی جانیشینی که در آن از دونگاشت‌ها برای جایگزینی دونویسه‌ها (زوج‌های مرتب از نویسه‌های متن اصلی استفاده می‌شود
birthday attack	حمله روز تولد	حمله‌ای مبتنی بر ناسازنمای روز تولد که به یافتن برخورد برای توابع چکیده‌ساز منجر می‌شود
birthday paradox syn. birthday problem	ناسازنمای روز تولد مت. مسئله روز تولد	گزاره‌ای که بنا بر آن به احتمال بیش از ۵۰ درصد می‌توان دست کم ۲ فرد در یک جمع حداقل ۲۳ نفری تصادفی یافت که دارای سالروز تولد یکسان باشند؛ این ناسازنمایی ناشی از این واقعیت است که ۲۳ بسیار کوچکتر از ۳۶۵ روز سال است
bit commitment scheme	طرح تعهد بیتی	نوعی طرح تعهد که در آن X تنها از یک بیت تشکیل می‌شود
bit independence criterion	معیار استقلال بیتی	معیاری که به موجب آن، تغییر هر بیت ورودی در توابع بولی به تغییر هر دو بیت خروجی دلخواه، به‌طور مستقل از یکدیگر، منجر می‌شود
blind proxy signature	امضای وکالتی کور	امضایی که در آن امضاکننده اصلی نمی‌تواند امضاکننده وکالتی را تنها با استفاده از امضای وکالتی شناسایی کند
blind signature	امضای کور	نوعی امضای رقمی که در آن امضاکننده بدون اطلاع از محتوای پیام اقدام به امضای آن می‌کند
blind watermarking	ته‌نقش گذاری کور	

واژه بیگانه	معادل فارسی	تعریف
		نوعی ته‌نقش‌گذاری که در آن آشکارسازی ته‌نقش می‌تواند بدون نیاز به نشانک پوششی (cover signal) انجام شود
blinded message	پیام کورساخته مت. پیام کور	پیامی که فرد بدون اطلاع از محتوای آن و بنا به درخواست یک متقاضی، آن را امضا می‌کند
blinding	کورسازی	روشی در خدمات‌رسانی که در آن ارائه‌دهنده خدمات از درونداد یا برون‌داد واقعی بی‌خبر است
block	ریسه یک	یک‌های متوالی در یک دنباله دودویی که بیت پیش و پس از آن صفر باشد
branch number	عدد انشعاب	عددی که به‌عنوان معیاری برای سنجش قدرت پخش یک نگاهش به کار می‌رود
broadcast encryption	رمز‌گذاری پخش	روشی مؤثر برای پخش اطلاعات در میان یک گروه در حال تغییر، به‌صورتی که فقط افراد دارای مجوز دریافت اطلاعات، امکان رمزگشایی آن را داشته باشند
brute force attack syn. exhaustive key search	حمله غیرهوشمندانه مت. کلیدجویی فراگیر	حمله‌ای مبتنی بر آزمایش و به‌کارگیری تک‌تک کلیدها به‌منظور پیدا کردن کلید صحیح
C		
cascade cipher	رمز آبشاره‌ای	ترکیب چند خوارزمی / الگوریتم رمز
certificate authority syn. certification authority, CA	مرجع صدور گواهی	نهادی رسمی و معتبر که وظیفه صدور و مدیریت و انتشار و فسخ گواهینامه‌های کلید عمومی را بر عهده دارد
certificate revocation list	فهرست ابطال گواهی	

واژه بیگانه	معادل فارسی	تعریف
certification	صدور گواهی	فهرستی از گواهی‌های کلید عمومی که مرجع صدور گواهی، پیش از انقضا، از اعتبار ساقط کرده است روند صدور گواهی برای تأیید هر هستار
certification authority syn. certificate authority, CA	مرجع صدور گواهی	نهادی رسمی و معتبر که وظیفه صدور و مدیریت و انتشار و فسخ گواهینامه‌های کلید عمومی را بر عهده دارد
certification policy	خط‌مشی گواهی	سیاست حاکم بر همه مراحل مربوط به تولید و توزیع و حسابرسی و ابطال گواهی‌های رقمی
certification practice statement	شیوه‌نامه صدور گواهی	بیانیه‌ای که در مدیریت گواهی‌ها بر پایه آن عمل می‌شود
challenge-response authentication	اصالت‌سنجی چالش‌پاسخی	نوعی قرارداد احراز اصالت که در آن، در طی فرایند پرسش و پاسخ، هویت یک هستار احراز می‌شود
challenge-response identification	شناسایی چالش‌پاسخی	نوعی قرارداد شناسایی که در آن در طی فرایند پرسش و پاسخ یک هستار شناسایی می‌شود
cheater	فریب‌دهنده	یکی از طرفین قرارداد که در حین اجرای قرارداد دروغ می‌گوید یا از آن قرارداد پیروی نمی‌کند
chosen ciphertext attack	حمله با متن رمز منتخب	حمله‌ای (تحلیل رمز) که در آن مهاجم قادر به انتخاب متن‌های رمز و مشاهده متن‌های اصلی متناظر با آن است
chosen message attack	حمله پیام منتخب	نوعی تهاجم به صورت جعل امضا که براساس ارسال شماری پیام منتخب از سوی مهاجم و اقناع امضاکننده به امضای آنها انجام می‌شود

واژه بیگانه	معادل فارسی	تعریف
chosen plaintext attack	حمله با متن اصلی منتخب	حمله‌ای (تحلیل رمز) که در آن مهاجم توانایی انتخاب متن‌های ساده و مشاهده یا دریافت متن‌های رمزی شده متناظر را دارد
chosen related key attack	حمله کلید مرتبط منتخب	حمله‌ای به فرمانای کلید که در آن مهاجم با انتخاب رابطه بین چند کلید و دسترسی به توابع رمزگذاری متناظر در پی یافتن کلید است
chosen-key attack	حمله کلید منتخب	دسته‌ای از حمله‌ها که در آن مهاجم تنها با اطلاع از وجود رابطه‌ای بین کلیدهای مختلف و کاهش فضای جستجو، سعی در دستیابی به کلید دارد
chosen-text attack	حمله متن منتخب	حمله‌هایی مرکب از حمله‌های با متن اصلی منتخب و با متن اصلی منتخب وقتی و با متن رمز منتخب
cipher syn. encryption algorithm	رمز مت. الگوریتم/خوارزمی رمزگذاری	خوارزمی / الگوریتمی برای تبدیل متن اصلی به متن رمزی شده به نحوی که برای گیرنده غیرمجاز غیرقابل درک باشد.
cipher feedback mode	شیوه بازخورد رمز	یکی از روش‌های به کارگیری رمز قالبی که در آن از متن رمز تولید شده در یک مرحله از رمزگذاری، برای تولید متن رمز متناظر با متن اصلی بعدی استفاده می‌شود
cipher system syn. cryptosystem syn. cryptographic system	سامانه رمز مت. سامانه رمزنگاشتی	سامانه‌ای متشکل از خوارزمی‌ها / الگوریتم‌های رمزگذاری و رمزگشایی همراه با مجموعه سه گانه متن‌های اصلی و متن‌های رمزی شده و کلیدها
ciphertext/ cipher text syn. cryptogram	متن رمزی شده مت. متن رمز، رمزنگاشت	خروجی الگوریتم رمزگذاری، داده‌ی رمز شده
cipher text auto-key	خود کلید متن رمز	

واژه بیگانه	معادل فارسی	تعریف
		منطق رمزنگاشتی که در آن از متن رمز شده قبلی برای تولید یک دنباله کلید اجرایی استفاده می کنند
ciphertext-ciphertext compromise	مخاطرة کلید متن رمز - متن رمز	لو رفتن اطلاعات کلید که از تحلیل اطلاعات حاصل از رمز گذاری یک متن اصلی با دو کلید متفاوت حاصل می شود
ciphertext-only attack	حمله فقط با متن رمز	حمله ای که در آن تحلیلگر رمز به متن رمز شده شماری از پیام هایی دسترسی دارد که همگی با یک خوارزمی / الگوریتم، رمز گذاری (encryption) شده اند
ciphony 1	رمز آوا	اطلاعات صوتی رمز گذاری شده
ciphony 2	رمز آوایی	فرایند رمز گذاری اطلاعات صوتی
clear text/ cleartext syn. plaintext	متن آشکار متن ساده	متنی که اطلاعات یا محتوای آن رمز گذاری نشده و به راحتی قابل فهم است
clock-controlled generator	مولد ساعت فرما	مولدی برای تولید دنباله های دودویی که بر اساس سازوکار ساعت عمل می کند
code-based cryptography	رمزنگاری کدبنیاد	نوعی سامانه رمز پساکوانتومی که در آن اولیه رمزنگاشتی (تابع یک طرفه مینا) از یک کد تصحیح خطای C استفاده می کند؛ این اولیه ممکن است شامل اضافه کردن یک خطا به کلمه کد یا محاسبه یک نشانگان مرتبط با ماتریس توازن آزمایی (parity check matrix) کد باشد
codebook	کدنامه	مجموعه ای از زوج متن های اصلی و رمز متناظر با آنها که با استفاده از یک کلید ثابت مشترک به دست آمده اند
codebook attack	حمله کدنامه	

واژه بیگانه	معادل فارسی	تعریف
collision attack	حمله برخوردی	نوعی حمله متن اصلی معلوم که در آن حمله کننده به یک مجموعه از زوج متن های اصلی و رمز متناظر با آنها (کتاب کد) دسترسی دارد و بدون دانستن کلید مخفی از آنها برای رمزگشایی پاره ای از ارتباطات بعدی کمک می گیرد
collision free hash function	تابع چکیده ساز بی برخورد	نوعی تابع چکیده ساز یک طرفه که در آن دو پیام ورودی متفاوت، از نظر محاسباتی، خروجی یکسان نداشته باشد
collision resistance	برخوردتابی	عدم امکان یافتن دو ورودی با خروجی یکسان برای یک تابع چکیده ساز از نظر محاسباتی
commitment scheme	طرح تعهد	قراردادی که براساس آن یکی از طرفین (فرستنده) می تواند در برابر طرف مقابل (گیرنده) نسبت به مقداری مانند X متعهد شود به گونه ای که بعداً قادر به افشای آن باشد، ولی تا آن لحظه این مقدار برای گیرنده پوشیده باقی می ماند و پس از افشا، گیرنده می تواند درستی مقدار افشاشده و برابری آن را با مقداری که نسبت به آن تعهد داده شده واریسی کند
communications cover	پوشش ارتباطاتی	پنهان سازی یا تغییر مشخصات الگوهای ارتباطات برای مخفی کردن اطلاعاتی که می تواند برای رقیب یا دشمن ارزشمند باشد
communications deception	فریب ارتباطاتی	ارسال یا بازارسال یا تغییر آگاهانه ارتباطات با هدف گمراه سازی دشمن
communications profile	رخ نمای ارتباطات	الگویی تحلیلی از ارتباطات وابسته به یک سازمان یا فعالیت که از آزمون نظام مند محتوا و الگوهای ارتباطات و توابع حاصل از آنها و سنجش های کاربردی امنیت ارتباطات حاصل می شود
communications security (COMSEC)	امنیت ارتباطات	

واژه بیگانه	معادل فارسی	تعریف
		اقدامات حفاظتی و واپایش‌هایی که از دسترسی افراد غیرمجاز به اطلاعات قابل دریافت از ارتباطات راه دور جلوگیری می‌کند تا اصالت این ارتباطات تضمین شود
compartmentalization	حیطه‌بندی	نوعی گروه‌بندی غیرسلسله‌مراتبی اطلاعات حساس برای واپایش دسترسی داده‌ها که دقیق‌تر از دسته‌بندی امنیتی سلسله‌مراتبی عمل می‌کند
compromise	به‌خطراتادگی کلید	افشا یا تغییر یا جایگزینی یا استفاده غیرمجاز از داده‌های حساس از جمله کلیدهای رمزنگاشتی (cryptographic keys) و دیگر پارامترهای امنیتی خطیر
compromised key	کلید به‌خطراتاده	کلیدی امنیتی (key security) که کل یا بخشی از آن افشا شده است
computational cryptography	رمزنگاری محاسباتی	بهبود و ارتقای پیاده‌سازی و تحلیل سامانه‌های رمز مبتنی بر نظریه اعداد و الگوریتم‌ها/ خوارزمی‌های محاسباتی
computational complexity theory	نظریه پیچیدگی محاسباتی	مطالعه کمیته منابع مورد نیاز برای حل مسائل محاسباتی
computational security	امنیت محاسباتی	امنیت کمی در مقابل رمزگشایی غیرمجاز بر پایه فرضیات خاصی که تحلیلگر در مورد رمز در نظر می‌گیرد
computationally secure steganography	نهان‌نگاری محاسباتی امن	نوعی خوارزمی/ الگوریتم نهان‌نگاری که مهاجم با در اختیار داشتن یک خوارزمی/ الگوریتم محاسباتی زمان چندجمله‌ای (polynomial-time computable algorithm) احتمالاتی تنها بتواند تمایز ناچیزی بین پوشانه و نهانه پیدا کند

واژه بیگانه	معادل فارسی	تعریف
computer incident response center (CIRC)	مرکز رویارویی با پیشامدهای رایانه‌ای	
syn. computer incident response team, CIRT	مت. گروه رویارویی با پیشامدهای رایانه‌ای	
syn. cyber incident response team	رایانه‌ای	
		گروهی از تحلیل‌گران امنیت رایانه که به‌منظور مهار و ریشه‌کشی پیشامدهای امنیتی در رایانه‌ها و بازیابی آسیب‌های ناشی از آنها گردهم آمده باشند
computer incident response team (CIRT),	گروه رویارویی با پیشامدهای رایانه‌ای	
syn. computer incident response center (CIRC)	مت. مرکز رویارویی با پیشامدهای رایانه‌ای	
syn. cyber incident response team	رایانه‌ای	
		گروهی از تحلیل‌گران امنیت رایانه که به‌منظور مهار و ریشه‌کشی پیشامدهای امنیتی در رایانه‌ها و بازیابی آسیب‌های ناشی از آنها گردهم آمده باشند
comsec (communications security)	سامانه واپایی اجزای امنیت ارتباطات (سوار)	
material control system		
abbr. cmcs		سامانه تدارکاتی و حسابداری که از طریق آن اجزای امنیت ارتباطات با برچسب «رمز» (CRYPTO) توزیع و واپایش و حراست می‌شوند
confirmer signature	امضای تأییدیار	
syn:designated confirmer signature	مت. امضای تأییدیار مشخص	
		نوعی امضا که بدون کمک امضاکننده یا یک شخص ثالث نیم‌معمد قابل واریسی نیست
Controlled Cryptographic Item	رمزاقلام واپاییده (راوا)	
abbr. CCI		سامانه اطلاعاتی یا مخابراتی امن یا مؤلفه رمزنگاشتی مرتبط با آن سامانه که بدون طبقه‌بندی است و به‌وسیله سامانه واپایی اجزای امنیت ارتباطات (سوار)، یک سامانه واپایی کلی معادل یا ترکیبی از هر دو راهبری می‌شود و پاسخ‌گویی و رؤیت‌پذیری را فراهم می‌کند
Controlled Cryptographic Item (CCI) Assembly	هم‌گذاری رمزاقلام واپاییده، اختصار: هم‌گذاری راو	
		دستگاهی حاوی یک منطق رمزنگاشتی یا یک طرح امنیت ارتباطاتی دیگر که مورد تأیید NSA (آژانس امنیت ملی آمریکا) به‌عنوان یک مؤلفه رمزاقلام واپاییده (مؤلفه راوا) باشد؛ این دستگاه کل عملیات امنیت ارتباطات را اجرا می‌کند ولی برای این کار به تجهیزات میزبان وابسته است
Controlled Cryptographic Item (CCI) Component	مؤلفه رمزاقلام واپاییده، مؤلفه راوا	

واژه بیگانه	معادل فارسی	تعریف
		قسمتی از اقلام رمزنگاشتی و پاییده که به تجهیزات میزبان یا همایه برای کامل کردن و اجرای کار امنیت ارتباطات وابسته است اما کل کار امنیت ارتباطات را انجام نمی دهد
Controlled Cryptographic Item (CCI) Equipment	تجهیزات رمزاقلام و پاییده، تجهیزات راوا	تجهیزات راهبری مخابرات یا اطلاعات که حاوی مؤلفه ای از اقلام رمزنگاشتی و پاییده یا همایه اقلام رمزنگاشتی و پاییده است و کل کار امنیت ارتباطات را بدون وابستگی به تجهیزات میزبان انجام می دهد
correlation attack	حمله همبستگی	نوعی حمله مبتنی بر روش تقسیم و حل که از وابستگی آماری بین دنباله کلید اجرایی و خروجی یکی از تاب های خطی سازنده رمز جریانی برای یافتن حالت اولیه همان تاب خطی استفاده می کند
correlation immunity	ایمنی از همبستگی	در توابع بولی، ویژگی یک تابع بولی n متغیره f ، هر گاه اطلاعات متقابل بین خروجی و همه زیربردارهای k تایی از متغیرهای ورودی صفر باشد
counter mode syn. integer counter mode	شیوه شمارگر مت. شیوه شمارگر صحیح	یکی از روش های معیار به کارگیری رمز قالبی (block cipher) که در آن ابتدا دنباله ای از اعداد به عنوان ورودی خوارزمی / الگوریتم رمز وارد می شود، سپس قالب های متن اصلی به ترتیب با قالب های خروجی خوارزمی / الگوریتم رمز ترکیب می شوند تا متن رمز شده متناظر با هر قالب به دست آید؛ پس از رمز گذاری هر قالب به مقدار شمارگر، مقدار ثابتی، معمولاً یک واحد، افزوده می شود
concurrent zero-knowledge proof	اثبات ناتراوای هم رو مت. اثبات دانش صفر هم رو	نوعی اثبات ناتراوا که حتی در صورت اجرای نسخه های پرشماری از آن در یک محیط ناهم زمان، مانند اینترنت، باز هم ناتراوا باقی بماند
coverttext	پوشانه	پیغامی که داده های پیغام محرمانه در داخل داده های آن درج می شود
cryptanalysis	تحلیل رمز	۱. بررسی امنیت سامانه های رمز از طریق جست و جوی خطاها یا ضعف های احتمالی خوارزمی / الگوریتم آنها به قصد ممانعت از نفوذ مهاجم و بالا بردن ضریب امنیت سامانه ۲. عملیات محاسباتی برای به دست آوردن کلید سامانه رمز، بدون آگاهی از کلید آن، با هدف نفوذ به سامانه

واژه بیگانه	معادل فارسی	تعریف
cryptanalyst	تحلیل‌گر رمز	فردی که تحلیل رمز می‌کند و در آن تخصص دارد
cryptographic primitive	نخستینه رمزنگاشتی	الگوریتم‌ها/خوارزمی‌های رمزنگاشتی شناخته‌شده و سطح‌پایین، شامل توابع چکیده‌ساز یک‌طرفه و توابع رمزگذاری که به‌طور معمول به‌منظور ساخت (طراحی) قراردادهای رمزنگاشتی برای سامانه‌های امنیت رایانه‌ای به‌کار می‌روند
cryptographic protocol	قرارداد رمزنگاشتی	یک الگوریتم/خوارزمی توزیع‌شده که به‌طور دقیق تعامل میان دو یا چند هستار را برای دسترسی به اهداف امنیتی مشخص بیان می‌کند
crypto officer	کارشناس رمز، مسئول رمز	فرد یا اداره‌ای برای اجرای امور رمزنگاشتی
crypto period syn. key lifetime	رمز دوره مت. طول عمر کلید	بازه‌ای زمانی که در آن کلید رمزگزاری برای یک سامانه رمز معتبر است
cryptocurrency	رمزارز	نوعی ارز که تنها به صورت رقمی وجود دارد و برای تنظیم فرایندهای تولید، واریسی و انتقال آن به صورت مستقل از یک بانک مرکزی، از روش‌های رمزنگاشتی استفاده می‌شود
cryptogram syn. ciphertext	متن رمز، رمزنگاشت مت. متن رمزی شده	خروجی الگوریتم رمزگذاری، یا داده‌ی رمز شده
cryptographic	رمزنگاشتی	مربوط به رمزنگاری یا به شیوه رمزنگاری
cryptographic algorithm	الگوریتم رمزنگاشتی مت. خوارزمی رمزنگاشتی	یک رویه محاسباتی که بر مبنای تعدادی متغیر ورودی، شامل یک کلید رمزنگاشتی، خروجی را تولید می‌کند

واژه بیگانه	معادل فارسی	تعریف
cryptographic hash function syn. hash function syn. hashing algorithm	تابع چکیده‌ساز رمزنگاشتی مت. تابع چکیده‌ساز مت. الگوریتم چکیده‌سازی	تابعی که طول ورودی آن دلخواه و طول خروجی آن ثابت است و از ویژگی‌های آن یک‌طرفه بودن، وابستگی خروجی به تمامی بیت‌های ورودی و بدون برخورد است
cryptographic mode	شیوه رمزنگاشتی	شیوه‌ای برای تأمین امنیت که در آن الگوریتم/خوارزمی‌های رمز پایه و انواعی از بازخوردها و عملگرهای ساده به گونه‌ای ترکیب می‌شوند که امنیت مجموعه حاصل، تابعی از امنیت الگوریتم/خوارزمی رمز به کاررفته باشد
cryptographic module	پودمان رمزنگاشتی	مجموعه سخت‌افزار و نرم‌افزار و ثابت‌افزار برای اجرای توابع امنیتی تأییدشده شامل الگوریتم‌ها / خوارزمی‌های رمزنگاشتی و تولید کلید
cryptographic module security policy	خط‌مشی امنیتی پودمان رمزنگاشتی	قواعد دقیق امنیتی که یک واحد رمزنگاشتی بر اساس آن عمل می‌کند
cryptographic coprocessor syn.cryptoprocessor/crypto-processor	همپرداز رمزنگاشتی مت. رمزپرداز	واحدی سخت‌افزاری شامل یک پردازنده خاص برای عملیات رمزنگاشتی و پردازش‌های مرتبط
cryptographic scheme	طرح رمزنگاشتی	مجموعه‌ای از الگوریتم‌ها/خوارزمی‌ها و قراردادهای رمزنگاشتی مرتبط برای دستیابی به اهداف امنیتی مشخص
cryptographic security	امنیت رمزنگاشتی	یکی از مؤلفه‌های امنیت ارتباطات، حاصل از تأمین و استفاده فنی صحیح از سامانه‌های رمزنگاشتی مناسب
cryptographic strength	استحکام رمزنگاشتی	معیاری برحسب تعداد عملیات مورد انتظار که برای شکستن یک سازوکار رمزنگاشتی نیاز است

واژه بیگانه	معادل فارسی	تعریف
cryptographic system syn. cipher system syn. cryptosystem	سامانه رمزنگاشتی مت. سامانه رمز	سامانه‌ای متشکل از خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی همراه با مجموعه‌ی سه‌گانه‌ی متن‌های اصلی و متن‌های رمز‌ی‌شده و کلیدها
cryptologist	رمزشناس	متخصص علم رمزشناسی
cryptology	رمزشناسی	شاخه‌ای از دانش که در آن روش‌های تبادل اطلاعات و ارتباطات محرمانه در شبکه‌های رایانه‌ای بررسی می‌شود
cryptoprocessor/crypto-processor syn.: cryptographic coprocessor	رمزپرداز مت. همپرداز رمزنگاشتی	واحدی سخت‌افزاری شامل یک پردازنده‌ی خاص برای عملیات رمزنگاشتی و پردازش‌های مرتبط
cryptosystem syn. cipher system syn. cryptographic system	سامانه رمز مت. سامانه رمزنگاشتی	سامانه‌ای متشکل از خوارزمی‌ها/ الگوریتم‌های رمزگذاری و رمزگشایی همراه با مجموعه‌ی سه‌گانه‌ی متن‌های اصلی و متن‌های رمز‌ی‌شده و کلیدها
cyber incident response team syn. computer incident response center (CIRC) syn. computer incident response team (CIRT)	گروه رویارویی با پیشامدهای رایانه‌ای مت. مرکز رویارویی با پیشامدهای رایانه‌ای	گروهی از تحلیل‌گران امنیت رایانه که به‌منظور مهار و ریشه‌کشی پیشامدهای امنیتی در رایانه‌ها و بازیابی آسیب‌های ناشی از آنها گردهم آمده باشند
D		
data complexity	پیچیدگی داده‌ای	میزان داده‌ی مورد نیاز برای انجام یک حمله
data encapsulation mechanism	سازوکار لفاف‌بندی داده (سِلِد)	محافظت از رازمانی و یکپارچگی انبوه داده‌ها به روش‌های متقارن
data encryption	رمزگذاری داده‌ها	

واژه بیگانه	معادل فارسی	تعریف
		فرایندی که در آن داده‌ها به دلایل امنیتی رمزگذاری شوند.
data encryption standard, DES	استاندارد رمزگذاری داده‌ها	
		خوارزمی / الگوریتم مورد توافق (استاندارد) برای رمزگذاری یا رمزگشایی داده‌ها با استفاده از جدول رمز ۶۴ بیتی
data security	امنیت داده	
		حفاظت از داده‌ها در مقابل تغییر غیرمجاز عمدی یا تصادفی، تخریب یا افشای آن‌ها
decipher syn. decrypt	رمزگشایی کردن	
		تبدیل متن رمز به متن آشکار با استفاده از خوارزمی / الگوریتم رمزگشایی و کلید
deciphering syn. decrypting	رمزگشایی	
		فرآیند تبدیل اطلاعات رمز شده به متن اصلی متناظر با استفاده از خوارزمی / الگوریتم خاص آن
decisional Diffie-Hellman problem	مسئله تصمیم دیفی - هلمن	
		مسئله اخذ تصمیم در مورد برقراری رابطه $c = ab \pmod{q}$ بر اساس سه تایی (ap, bp, cp) داده شده در گروه G از مرتبه q
decrypt syn. decipher	رمزگشایی کردن	
		تبدیل متن رمز به متن آشکار با استفاده از خوارزمی / الگوریتم رمزگشایی و کلید
decrypted	رمزگشایی شده	
		اطلاعات یا داده‌های رمزگذاری شده‌ای که به اطلاعات یا داده‌های آشکار تبدیل شده باشند
decrypting syn. deciphering	رمزگشایی	
		فرآیند تبدیل اطلاعات رمز شده به متن اصلی متناظر با استفاده از خوارزمی / الگوریتم خاص آن
decryption mixnet	شبکه مخلوط رمزگشایی	
		نوعی شبکه مخلوط که در آن ورودی‌های هر مرحله با استفاده از کلید خصوصی متناظر با آن مرحله بازگشایی می‌شوند
delay-based silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی تأخیر مبنا / تفت سیلیکونی تأخیر مبنا	

واژه بیگانه	معادل فارسی	تعریف
		دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی که خروجی آن‌ها از طریق اندازه‌گیری متغیرهای تصادفی حاصل از تأخیر یک مدار رقمی/دیجیتال به دست می‌آید
deniable authentication	احراز اصالت انکارپذیر مت. اصالت‌سنجی انکارپذیر	نوعی قرارداد احراز اصالت که به فرستنده امکان می‌دهد که پیامی را برای گیرنده احراز اصالت کند به نحوی که گیرنده نتواند شخص سومی را متقاعد کند که چنین احراز اصالتی (یا هر احراز اصالتی) تا کنون انجام شده است
deniable encryption syn. sender deniable encryption	رمزگذاری انکارپذیر مت. رمزگذاری فرستنده انکارپذیر	نوعی رمزگذاری که در آن فرستنده بتواند در صورت لزوم رمزگذاری پیام ارسال شده را انکار کند
derived key	کلید مشتق	کلید محاسبه شده توسط یک الگوریتم/خوارزمی مشخص که ورودی آن شامل داده‌های عمومی و محرمانه است
designated confirmer signature syn: confirmer signature	امضای تأییدیار مشخص مت. امضای تأییدیار	نوعی امضا که بدون کمک امضاکننده یا یک شخص ثالث نیم‌معتد قابل واریسی نیست
designated-verifier signature	امضای واریس مشخص	نوعی امضای رقمی که در آن واریسی‌کننده مشخصی از اعتبار پیام امضا شده مطمئن می‌شود، اما نمی‌تواند شخص ثالث یا نهاد دیگری را قانع کند
deterministic encryption	رمزگذاری تعینی	نوعی خوارزمی/الگوریتم رمزگذاری که در آن به ازای یک متن ساده و کلید مشخص فقط یک متن رمز بدست می‌آید
dictionary attack	حمله واژه‌نامه‌ای	نوعی حمله برای شناسایی گذرواژه با آزمودن پی‌درپی واژه‌های واژه‌نامه‌ای که احتمال می‌رود در بردارنده گذرواژه باشند
differential cryptanalysis	تحلیل تفاضلی رمز	

واژه بیگانه	معادل فارسی	تعریف
		تحلیل رمزی که در آن تحلیلگر می‌کوشد با به دست آوردن رابطهٔ محتمل بین تفاضل ورودی‌ها و خروجی‌ها، کلید رمز را به دست آورد
differential linear attack	حملهٔ تفاضلی - خطی	نوعی حمله با متن اصلی منتخب که در دو مرحله انجام می‌شود. در مرحلهٔ نخست حمله، تحلیل تفاضلی و در مرحلهٔ دوم، تحلیل خطی صورت می‌گیرد
differential-linear attack	حملهٔ تفاضلی-خطی	نوعی تحلیل با متن اصلی منتخب با راهکار دو مرحله‌ای که در آن در مرحلهٔ نخست، تحلیل رمز تفاضلی، از ابتدا تا دور میانی رمز قالبی، انجام می‌شود، سپس در مرحلهٔ دوم از دور میانی تا انتها تحلیل خطی اجرا می‌شود
Diffie-Hellman problem	مسئلهٔ دیفی - هلمن	مسئلهٔ محاسبهٔ g^{xy} با در اختیار داشتن g و g^x و g^y در گروه دوری G با مولد g و x و y به عنوان دو عدد صحیح مثبت
digital signature schemes	طرح‌های امضای رقمی	روش‌هایی برای اطمینان از تأیید ارسال یک پیام مشخص توسط یک هستار، که به طور معمول با استفاده از کلید خصوصی فرستنده برای تولید امضا انجام می‌شوند
digital steganography	نهان‌نگاری رقمی	پنهان سازی اطلاعات رقمی محرمانه از طریق درج آن‌ها در داخل داده‌های پیام عادی
digraph syn.: bigram	دونویسه	یک زوج مرتب متشکل از حروف (نویسه‌ها) در متن رمز
digraphic substitution syn.: bipartite substitution	جانشینی دوبخشی	نوعی جانشینی که در آن از دونگاشت‌ها برای جایگزینی دونویسه‌ها (زوج‌های مرتب از نویسه‌ها)ی متن اصلی استفاده می‌شود
discretionary access control	واپایش دسترسی انتخابی	

واژه بیگانه	معادل فارسی	تعریف
		نوعی واپایش دسترسی که در آن کاربر براساس صلاحدید خود افراد مجاز به دسترسی به منابع مربوط به خود و سطح دسترسی آن ها را تعیین می کند
distance bounding protocol	قرارداد فاصله محدود	قراردادی رمزنگاشتی که در آن یکی از طرفین ارتباط مایل است برای فاصله فیزیکی خود با طرف مقابل یک کران بالا تعیین کند
distinguishing attack	حمله تمایزی	حمله ای با هدف تفکیک جریان کلید از یک دنباله واقعا تصادفی
divide-and-conquer attack	حمله تقسیم و حل	نوعی حمله که در آن کلید رمز با استفاده از وجود همبستگی بین خروجی تابع ترکیب کننده رمز و شماری از مؤلفه های ورودی آن به دست می آید
dynamic adversary syn. adaptive adversary	مهاجم پویا مت: مهاجم وقتی	مهاجمی که در طول اجرای یک پروتکل تصمیم می گیرد که کدامیک از نهادهای های شرکت کننده در پروتکل را به عنوان نهاد تسخیر شده انتخاب کند
dynamic group signature	امضای گروهی پویا	نوعی امضای گروهی که در آن کلید عمومی گروه حتی پس از پیوستن یا ترک یک یا چند عضو گروه یا به روزرسانی زوج کلیدهای اختصاصی یک یا چند عضو گروه بدون تغییر باقی می ماند
E		
eavesdropper	شنودگر	شخص یا نهادی که به صورت غیرمجاز به داده های یک شبکه ارتباطی دسترسی می یابد
eavesdropping	شنود	ورود مخفیانه به یک شبکه ارتباطی، اعم از صوتی یا نوشتاری، بدون ایجاد هرگونه تغییر در محتوا یا اختلال در آن

واژه بیگانه	معادل فارسی	تعریف
electromagnetic attack	حمله الکترومغناطیسی	حمله‌ای که در آن حمله‌کننده از نشت تابش الکترومغناطیسی سامانه رمز، به اطلاعات مربوط به کلید مخفی دست می‌یابد
electronic codebook mode	شیوه کدنامه الکترونیکی	ساده‌ترین شیوه به کارگیری رمزهای‌های قالبی که در آن قالب‌های یکسان متن اصلی همیشه به قالب‌هایی یکسان از متن رمز شده تصویر می‌شوند و بدین ترتیب، امکان تشکیل یک کتاب‌کد از زوج‌های متن اصلی و رمز متناظر فراهم می‌شود
elliptic curve cryptography	رمزنگاری مبتنی بر خم بیضوی	نوعی سامانه رمزنگاری کلید عمومی، مبتنی بر ساختار ریاضی خم‌های بیضوی
encipher syn. encrypt	رمزگذاری کردن	تبدیل متن اصلی به متن رمز شده با استفاده از ابزار رمزنگاشتی
enciphered syn. encrypted	رمزگذاری شده، رمزیده	داده‌های رمز شده
enciphered code	کد رمزگذاری، کد رمزیده	کدی که تبدیل به رمز شده باشد و معنای آن برای گیرنده غیرمجاز قابل درک نباشد
enciphering syn. encryption	رمزگذاری	فرآیند تبدیل متن اصلی به متن رمز شده با استفاده از خوارزمی (الگوریتم) رمزنگاشتی
encrypt syn. encipher	رمزگذاری کردن	تبدیل متن اصلی به متن رمز شده با استفاده از ابزار رمزنگاشتی
encrypted syn. enciphered	رمزگذاری شده، رمزیده	داده‌های رمز شده
encrypted data	داده‌های رمزگذاری شده، داده‌های رمزیده	

واژه بیگانه	معادل فارسی	تعریف
		داده‌های تغییر داده‌شده با استفاده از یک سامانه رمزنگاشتی که برای اشخاص یا طرف‌های غیرمجاز مفهوم نباشد
encryption syn. enciphering	رمز گذاری	فرآیند تبدیل متن اصلی به متن رمز شده با استفاده از خوارزمی (الگوریتم) رمزنگاشتی
encryption algorithm syn. cipher	خوارزمی رمز گذاری ، الگوریتم رمز گذاری مت. رمز	
		خوارزمی / الگوریتمی برای تبدیل متن اصلی به متن رمز شده به نحوی که برای گیرنده غیرمجاز غیرقابل درک باشد
end-to-end encryption	رمز گذاری سرتاسر	
		رمز گذاری اطلاعات در مبدأ و رمز گشایی آن در مقصد، بدون امکان رمز گشایی در نقاط میانی
end-to-end security	امنیت سرتاسر	
		محافظت از اطلاعات در یک سامانه اطلاعاتی از مبدأ تا مقصد
entrapment	تله گذاری	
		تعیین عمدی رخنه‌های مشخص در یک سامانه اطلاعات با هدف آشکار سازی تلاش‌هایی که برای نفوذ به سامانه صورت می‌گیرند
ephemeral key	کلید موقت	
		کلید کوتاه‌مدت و غیرقابل تکراری که با هر بار اجرای فرایند برقراری کلید، تولید می‌شود
evasion attack	حمله دورزنی	
		حمله‌ای که در آن مهاجم بدون آن که افزاره امنیتی متصل به شبکه یا سامانه هدف متوجه شود از آن عبور می‌نماید
exhaustive key search syn. brute force attack	کلید جویی فراگیر مت. حمله غیرهوشمندانه	
		حمله‌ای مبتنی بر آزمایش و به کارگیری تک‌تک کلیدها به منظور پیدا کردن کلید صحیح

واژه بیگانه	معادل فارسی	تعریف
-------------	-------------	-------

existential forgery

جعل امضای وجودی

نوعی جعل امضا که در آن مهاجم، بدون در اختیار داشتن کلید خصوصی، قادر به تولید امضای معتبر بر روی یک پیام دلخواه امضا نشده باشد

explicit key authentication

احراز اصالت صریح کلید
مت. اصالت‌سنجی صریح کلید

فرایندی در طرح‌های برقراری کلید که علاوه بر تضمین عدم دستیابی هستاری دیگر، به جز هستار موردنظر، دستیابی طرف مقابل به کلید را نیز تأیید می‌کند

F

fabrication attack

حملهٔ برساختی

وارد کردن اطلاعات جعلی توسط یک هستار غیرمجاز در سامانه

fail-stop digital signature

امضای رقمی جعل-اثبات
مت. امضای جعل-اثبات

نوعی امضای رقمی که در آن امضاکننده از جعل ناپذیری امضای خود به صورت بی‌قید و شرط اطمینان می‌یابد و در صورت مشاهدهٔ امضایی که خود تولید نکرده می‌تواند جعلی بودن آن را اثبات کند؛ درحالی که واریسی کننده با خطر تأیید امضای جعلی مواجه است و اطمینان او از اعتبار امضا تنها به شیوهٔ محاسباتی برآورده می‌شود

fail-stop signature
syn. fail-stop digital signature

امضای جعل-اثبات
مت. امضای رقمی جعل-اثبات

نوعی امضای رقمی که در آن امضاکننده از جعل ناپذیری امضای خود به صورت بی‌قید و شرط اطمینان می‌یابد و در صورت مشاهدهٔ امضایی که خود تولید نکرده می‌تواند جعلی بودن آن را اثبات کند؛ درحالی که واریسی کننده با خطر تأیید امضای جعلی مواجه است و اطمینان او از اعتبار امضا تنها به شیوهٔ محاسباتی برآورده می‌شود

fast correlation attack

حملهٔ همبستگی سریع

واژه بیگانه	معادل فارسی	تعریف
		نوعی حمله همبستگی که به علت استفاده از فنون تصحیح خطای کارا (efficient error-correcting techniques) و اجتناب از جستجوی کامل حالت‌های اولیه، به میزان قابل توجهی از حمله همبستگی سریع تر است
fault attack	حمله عیب‌افزایی	هر نوع حمله با استفاده از ترکیبی از شرایط محیطی مختلف که سبب ایجاد خطاهای محاسباتی در تراشه و در نتیجه نشت اطلاعات حفاظت شده می‌شود
feedback shift register (FSR)	ثبات انتقال بازخوردی (ثاب)	ساختاری متشکل از دو بخش شامل یک ثبات انتقال و یک تابع بازخورد که به عنوان عنصر اصلی مولد کلید اجرایی در رمز جریانی استفاده می‌شود
filter generator	مولد پالایه‌ای	نوعی مولد کلید جریانی برای الگوریتم/خوارزمی‌های رمز جریانی، متشکل از یک ثاب خطی (ثبات انتقال بازخوردی خطی) که خروجی آن از اعمال یک تابع غیرخطی بر روی برخی از حالت‌های ثبات حاصل می‌شود
first-preimage attack	حمله به پیش‌تصویر اول	حمله‌ای به توابع چکیده‌سازی با خروجی به طول n ، که در آن مهاجم با داشتن یک مقدار چکیده (hash value)، با کمتر از 2^n به توان n بار اقدام، موفق به یافتن پیامی با همان مقدار چکیده شود
first-preimage resistance syn. preimage resistance	مقاومت در برابر پیش‌تصویر اول مت. مقاومت در برابر پیش‌تصویر	یکی از خصوصیات مطلوب در توابع چکیده‌سازی که باعث می‌شود به‌ازای هر یک از مقادیر خروجی یک تابع چکیده‌سازی، یافتن دست‌کم یک ورودی که به آن مقدار خروجی تصویر شود، از نظر محاسباتی عملی نباشد
fixed point attack	حمله نقطه ثابتی	حمله‌ای علیه توابع چکیده‌سازی که در آن برای یافتن برخورد، از نقطه ثابت در زیرتابع (subfunction) فشرده‌ساز مورد استفاده در تابع چکیده‌سازی، استفاده می‌شود
flooding attack	حمله سیلابی	

واژه بیگانه	معادل فارسی	تعریف
		بکارگیری تمام منابع محاسباتی یا ارتباطی با ارسال درخواست‌های زیاد برای اختلال در کار یک سامانه
forward secrecy	رازمانی پیش‌سو	خصوصیتی در طرح تبادل کلید که بنا بر آن لو رفتن کلید یک نشست تنها بر امنیت همان نشست تأثیر گذارد و تهدیدی برای امنیت نشست‌های پیشین نباشد
freshness attack syn. replay attack	حمله تکرار	حمله‌ای با هدف نقض تازگی پیام، که در آن مهاجم پیامی را که در اجرای قبلی قرارداد احراز اصالت ذخیره کرده است، در اجرای جدید آن تکرار می‌کند
full non-volatile memory attacker	مهاجم تام‌آگاه از حافظه غیر فرآر	مهاجمی که قادر به استخراج تمام اطلاعات سرّی ذخیره شده در حافظه غیر فرآر است
fully memory leakage resilient (FMLR) protocol	قرارداد تام‌نشست تاب حافظه	قرارداد(پروتکلی) امن در برابر نشت کامل اطلاعات از حافظه غیر فرآر
functional encryption	رمز گذاری تابعی	نوعی رمز گذاری نامتقارن که در آن هر کاربر مجاز، با استفاده از یک کلید خصوصی، قادر به دستیابی به تابعی مشخص از متن اصلی می‌شود
G		
gap	ریسه صفر	صفرهای متوالی در یک دنباله دودویی که بیت پیش و پس از آن یک باشد
gap Diffie-Hellman group	گروه گسست دیفی - هلمن	
		گروهی که حل مسئله تصمیم دیفی - هلمن روی آن در زمان چند جمله‌ای امکان پذیر باشد، اما احتمال وجود یک الگوریتم/خوارزمی احتمالاتی برای حل مسئله محاسباتی دیفی - هلمن بر روی آن در زمان چند جمله‌ای ناچیز باشد
gap Diffie-Hellman problem	مسئله گسست دیفی - هلمن	

واژه بیگانه	معادل فارسی	تعریف
		مسئله پیدا کردن عنصر $c = g^{ab}$ با فرض در اختیار داشتن سه تایی (g^b, g^a, g) و نیز با فرض توانایی حل مسئله تصمیم دینی-هلمن
generalized inversion attack	حمله وارونی تعمیم یافته	نوعی حمله وارونی که بر همه مولدهای پالایه‌ای، اعم از خطی و غیرخطی، قابل اجرا است
group authenticator	اصالت نشان گروهی	ابزاری که دسترسی به برخی داده‌ها یا منابع به اشتراک گذاشته شده را برای اعضای یک گروه مشخص فراهم می کند
group key agreement syn. group key distribution	توافق کلید گروهی مت. توزیع کلید گروهی	صورت گسترش یافته توافق کلید که در آن کلید مشترک بین چند نهاد به اشتراک گذاشته می شود
group key distribution syn. group key agreement	توزیع کلید گروهی مت. توافق کلید گروهی	صورت گسترش یافته توافق کلید که در آن کلید مشترک بین چند نهاد به اشتراک گذاشته می شود
group signature	امضای گروهی	نوعی امضای رقمی که در آن هر یک از اعضای گروه تشکیل شده، از جانب آن گروه و به طور گمنام، قادر به تولید امضا باشند؛ مدیر گروه یک هشتر معتمد است که بر خروج یا ورود افراد جدید نظارت می کند و در صورت لزوم قادر به شناسایی امضاکننده است
H		
hardware security module abbr.: HSM	پودمان امنیتی سخت افزاری (پاس)	افزازه محاسباتی فیزیکی مقاوم در برابر دستکاری و نفوذ، برای حفاظت و مدیریت کلیدهای رقمی و سایر رازها، و همچنین پردازش های رمزنگاشتی
hash-based cryptography	رمزنگاری چکیده بنیاد	نوعی رمزنگاری مبتنی بر نخستینه های (primitives) رمزنگاشتی، که امنیت آنها بر امنیت توابع چکیده ساز استوار است

واژه بیگانه	معادل فارسی	تعریف
hash-based message authentication code (HMAC)	کد احراز اصالت پیام چکیده‌بنیاد، کد اصالت‌سنجی پیام چکیده‌بنیاد (اختصار: کاپ چکیده بنیاد)	نوعی کد احراز اصالت پیام (کاپ) با استفاده از یک کلید رمزنگاشتی و یک تابع چکیده‌ساز
hash function syn. cryptographic hash function syn. hashing algorithm	تابع چکیده ساز مت. تابع چکیده ساز رمزنگاشتی مت. الگوریتم چکیده سازی	تابعی که طول ورودی آن دلخواه و طول خروجی آن ثابت است و از ویژگی‌های آن یک‌طرفه بودن، وابستگی خروجی به تمامی بیت‌های ورودی و بدون برخورد است
hashing algorithm syn. cryptographic hash function syn. hash function	الگوریتم چکیده سازی مت. تابع چکیده‌ساز مت تابع چکیده ساز رمزنگاشتی	تابعی که طول ورودی آن دلخواه و طول خروجی آن ثابت است و از ویژگی‌های آن یک‌طرفه بودن، وابستگی خروجی به تمامی بیت‌های ورودی و بدون برخورد است
heuristic security	امنیت یافتاری	امنیت اثبات‌نشده و مبتنی بر نتیجه تلاش ناموفق تعداد زیادی افراد حرفه‌ای برای شکستن یک سامانه رمز
homophonic substitution cipher	رمز جانشینی هم‌نوا	نوعی رمز جانشینی که در آن هر حرف متن اصلی به حرفی از یک مجموعه چندتایی از حروف الفبای رمز نگاشته می‌شود
hybrid encryption	رمز گذاری ترکیبی	نوعی رمز گذاری که از ترکیب دو یا چند خوارزمی / الگوریتم رمز گذاری حاصل می‌شود و غالباً ترکیبی از رمز گذاری متقارن و نامتقارن است
ID-based access control	واپایش دسترسی شناسه‌بنیاد	نوعی واپایش دسترسی مبتنی بر شناسه کاربر

واژه بیگانه	معادل فارسی	تعریف
ID-based cryptosystem Syn. identity-based cryptosystem	سامانه رمز شناسه‌بنیاد	نوعی سامانه رمز کلید عمومی برای حذف گواهی‌های مربوط به کلیدهای عمومی و ساده‌سازی مدیریت گواهی‌ها که در آن کلید عمومی هر کاربر با استفاده از یک شناسه متناظر با او مانند نشانی رایانامه یا نام کاربر یا شماره تلفن قابل تولید است
identity binding	ترابست شناسه	ایجاد ارتباط بین هویت یک فرد با شناسه ادعایی توسط یک مرجع رسمی
identity proofing	اثبات شناسه	فرایند ارائه و تأیید اطلاعات کافی برای شناسایی منحصر به فرد هر فرد از سوی مراجع ثبت گواهی و صدور اعتبارنامه
identity registration	ثبت شناسه	فرایند معرفی شناسه یک شخص به سامانه واری شناسه شخصی با استفاده از یک شناسه منحصر به فرد متناظر
identity-based cryptosystem syn. ID-based cryptosystem	سامانه رمز شناسه‌بنیاد	نوعی سامانه رمز کلید عمومی برای حذف گواهی‌های مربوط به کلیدهای عمومی و ساده‌سازی مدیریت گواهی‌ها که در آن کلید عمومی هر کاربر با استفاده از یک شناسه متناظر با او مانند نشانی رایانامه یا نام کاربر یا شماره تلفن قابل تولید است
imitative communications deception	فریب ارتباطاتی بدلی	تزریق پیام یا نشانک‌های / سیگنال‌های فریب‌آمیز به نشانک‌های / سیگنال‌های ارتباطاتی مهاجم
impersonation attack	حمله جعل هویت	حمله‌ای که در آن مهاجم هویت یکی از طرف‌های مجاز در یک سامانه یا قرارداد (پروتکل) ارتباطی (communications protocol) را به خود نسبت می‌دهد
implicit key authentication syn. key authentication	اصالت سنجی کلید مت. احراز اصالت کلید اصالت سنجی کلید	احراز اصالت ضمنی کلید

فرایند معمول در طرح‌های برقراری کلید برای تضمین عدم دستیابی هستاری دیگر، به جز هستار مورد نظر، به کلید

واژه بیگانه	معادل فارسی	تعریف
information assurance	تضمین اطلاعات	اقداماتی برای حفاظت از اطلاعات و سامانه‌های اطلاعاتی از طریق کسب اطمینان از دسترس‌پذیری، یکپارچگی، احراز اصالت (اصالت سنجی)، محرمانگی و عدم انکار
information warfare	جنگ اطلاعاتی	عملیاتی با هدف تخریب یا دستیابی به منابع اطلاعاتی طرف مقابل (قربانی)
information-theoretically secure steganography	نهان‌نگاری نظریه‌اطلاعاتی امن	نوعی نهان‌نگاری با ویژگی امن کامل یا امن آماری
integer counter mode syn. counter mode	شیوه شمارگر صحیح مت. شیوه شمارگر	یکی از روش‌های معیار به کارگیری رمز قالبی (block cipher) که در آن ابتدا دنباله‌ای از اعداد به عنوان ورودی خوارزمی / الگوریتم رمز وارد می‌شود، سپس قالب‌های متن اصلی به ترتیب با قالب‌های خروجی خوارزمی / الگوریتم رمز ترکیب می‌شوند تا متن رمز شده متناظر با هر قالب به دست آید؛ پس از رمز گذاری هر قالب به مقدار شمارگر، مقدار ثابتی، معمولاً یک واحد، افزوده می‌شود
integrity check value	قدر آزمای یکپارچگی	نوعی جمع‌آزما (checksum) با قابلیت کشف تغییر در یک سامانه اطلاعاتی
intractable problems	مسائل مهارناپذیر	مسائلی که در زمان چندجمله‌ای قابل حل نیستند، زیرا محاسبه جواب آن‌ها به سرعت غیرعملی می‌شود
invasive attack	حمله تهاجمی	اقداماتی برای حفاظت از اطلاعات و سامانه‌های اطلاعاتی از طریق کسب اطمینان از دسترس‌پذیری، یکپارچگی، احراز اصالت (اصالت سنجی)، محرمانگی و عدم انکار
inversion attack	حمله وارونی	نوعی حمله با متن اصلی معلوم به برخی مولدهای پالایه‌ای، برای بازیابی حالت اولیه ثابت خطی (ثبات انتقال بازخوردی خطی) از یک قطعه کلید جریانی، هرگاه چندجمله‌ای بازخوردی ثابت و نقاط انشعاب و مولد پالایه‌ای معلوم باشند

واژه بیگانه	معادل فارسی	تعریف
K		
key agreement	توافق کلید	نوعی تبادل کلید که در آن دو یا چند کاربر با اجرای یک قرارداد به روش امن، یک کلید را به اشتراک می‌گذارند
key authentication syn. implicit key authentication	احراز اصالت کلید، اصالت‌سنجی کلید مت. احراز اصالت ضمنی کلید، اصالت‌سنجی ضمنی کلید	فرایند معمول در طرح‌های برقراری کلید برای تضمین عدم دستیابی هستاری دیگر، به جز هستار مورد نظر، به کلید
key confirmation	تأیید کلید	کسب اطمینان هر یک از طرف‌های شرکت کننده در پروتکل (قرارداد) از دستیابی طرف‌های مقابل به اطلاعات سرّی یکسان برای تولید کلید
key distribution	توزیع کلید	یکی از مهم‌ترین مباحث مرتبط با سامانه‌های رمز که کلیدها را در اختیار پودمان‌ها قرار می‌دهد
key distribution centre	مرکز توزیع کلید	هستاری که شاه کلید گره‌های موجود در شبکه را در اختیار دارد و همچنین قادر است کلید جلسه را برای همه گره‌ها به صورت دوه‌دو تولید کند
Key Encapsulation Mechanism (KEM)	سازوکار لفاف‌بندی کلید (سلک)	رمزگذاری نامتقارن برای رمزگذاری یک کلید متقارن
key escrow	امان‌سپاری کلید	سپردن کلید رمزنگاشتی به یک یا چند نهاد ثالث برای بازیابی آن تحت شرایطی خاص
key establishment	برقراری کلید	روند توزیع امن کلیدهای رمزنگاشتی بین پودمان‌ها

واژه بیگانه	معادل فارسی	تعریف
key exchange	تبادل کلید	به اشتراک گذاشتن یک کلید مخفی بین طرفین برای برقراری یک ارتباط امن
key expansion	گسترش کلید	روالی برای تولید کلیدهای دور یا زیر کلیدها (sub-key) از کلید رمز یا کلید اصلی (main key)
key lifetime syn.crypto period	طول عمر کلید مت. رمز دوره	بازه‌ای زمانی که در آن کلید رمز‌گذاری برای یک سامانه رمز معتبر است
key management device	افزایه مدیریت کلید	افزایه‌ای به منظور توزیع امن کلیدهای رمزنگاشتی به صورت الکترونیکی برای کاربران مجاز
key management infrastructure	زیرساخت مدیریت کلید	همه بخش‌های مربوط به پشتیبانی و تهیه ملزومات لازم برای مدیریت کلید شامل سخت‌افزار و ثابت‌افزار و نرم‌افزارهای رایانه‌ای و دیگر تجهیزات و مستندات
key pair	زوج کلید	دو کلید که با یکدیگر رابطه ریاضی دارند و یکی برای رمز‌گذاری و دیگری برای رمزگشایی پیام به کار می‌رود؛ با شناسایی یکی از آنها و استفاده از روش‌های محاسباتی نمی‌توان کلید دیگر را پیدا کرد
key recovery	بازیابی کلید	تولید مجدد کلید رمزنگاشتی در صورت سرقت یا گم شدن یا تخریب آن
key recovery attack	حمله بازیابی کلید	نوعی حمله به قصد یافتن کلید یک سامانه رمز
key schedule	فرانمای کلید	الگوریتمی برای تولید زیر کلیدها در دوره‌های مختلف یک رمز قالبی، با استفاده از کلید منتخب کاربر

واژه بیگانه	معادل فارسی	تعریف
keystream/ key stream/ key-stream syn. running-key	جریان کلید مت. کلید جریانی	دنباله‌ای که در رمزهای جریانی نماد به نماد با دنباله متن ساده ترکیب می‌شود تا دنباله متن رمز به دست آید
key whitening	سپیدسازی کلید	روشی برای افزایش امنیت رمز قالبی (block cipher) که در آن قبل از دور اول و بعد از دور آخر رمزگذاری، داده با بخشی از کلید ترکیب می‌شود
keying	کلید گذاری	جانشانی کلید در یک ابزار رمزنگاشتی
keystream/ key stream/ key-stream	جریان کلید	دنباله‌ای مورد استفاده در رمزهای جریانی که از ترکیب نماد به نماد اعضای آن با عناصر دنباله متن اصلی، دنباله متن رمز به دست می‌آید
kleptography	سرفت شناسی	بررسی چگونگی دستیابی طراح یک سامانه رمز به اطلاعات کاربران بدون اطلاع آن‌ها
knapsack problem	مسئله کوله پشتی	مسئله یافتن زیرمجموعه‌ای از یک مجموعه اعداد صحیح مثبت، که حاصل جمع اعضای آن برابر با یک عدد مشخص باشد
known related key attack	حمله کلیدمرتبط معلوم	حمله کلیدمرتبطی که بر پایه آگاهی مهاجم از ارتباط بین کلیدها استوار است
known signature attack	حمله امضامعلوم	حمله‌ای که تنها با در اختیار داشتن کلید عمومی امضاکننده و مجموعه‌ای از زوج‌های پیام-امضا (message-signature pairs) صورت می‌گیرد
known-plaintext attack	حمله با متن اصلی معلوم	

واژه بیگانه	معادل فارسی	تعریف
-------------	-------------	-------

حمله‌ای (تحلیل رمزی) که با استفاده از شماری متن اصلی معلوم و متن‌های رمز متناظر با آنها انجام می‌شود

L

lattice-based cryptography رمزنگاری مشبکه‌بنیاد

نوعی رمزنگاری که امنیت آن براساس سختی چند مسئله دشوار در حوزه مشبکه‌ها استوار است

LFSR
Syn. linear feedback shift register
ثاب خطی
مت. ثبات انتقال بازخوردی خطی

نوعی ثبات انتقال بازخوردی که تابع بازخورد آن خطی است

lightweight cryptography رمزنگاری سبک

شاخه‌ای از رمزنگاری با هدف طراحی و تحلیل طرح‌ها و قرارداد(پروتکل)های رمزنگاشتی قابل استفاده در محیط‌های دارای منابع محاسباتی و ذخیره‌سازی محدود

linear cryptanalysis تحلیل خطی رمز

تحلیل رمز مبتنی بر یافتن تقریب‌های همگر

linear feedback shift register
syn. LFSR
ثبات انتقال بازخوردی خطی
مت. ثاب خطی

نوعی ثبات انتقال بازخوردی که تابع بازخورد آن خطی است

linear syndrome attack حمله نشانگان خطی

نسخه‌ای ضعیف از حمله همبستگی سریع که بر روی مولدهای جریان کلید مبتنی بر ثاب خطی اعمال می‌شود

linguistic steganography نهمان‌نگاری زبانی

هنر پنهان کردن اطلاعات با استفاده از روش‌ها و قواعد زبانی

link encryption رمزگذاری پیوند

روشی برای رمزگذاری تمام داده‌های یک خط ارتباطی مانند ارتباطات ماهواره ای یا مدارهای تلفنی، که با توجه به رمزگذاری تمامی داده‌ها از جمله داده‌های مسیریابی، انجام عملیات رمزگشایی برای ادامه مسیر، در مسیریاب‌ها ضروری

واژه بیگانه	معادل فارسی	تعریف
		است
logical attack	حمله منطقی	حمله‌ای با هدف بازیابی داده‌های سرّی از تجهیزات امن بدون آسیب‌رسانی جدی به آنها
M		
malleability	چکش‌پذیری	خاصیت یک خوارزمی/الگوریتم که به‌موجب آن با داشتن متن رمزشده c1، تولید یک متن رمزشده دیگر مانند c2، با ارتباط معلوم بین متن‌های اصلی متناظر آنها امکان‌پذیر باشد
mandatory access control	واپایش دسترسی اجباری	نوعی واپایش برای محدود سازی دسترسی به منابع، توسط مدیر شبکه براساس مجموعه‌ای از قوانین و مقررات الزامی
man-in-the-middle attack	حمله فرد در میان	حمله‌ای که در آن مهاجم در بین دو طرف یک مسیر امن قرار می‌گیرد و هر بار خود را به جای یکی از دو طرف معرفی می‌کند
manipulative communications deception	فریب ارتباطاتی ساختگی	تغییر یا شبیه‌سازی ارتباطات دوستانه به‌منظور فریب
master key	شاه کلید	کلیدی رمزنگاشتی که کاربرد اصلی آن محافظت یا تولید کلیدهای دیگر است
maximum disclosure proof	اثبات بیش‌تراوا مت. اثبات بیشینه‌افشا	نوعی روش اثبات در رمزنگاری که در آن اثبات‌کننده دارای اطلاعات واریسی‌پذیر است و برای متقاعد ساختن واریسی‌کننده به این واقعیت، اطلاعات را در اختیار او قرار می‌دهد، به‌طوری‌که واریسی‌کننده خود قادر به اجرای روند واریسی باشد

واژه بیگانه	معادل فارسی	تعریف
meet-in-the-middle attack	حمله تلاقی در میان	حمله‌ای که در آن مهاجم سعی می‌کند با داشتن تکه‌ای از متن رمز شده و متن اصلی متناظر با آن و نیز با تشکیل جداول تطبیق کلید، کلید رمزنگاری را بیابد
memory-based silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی حافظه مینا	مت. تفت سیلیکونی حافظه مینا
message authentication code (MAC)	کد احراز اصالت پیام، کد اصالت‌سنجی پیام (کاپ)	دسته‌ای از توابع فیزیکی تکثیرناپذیر سیلیکونی که خروجی آن‌ها از طریق اندازه‌گیری تغییرات آن مشخصه‌های تصادفی که بین افزاره‌های سیلیکونی مشابه در عناصر حافظه‌های دو حالتی وجود دارد به دست می‌آید
message digest	چکیده پیام	نوعی جمع‌آزمای رمزنگاشتی مبتنی بر رمزنگاری متقارن برای کشف تغییرات رخ-داده بر روی داده‌ها، اعم از عمدی یا تصادفی
minimum disclosure proof	اثبات کم‌تراوا مت. اثبات کمینه‌افشا	نسخه فشرده شده یک پیام اصلی که با استفاده از خوارزمی / الگوریتم چکیده‌ساز تولید می‌شود
mirror attack syn. reflection attack	حمله بازتابی	نوعی روش اثبات در رمزنگاری که در آن اثبات‌کننده بدون هیچ شبهه‌ای می‌تواند واریسی‌کننده را به صحت اطلاعات خود متقاعد کند به طریقی که واریسی‌کننده نتواند از محتوای این اطلاع باخبر شود
miss in the middle attack	حمله بی‌تلاقی در میان	نوعی حمله تکرار که در آن مهاجم با قطع ارتباط، پیام ارسالی توسط یکی از دو طرف ارتباط را به خود او باز می‌گرداند
mix network syn. mixnet	شبکه مخلوط	روشی برای یافتن تفاضل‌های ناممکن در خوارزمی / الگوریتم رمز که ایده آن یافتن زوج‌متن‌هایی است که نتایج میانی حاصل از اعمال فرایند خوارزمی‌ها / الگوریتم‌های رمزگذاری و رمزگشایی بر روی آن‌ها با هم مطابقت ندارند

واژه بیگانه	معادل فارسی	تعریف
		سامانه‌ای برای گمنام‌سازی فرستندگان پیام با استفاده از عملیات رمزنگاشتی و جای‌گشتی در چند مرحله
mixnet Syn.mix network	شبکه مخلوط	سامانه‌ای برای گمنام‌سازی
		سامانه‌ای برای گمنام‌سازی فرستندگان پیام با استفاده از عملیات رمزنگاشتی و جای‌گشتی در چند مرحله
monoalphabetic cipher, monoalphabetic substitution cipher syn. simple substitution cipher	رمز جانشینی ساده	
		نوعی رمز جانشینی که در آن هر حرف متن اصلی جانشین یک حرف متناظر از الفبای رمز می‌شود
m-resilient	m-تابا	
		نوعی تابع بولی که حتی در صورت ثابت نگاه داشتن m متغیر ورودی آن، ویژگی توازن آن حفظ شود
mth order correlation-immune Boolean function	تابع بولی همبستگی‌ایمن مرتبه m	
		یک تابع بولی (نه لزوماً متوازن) که توزیع احتمال خروجی آن با ثابت نگه داشتن هر m بیت ورودی تغییر نکند
multi-designated verifiable signature	امضای چند وارس مشخص	
		نوع تعمیم‌یافته‌ای از امضای وارس مشخص که در آن واری امضا توسط گروهی مشخص که امضاکننده آن‌ها را تعیین می‌کند انجام‌پذیر است
multi proxy signature	امضای وکالتی چندگانه	
		نوعی امضای وکالتی آستانه‌ای که در آن شمار اعضای گروه و کلا با آستانه تعیین شده برابر است
multiset attack	حمله بیش مجموعه‌ای	
		حمله‌ای عام به رمزهای متقارن، که برخلاف حمله تفاضلی که در آن تنها رفتار یک زوج از متن‌های ورودی و خروجی توسط تحلیلگر مورد توجه قرار می‌گیرد، مجموعه‌ای بزرگتر و به دقت انتخاب شده مد نظر قرار می‌گیرد که بخش‌هایی از متن‌های ورودی آن تشکیل یک بیش مجموعه می‌دهند
multisignature	چندامضایی	
		نوعی امضای آستانه‌ای که در آن گمنامی امضاکنندگان حفظ نمی‌شود
multivariate public key cryptosystem	سامانه رمز کلید عمومی چندمتغیره	

واژه بیگانه	معادل فارسی	تعریف
		نوعی سامانه رمز کلید عمومی که امنیت آن مبتنی بر سخت بودن حل چند جمله‌ای‌های چند متغیره غیر خطی بر روی یک میدان متناهی است
N		
NLFSR Syn. nonlinear feedback shift register	ثاب غیر خطی مت. ثبات انتقال بازخوردی غیر خطی	نوعی ثبات انتقال بازخوردی که تابع بازخورد آن غیر خطی است
non-blind watermarking syn. private watermarking	ته نقش گذاری ناکور مت. ته نقش گذاری محرمانه	نوعی ته نقش گذاری که در آن برای آشکارسازی ته نقش، به کلید محرمانه فرستنده و پوشانه نیاز است
nonce	تک بار	عدد یا رشته ای عددی که برای مقابله با حمله تکرار، تنها یک بار در یک الگوریتم یا پروتکل (قرارداد) رمزنگاشتی به کار می‌رود
non-interactive zero-knowledge proof	اثبات ناتراوای غیر تعاملی مت. اثبات دانش صفر غیر تعاملی	روشی برای کاهش شمار دورها در یک اثبات ناتراوا با ارسال تنها یک پیام از طرف اثبات کننده به واریسی کننده همراه با تغییر مدل به طوری که یک رشته تصادفی مشترک مرجع در دسترس تمامی شرکت کنندگان در قرارداد قرار می‌گیرد و اثبات کننده یک تک پیام به واریسی کننده می‌فرستد
non-invasive attack	حمله غیرتهاجمی	حمله به سامانه‌های فیزیکی با بهره‌گیری از اطلاعات در دسترس، مانند زمان اجرا و مصرف توان، بدون نیاز به تخریب تراشه
nonlinear feedback shift register syn. NLFSR	ثبات انتقال بازخوردی غیر خطی مت. ثاب غیر خطی	نوعی ثبات انتقال بازخوردی که تابع بازخورد آن غیر خطی است

واژه بیگانه	معادل فارسی	تعریف
nonmalleability	چکش ناپذیری	خاصیت یک خوارزمی / الگوریتم که به موجب آن با داشتن متن رمز شده c_1 ، تولید یک متن رمز شده دیگر مانند c_2 ، با ارتباط معلوم بین متن های اصلی متناظر آنها امکان پذیر نباشد
non-transferable signature	امضای انتقال ناپذیر	نوعی امضای رقمی که تنها از طریق فرد مشخص شده توسط امضا کننده قابل واریسی است
O		
oblivious signature	امضای ناآگاهانه	نوعی امضای رقمی که در آن صاحب امضا بنا به درخواست یک متقاضی اقدام به امضای یک پیام از یک مجموعه پیام می کند، بدون آنکه قادر به تشخیص پیام مزبور از بین مجموعه پیام ها باشد یا یک پیام را با استفاده از یکی از کلیدهای خصوصی خود، بدون تشخیص آن کلید امضا می کند
oblivious transfer	انتقال ناآگاهانه	قراردادی (پروتکلی) بین فرستنده و گیرنده که براساس آن فرستنده اقدام به ارسال برخی از اطلاعات برای گیرنده می کند، بدون آنکه بداند گیرنده چه اطلاعاتی دریافت کرده است
one-more forgery	جعل امضای یکی بیش	نوعی حمله که در آن مهاجم با در اختیار داشتن n زوج پیام و امضا، به دنبال جعل امضا بر روی پیام $n+1$ ام است
one-time pad cipher syn. vernam cipher	رمز یک بار مصرف	رمزی که در آن از کلید رمز تنها یک بار استفاده می شود به طوری که هر حرف یا نماد کلید برای رمز کردن یک نماد متن اصلی به کار می رود
one-way function	تابع یک طرفه	یک تابع ریاضی که محاسبه آن ساده، اما محاسبه وارون آن بسیار دشوار باشد
original signer	امضا کننده اصلی	

واژه بیگانه	معادل فارسی	تعریف
		هستاری که حق امضای خود را به هستاری دیگر به عنوان امضاکننده و کالتهی واگذار می کند
out-of-band authentication abbr.: OOB	احراز اصالت فراباندی مت. اصالت سنجی فراباندی (افراب)	فرایندی برای احراز اصالت، مبتنی بر دو نشانک مختلف که از دو شبکه یا مسیر متفاوت ارسال می شوند
output feedback mode	شیوه بازخورد خروجی	یکی از روش های به کارگیری رمز قالبی که به کارگیری آن، عملکردی مشابه با رمزهای جریان را فراهم می سازد.
P		
pairing	زوج نگاشت	نگاشتی مانند $e: G_1 \times \overline{G_2} \rightarrow G_t$ با ویژگی های دوخطی بودن، و ناتباهیدگی (non-degeneracy) و محاسبه پذیری
partial preimage resistance	مقاومت در برابر پیش تصویر جزئی	خصوصیتی در توابع چکیده ساز که باعث می شود حتی با معلوم بودن بخش بزرگی از ورودی، بازیابی بخش باقیمانده ورودی دشوار باشد
partial signature	پارامضا	نوعی امضای رقمی که در آن با تولید بخشی از امضا، که تکمیل آن تنها توسط امضاکننده میسر است، گمنامی یک کاربر در میان مجموعه ای از کاربران، بدون نیاز به اطلاعات سایر کاربران، تأمین می شود
passive adversary	مهاجم غیرفعال	مهاجمی که فقط با جست و جوی تمام اطلاعات قابل دسترس برخی طرف های قرارداد و بدون تغییر دادن آنها، سعی در فهم اطلاعات ورودی طرف های امین دارد
passive cheater	فریب دهنده غیرفعال	فریب دهنده ای که قرارداد را اجرا می کند، ولی سعی می کند اطلاعاتی بیش از آنچه در قرارداد آمده است به دست آورد
passive eavesdropper	شنودگر غیرفعال	شنودگری که فقط می تواند متن رمز شده را بخواند یا گوش دهد

واژه بیگانه	معادل فارسی	تعریف
passive penetration test	آزمون نفوذ غیرفعال	آزمونی برای کاوش مرزهای محدوده هدف و بررسی ضعف‌های امنیتی در محیط هدف بدون قصد بهره‌گیری از دسترسی و بدون تأثیر منفی بر عملکرد عادی آن
passive wiretapping	خط‌شنود انفعالی	پایش یا ضبط داده‌هایی که با یک خط ارتباطی ارسال می‌شوند، بی‌آنکه تغییری در آنها ایجاد شود
penetration test syn.: penetration testing	آزمون نفوذ	نوعی روش آزمون که در آن ارزیاب‌ها با استفاده از همه مستندات در دسترس (مانند طراحی سامانه، کد منبع، کتابچه‌های راهنما) و تحت محدودیت‌های خاص، سعی در دور زدن ویژگی‌های امنیتی یک سامانه اطلاعاتی دارند
perfect forward secrecy	رازمانی پیش‌سوی کامل	خصوصیتی در طرح‌های تبادل کلید که بنا بر آن افشای کلید اصلی، که از آن برای تولید کلیدهای نشست استفاده می‌شود، امنیت کلید نشست‌های پیشین را تهدید نکند
perfect zero-knowledge proof	اثبات ناتراوای کامل، اثبات دانش صفر کامل	روشی که در آن مقدار اطلاعاتی که از اثبات‌کننده به واریسی‌کننده نیست می‌کند برابر با صفر است. این نوع اثبات در قراردادهای توافق کلید و طرح‌های رمزگذاری (encryption schemes) و امضاهای رقمی به کار می‌رود
perfectly secure steganography	نهان‌نگاری کاملاً امن	نوعی خوارزمی / الگوریتمی نهان‌نگاری که احتمال موفقیت مهاجمی با قدرت محاسباتی نامحدود برای یافتن تمایز بین پوشانه و نهانه آن صفر است
physical attack	حمله فیزیکی	حمله‌ای به افزاره‌های رمزنگاشتی، مبتنی بر ابزارهای فیزیکی
physical unclonable function (PUF)	تابع فیزیکی تکثیرناپذیر (تفت)	تابعی مبتنی بر پیچیدگی بسیار زیاد ساختار یک سامانه فیزیکی، برای نگاشت مجموعه‌ای از چالش‌ها به مجموعه‌ای از پاسخ‌ها
plaintext syn. clear text/ cleartext	متن آشکار متن اصلی	

متنی که اطلاعات یا محتوای آن رمزگذاری نشده و به راحتی قابل فهم است

plaintext-ciphertext compromise مخاطره کلید متن اصلی - متن رمز

لو رفتن اطلاعات کلید با در اختیار داشتن یک زوج متن اصلی و متن رمز متناظر با آن

plaintext-plaintext compromise مخاطره کلید متن اصلی - متن اصلی

لو رفتن اطلاعات کلید که از تحلیل داده های حاصل از رمزگذاری دو متن اصلی P1 و P2 با یک کلید حاصل می شود

polyalphabetic cipher

syn. polyalphabetic encryption

syn. polyalphabetic substitution cipher

رمز چند الفبایی

مت. رمز جانشینی چند الفبایی

نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می شود و هر جانشینی با یک عنصر از کلید مشخص می شود

polyalphabetic encryption

syn. polyalphabetic cipher

syn. polyalphabetic substitution cipher

رمز چند الفبایی

مت. رمز جانشینی چند الفبایی

نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می شود و هر جانشینی با یک عنصر از کلید مشخص می شود

polyalphabetic substitution cipher

syn.: polyalphabetic encryption

syn. polyalphabetic cipher

رمز جانشینی چند الفبایی

مت. رمز چند الفبایی

نوعی رمزگذاری که در آن هر حرف متن اصلی جانشین بیش از یک حرف از الفبای رمز می شود و هر جانشینی با یک عنصر از کلید مشخص می شود

polygram substitution cipher

رمز جانشینی چند نویسه ای

نوعی رمز جانشینی که در آن قالب هایی از حروف متن اصلی جانشین قالب های متناظر در حروف متن رمز می شوند

polygraphic substitution cipher

رمز جانشینی چندنگاره ای

نوعی رمزگذاری جانشینی که در آن هر حرف متن اصلی جانشین دو یا چند حرف از الفبای متن رمز می شود

polynomial time algorithm

الگوریتم زمان چند جمله ای /

خوارزمی زمان چند جمله ای

واژه بیگانه	معادل فارسی	تعریف
		الگوریتم / خوارزمی ای که زمان اجرای آن تابعی چندجمله‌ای از طول ورودی آن است
port scanner syn. vulnerability scanner	پویشگر درگاه مت. پویشگر آسیب پذیری	برنامه‌ای رایانه‌ای که برای ارزیابی ضعف‌های امنیتی سامانه‌های رایانه‌ای و شبکه‌ها و برنامه‌های کاربردی یا نرم‌افزاری طراحی شده است
power analysis attack syn. simple power analysis attack syn. power consumption attack	حمله تحلیل توانی	حمله‌ای که در آن مهاجم با اندازه‌گیری توان مصرفی یک ابزار رمزنگاشتی در خلال عملیات رمزنگاشتی، می‌تواند به جزئیات مشخصه‌های اصلی آن و پیاده‌سازی خوارزمی / الگوریتم رمز دست یابد
power consumption attack syn. power analysis attack syn. simple power analysis attack	حمله تحلیل توانی	حمله‌ای که در آن مهاجم با اندازه‌گیری توان مصرفی یک ابزار رمزنگاشتی در خلال عملیات رمزنگاشتی، می‌تواند به جزئیات مشخصه‌های اصلی آن و پیاده‌سازی خوارزمی / الگوریتم رمز دست یابد
preimage resistance syn. first-preimage resistance	مقاومت در برابر پیش‌تصویر مت. مقاومت در برابر پیش‌تصویر اول	یکی از خصوصیات مطلوب در توابع چکیده‌ساز که باعث می‌شود به‌ازای هر یک از مقادیر خروجی یک تابع چکیده‌ساز، یافتن دست‌کم یک ورودی که به آن مقدار خروجی تصویر شود، از نظر محاسباتی عملی نباشد
primitive element	عنصر اولیه	عضوی از مرتبه n مانند g در G ، یک گروه (ضربی) متناهی n عضوی، به‌گونه‌ای که هر عنصر ناصفر گروه را بتوان به شکل توان صحیحی از g مانند g^t نمایش داد
primitive polynomial	چندجمله‌ای اولیه	یک چندجمله‌ای یکین از درجه m ، مانند f بر روی میدان F_q که $f(0) \neq 0$ و مرتبه آن برابر با $q^m - 1$ باشد
primitive root	ریشه اولیه	مولد یک گروه ضربی به پیمانه یک عدد صحیح n
private key cryptography syn. secret key cryptography	رمزنگاری با کلید مخفی	

واژه بیگانه	معادل فارسی	تعریف
		مهاجمی با توانایی اجرای الگوریتم‌ها/خوارزمی‌های زمان چندجمله‌ای احتمالاتی
probabilistic polynomial-time algorithm	الگوریتم زمان چندجمله‌ای احتمالاتی / خوارزمی زمان چندجمله‌ای احتمالاتی	
		مهاجمی با توانایی اجرای الگوریتم‌ها/خوارزمی‌های زمان چندجمله‌ای احتمالاتی
probabilistic public-key encryption	رمزگذاری احتمالاتی با کلید عمومی	
		نوعی خوارزمی/الگوریتم رمزگذاری با کلید عمومی که در آن هر بار عمل رمزگذاری یک پیام با استفاده از یک کلید ثابت، به تولید متن‌های رمز متفاوت می‌انجامد
processing complexity	پیچیدگی پردازشی	
		زمان لازم برای انجام یک حمله
product cipher syn. superencryption	رمز ترکیبی مت. آبررمزگذاری	
		رمزی که از ترکیب دو یا چند تابع رمزگذاری مختلف ساخته می‌شود
protected proxy signature	امضای وکالتی حفاظت‌شده	
		نوعی امضای وکالتی که در تولید کلید امضا هم وکیل و هم موکل نقش دارند؛ و در نتیجه موکل نمی‌تواند به جای وکیل به صورت وکالتی امضا کند
provable security	امنیت اثبات‌پذیر	
		امنیت یک سامانه رمزنگاری که بتوان الزامات امنیتی آن را در یک مدل مهاجمی به شکل صوری بیان کرد
proxy blind signature	امضای کور وکالتی	
		نوعی امضا که در آن وکیل، با استفاده از کلید امضای وکالتی، یک پیام کور را برای درخواست‌کننده امضا می‌کند
proxy resignation	بازامضای وکالتی	
		نوعی امضا که در آن وکیلی نسبتاً معتمد، امضای یک نهاد بر روی یک پیام مشخص را به امضای نهاد دیگر بر روی همان پیام تبدیل می‌کند؛ در حالی که این وکیل قادر به تولید امضا بر روی پیام‌های دلخواه از سوی هیچ کدام از نهادها نیست

واژه بیگانه	معادل فارسی	تعریف
proxy ring signature	امضای حلقوی و کالتی	نوعی امضای و کالتی که در آن موکل به گروهی از وکلا برای تولید امضا و کالت می‌دهد، به طوری که هویت امضاکننده (وکیل) از دید مهاجم و حتی امضاکننده اصلی مخفی بماند
proxy signature syn. public key proxy signature	امضای و کالتی	نوعی امضای رقمی با قابلیت واگذاری حق امضا از سوی امضاکننده اصلی به وکیل، به صورت کارا و شفاف
proxy signer	امضاکننده و کالتی	نوعی امضای رقمی با قابلیت واگذاری حق امضا از سوی امضاکننده اصلی به وکیل، به صورت کارا و شفاف
pseudorandom function	تابع شبه تصادفی	یک تابع تعینی برحسب یک کلید و ورودی که از یک تابع واقعاً تصادفی برحسب ورودی تمایزناپذیر است
pseudorandom number generator (PRNG)	مولد اعداد شبه تصادفی	مولدی که پس از مقداردهی اولیه با هر مقدار تصادفی (به نام بذر) دنباله‌ای شبیه به یک دنباله تصادفی را تولید می‌کند، به طوری که یک ناظر بدون اطلاع از مقدار بذر نتواند دنباله مزبور را از دنباله تولیدشده توسط یک مولد واقعاً تصادفی تمیز دهد
public-key cryptography syn. asymmetric cryptography	رمزنگاری با کلید عمومی مت: رمزنگاری نامتقارن	روشی برای رمزگذاری پیام که در آن از کلید عمومی و کلید مخفی استفاده می‌شود: کلید عمومی برای رمزگذاری و کلید مخفی برای رمزگشایی
public key proxy signature syn. proxy signature	امضای و کالتی	نوعی امضای رقمی با قابلیت واگذاری حق امضا از سوی امضاکننده اصلی به وکیل، به صورت کارا و شفاف
public-key infrastructure	زیرساخت کلید عمومی	

مجموعه‌ای از خط‌مشی‌ها و فن‌آوری‌های مبتنی بر رمزنگاری کلید عمومی که برای احراز اصالت و صدور گواهی و محرمانگی و امضای رقمی به کار می‌رود

public-key stegosystem

سامانه نهمان‌نگاری کلید عمومی

سامانه‌ای شامل سه الگوریتم/خوارزمی احتمالاتی تولید کلید و کدگذاری (درج) و کدگشایی (آشکارسازی) که در آن الگوریتم/خوارزمی تولید کلید پارامتر امنیتی را به عنوان ورودی دریافت و یک زوج کلید خصوصی و عمومی نهمان‌نگاری را تولید می‌کند و الگوریتم/خوارزمی کدگذاری با به کارگیری کلید عمومی، نهمانه را تولید، و الگوریتم/خوارزمی کدگشایی با استفاده از کلید خصوصی نهمانه را کدگشایی می‌کند

public-key watermarking
syn.asymmetric watermarkingته‌نقش‌گذاری کلید عمومی
مت. ته‌نقش‌گذاری نامتقارن

نوعی روش ته‌نقش‌گذاری که در آن فرستنده ته‌نقش را با استفاده از کلید خصوصی (مشابه تولید امضای دیجیتال) ایجاد می‌کند و هر هستار کدگشا که به کلید عمومی متناظر دسترسی داشته باشد می‌تواند ته‌نقش مربوط را آشکار و بازشناسی کند

Q

quantum cryptography

رمزنگاری کوانتومی

رمزنگاری با استفاده از قوانین مکانیک کوانتومی

quantum deniable authentication

احراز اصالت انکارپذیر کوانتومی
مت. اصالت‌سنجی انکارپذیر کوانتومی

نوعی احراز اصالت اتکارپذیر مبتنی بر تبدیل یکانی و تابع یک‌طرفه کوانتومی

R

random oracle model

مدل پیشگوی تصادفی

روشی مبتنی بر استفاده از یک تابع ریاضی برای اثبات امنیت یک طرح رمزنگاشتی که در اختیار تمام کاربران، اعم از عادی و مهاجم، قرار داشته و به صورت تصادفی به هر ورودی مقدار خروجی صحیحی را نسبت می‌دهد

receiver deniable encryption

رمزگذاری گیرنده‌انکارپذیر

نوعی رمزگذاری که در آن گیرنده بتواند دریافت پیام رمز شده را انکار کند

recipient anonymity

گمنامی گیرنده

واژه بیگانه	معادل فارسی	تعریف
		در یک سامانه پیام، عدم امکان شناسایی گیرنده پیام از طریق شنود
re-encryption mixnet	شبکه مخلوط با رمزگذاری	نوعی شبکه مخلوط که در آن ورودی‌های هر مرحله با استفاده از یک کلید عمومی مشترک رمزگذاری می‌شوند
reflection attack syn. mirror attack	حمله بازتابی	نوعی حمله تکرار که در آن مهاجم با قطع ارتباط، پیام ارسالی توسط یکی از دو طرف ارتباط را به خود او باز می‌گرداند
rekeying	کلیدگذاری مجدد	روند تغییر کلید رمزگذاری در بخش‌های باقی‌مانده یک متن در حال رمزی شدن برای محدود کردن حجم داده‌های رمزگذاری شده با کلید پیشین
related key attack	حمله کلید مرتبط	حمله‌ای که در آن مهاجم با اطلاع از رابطه بین چند کلید و دسترسی به توابع رمزگذاری متناظر در پی یافتن کلید است
related-key cryptanalysis	تحلیل رمز کلید مرتبط	نوعی تحلیل رمز مشابه با تحلیل تفاضلی رمز که در آن تفاضل بین کلیدها بررسی می‌شود
relay attack	حمله بازرسانی	نوعی حمله فرد در میان که در آن فرد مهاجم در نقش طرف اول، با طرف دوم ارتباط برقرار می‌کند و پاسخ طرف اول را بدون دستکاری یا حتی خواندن آن برای طرف دوم ارسال می‌کند تا با معرفی خود به جای طرف اول به هدف حمله دست یابد
replay attack syn. freshness attack	حمله تکرار	حمله‌ای با هدف نقض تازگی پیام، که در آن مهاجم پیامی را که در اجرای قبلی قرارداد احراز اصالت ذخیره کرده است، در اجرای جدید آن تکرار می‌کند
resettable zero-knowledge proof	اثبات ناتراوای باز نشان‌پذیر، مت. اثبات دانش صفر باز نشان‌پذیر	نوعی روش اثبات دانش صفر که حتی در صورت تعامل چندباره مهاجم با اثبات‌کننده، هر بار با بازنشانی اثبات‌کننده به حالت اولیه و وادار کردن او به استفاده از همان نوار تصادفی (random tape)، همچنان ناتراوا باقی بماند

واژه بیگانه	معادل فارسی	تعریف
resiliency order	مرتبه تابایی	بیشینه مقدار m که به ازای آن تابع f ، m -پایدار باشد
ring signature	امضای حلقوی	نوعی امضای رقمی که در آن یک کاربر می‌تواند، بدون افشای نام خود، از سوی گروهی از کاربران اقدام به تولید امضا کند و برخلاف امضای گروهی، به یک نهاد مرکزی مورداعتماد نیاز ندارد
run	ریسه	بیت‌های یکسان متوالی در یک دنبالهٔ دودویی که با بیت‌های پیش و پس از خود متفاوت باشند
running-key syn. keystream/ key stream/ key-stream	کلید جریانی مت. جریان کلید	دنباله‌ای که در رمزهای جریانی نماد به نماد با دنبالهٔ متن ساده ترکیب می‌شود تا دنبالهٔ متن رمز به دست آید
S		
second-preimage attack	حمله به پیش‌تصویر دوم	حمله‌ای که در آن مهاجم یک پیام تصادفی انتخاب می‌کند و امیدوار است که چکیدهٔ مفروضی به دست آورد
second-preimage resistance syn. weak collision resistance	مقاومت در برابر پیش‌تصویر دوم مت. برخوردتایی ضعیف	یکی از خصوصیات توابع چکیده‌ساز، که در صورت وجود آن، با در اختیار داشتن m_1 ، یافتن m_2 به طوری که $hash(m_1) = hash(m_2)$ دشوار باشد
secret handshake	دست‌داد سری	طرحی برای شناسایی متقابل اعضای یک گروه به گونه‌ای که: الف) افراد خارج از گروه قادر به شناسایی اعضای گروه نباشند، ب) افراد خارج از گروه نتوانند خود را به‌عنوان یکی از اعضای گروه به دیگر اعضای گروه معرفی کنند
secret key	کلید مخفی	

واژه بیگانه	معادل فارسی	تعریف
		کلیدی که از آن در رمزنگاری متقارن استفاده می‌شود
secret key cryptography syn.private key cryptography, symmetric cryptography	رمزنگاری با کلید مخفی مت. رمزنگاری متقارن	
		روشی برای رمزگذاری پیام که در آن برای رمزگذاری و رمزگشایی تنها از یک کلید استفاده می‌شود
secret sharing scheme	طرح تسهیم راز	
		به اشتراک گذاشتن اطلاعات محرمانه میان تعدادی شرکت‌کننده به طوری که زیرمجموعه مشخصی از آنها قادر به بازیابی آن اطلاعات باشند درحالی که سایر اعضا قادر به درک هیچ گونه اطلاعات مرتبط با آن نباشند
secure socket layer (SSL)	لایه اتصال امن (لام)	قراردادی برای ایجاد ارتباط امن در اینترنت
security association	همایند امنیتی	رابطه‌ای بین دو یا چند هستار که آنها را قادر به حفاظت از داده‌هایی می‌کند که بین آنها مبادله شده است
security specifications	مشخصات امنیتی	شرح دقیق حفاظ‌های موردنیاز برای حفاظت از یک سامانه اطلاعاتی
security strength	استحکام امنیتی	تعداد عملیات موردنیاز برای شکستن یک الگوریتم/خوارزمی یا سامانه رمزنگاشتی
security tag	برچسب امنیتی	واحد اطلاعاتی که اطلاعات مرتبط امنیتی معینی را نمایش می‌دهد
security target	هدف امنیتی	مشخصات معیارهای مشتری که نشان‌دهنده مجموعه‌ای از نیازمندی‌های امنیتی است و بر مبنای آن ارزیابی امنیتی انجام می‌شود
seed key	بذر کلید	کلید اولیه‌ای که برای شروع فرایند تولید یا به‌روزرسانی کلید به کار گرفته می‌شود

واژه بیگانه	معادل فارسی	تعریف
selective forgery	جعل امضای انتخابی	حمله‌ای علیه طرح‌های امضای رقمی که در آن مهاجم با انتخاب حداقل یک پیام بتواند امضای آن را جعل کند
semantic security	امنیت معنایی	عدم نشت هرگونه اطلاعات از متن رمز شده در مورد متن اصلی، فارغ از توان مهاجم و مستقل از معنای نهفته در رمز گذاری
semi-invasive attack	حمله نیم‌تهاجمی	نوعی حمله به سامانه‌های فیزیکی که از نظر عملکرد در رده‌ای بین حملات تهاجمی و غیرتهاجمی قرار می‌گیرد
sender anonymity	گمنامی فرستنده	در یک سامانه پیام، عدم امکان شناسایی فرستنده پیام از طریق شنود
sender deniable encryption syn. deniable encryption	رمز گذاری فرستنده‌انکارپذیر مت. رمز گذاری انکارپذیر	نوعی رمز گذاری که در آن فرستنده بتواند در صورت لزوم رمز گذاری پیام ارسال شده را انکار کند
session key	کلید نشست	کلیدی که از آن برای رمز گذاری متقارن در یک نشست استفاده و سپس آن را نابود می‌کنند
signatory	صاحب‌امضا	شخص یا کشور یا نهادی که با داشتن زوج کلید عمومی و خصوصی مجاز به امضای رقمی یک معاهده یا سند رسمی است؛ این امضا با کلید خصوصی تولید و با کلید عمومی واریسی می‌شود و تعهداتی را برای طرفین ایجاد می‌کند
signature validation	اعتبارسنجی امضا	درستی‌سنجی یک امضای رقمی، به صورت ریاضی، و کسب اطمینان لازم از اعتبار کلید عمومی، مالکیت کلید خصوصی و غیره
signature verification	درستی‌سنجی امضا مت. واریسی امضا	

واژه بیگانه	معادل فارسی	تعریف
		استفاده از یک الگوریتم/خوارزمی امضای رقمی و یک کلید عمومی برای تعیین درستی یک امضا
signcryption	رمز امضا	انجام هم‌زمان امضای رقمی و رمزگذاری مثل رمزنگاری با کلید عمومی
signee syn. signatory	امضاصاحب	شخص یا کشور یا نهادی که با داشتن زوج کلید عمومی و خصوصی مجاز به امضای رقمی یک معاهده یا سند رسمی است؛ این امضا با کلید خصوصی تولید و با کلید عمومی واری می‌شود و تعهداتی را برای طرفین ایجاد می‌کند
signer	امضاکننده	هستاری که متن یا محتوای رقمی را امضا می‌کند
silicon PUF	تابع فیزیکی تکثیرناپذیر سیلیکونی / تفت سیلیکونی	دسته‌ای اصلی از توابع فیزیکی تکثیرناپذیر الکترونیکی که در تراشه‌های سیلیکونی تعبیه می‌شوند
simple power analysis attack syn. power analysis attack syn. power consumption attack	حمله تحلیل توانی ساده مت. حمله تحلیل توانی	حمله‌ای که در آن مهاجم با اندازه‌گیری توان مصرفی یک ابزار رمزنگاشتی در خلال عملیات رمزنگاشتی، می‌تواند به جزئیات مشخصه‌های اصلی آن و پیاده‌سازی خوارزمی/الگوریتم رمز دست یابد
simple substitution cipher syn.: monoalphabetic cipher, monoalphabetic substitution cipher	رمز جانشینی ساده	نوعی رمز جانشینی که در آن هر حرف متن اصلی جانشین یک حرف متناظر از الفبای رمز می‌شود
slide attack	حمله لغزشی	حمله‌ای عام (attack generic) به رمزهای تکراری که در آن از رابطه بین یک کلید با خودش بهره‌برداری می‌شود
software attack	حمله نرم‌افزاری	هر نوع حمله از طریق رخنه‌های موجود در نرم‌افزار با استفاده از یک کانال ارتباطی عادی
space complexity	پیچیدگی حافظه‌ای	

واژه بیگانه	معادل فارسی	تعریف
		پیچیدگی محاسباتی یک الگوریتم/خوارزمی به لحاظ حافظه مورد نیاز برای اجرای آن
square attack	حمله مربعی	نوعی حمله بیش مجموعه‌ای که اولین بار حین تحلیل رمز مربع شناسایی شد و در آن تحلیل‌گر به جای مطالعه رفتار یک زوج از متن‌های اصلی، مجموعه بسیار بزرگ‌تری از متن‌های رمز را بررسی می‌کند که در آن بخش‌هایی از متن ورودی، تشکیل یک بیش مجموعه می‌دهند
static adversary	مهاجم ایستا	مهاجمی که در ابتدای اجرای قرارداد تصمیم بگیرد که به کدام طرف قرارداد حمله کند
static group signature	امضای گروهی ایستا	نوعی امضای گروهی که در آن به‌روزرسانی کلید عمومی گروه در صورتی ضروری است که یک یا چند عضو به گروه بپیوندند یا آن را ترک کنند، یا زوج کلیدهای اختصاصی یک یا چند عضو به‌روزرسانی شوند
static keys	کلیدهای ایستا	کلیدهایی که طول عمر نسبتاً زیادی دارند و در تعدادی از اجراهای یک الگوریتم/خوارزمی مشترک هستند
statistical zero-knowledge proof	اثبات ناتراوی آماری، اثبات دانش صفر آماری	
syn.almost-perfect knowledge	zero- مت. اثبات ناتراوی تقریباً کامل، اثبات دانش صفر تقریباً کامل	
		اثباتی که در آن، برخلاف حالت‌های کلی اثبات‌ناتراوا، توزیع مکالمات واقعی با توزیع مکالمات شبیه‌سازی‌شده از نظر آماری تمایزناپذیر است؛ یعنی فاصله آماری میان توزیع‌ها ناچیز است
statistically secure steganography	نهان‌نگاری آماری‌امن	
		نوعی خوارزمی/الگوریتمی نهان‌نگاری که مهاجم با قدرت محاسباتی نامحدود تنها بتواند در آن تمایز ناچیزی بین پوشانه و نهانه پیدا کند
steganalysis	نهان‌شکنی	
		دانش و فن یافتن داده‌هایی که با استفاده از نهان‌نگاری پنهان شده است
stegosystem	سامانه نهان‌نگاری	

واژه بیگانه	معادل فارسی	تعریف
stegotext	نهانه	سامانه‌ای شامل سه خوارزمی / الگوریتم تولید کلید و کدگذاری و کدگشایی نهان‌نگاشتی که ورودی آن شامل مؤلفه‌های بیتی و پوشانه و پیامی است که باید نهفته شود و خروجی آن نهانه است
still imagery steganography	نهان‌نگاری تصویرسازکن	پیغامی که از درج داده‌های پیغام محرمانه در داخل داده‌های پوشانه ایجاد می‌شود
storage complexity	پیچیدگی انبارشی	بنهان کردن پیام محرمانه در داخل تصاویر رقمی
stream cipher	رمز جریانی	ظرفیت انباره مورد نیاز برای انجام یک حمله
strict avalanche criterion	معیار بهمنی اکید	نوعی رمز متقارن که در آن با تولید رشته‌ای از بیت‌ها به نام جریان کلید و ترکیب آن با متن اصلی رمزگذاری انجام می‌شود
strong designated verifier signatures	امضای وارس مشخص قوی	نوعی معیار بهمنی برای ارزیابی توابع بولی که با تغییر هر بیت در ورودی این توابع هر یک از بیت‌های خروجی با احتمال یک‌دوم تغییر یابد
strong PUF	تابع فیزیکی تکثیرناپذیر قوی / تفت قوی	نوعی امضای وارس مشخص با دو ویژگی جعل‌ناپذیری و واری‌ناپذیری عمومی که در آن تولید امضا تنها توسط امضاکننده اصلی و واری‌ناپذیری امضا تنها توسط وارس تعیین شده امکان‌پذیر باشد
subset sum problem	مسئله جمع زیرمجموعه‌ها	نوعی تابع فیزیکی تکثیرناپذیر غیرقابل پیش‌بینی، با تعداد بسیار زیاد چالش و دسترسی واپایش نشده مهاجم به آن
		مسئله یافتن زیرمجموعه‌ای از یک مجموعه اعداد صحیح مثبت، که حاصل جمع اعضای آن برابر با یک عدد مشخص باشد

واژه بیگانه	معادل فارسی	تعریف
substitution cipher	رمز جانشینی	روشی ابتدایی برای رمزگذاری یک پیام که از طریق آن می‌توان یک حرف متن اصلی را جانشین یک و فقط یک حرف از الفبای رمز کرد.
substitution-permutation network (SPN)	شبکه جانشینی-جایگشتی	رمز ترکیبی متشکل از تعدادی مرحله که هر یک شامل توابع جانشینی و جایگشتی هستند
superencryption syn. product cipher	آبرمزگذاری مت. رمز ترکیبی	رمزی که از ترکیب دو یا چند تابع رمزگذاری مختلف ساخته می‌شود
superincreasing knapsack syn. superincreasing knapsack problem	کوله پستی آبرافزایی مت. مسئله کوله پستی آبرافزایی	نوعی مسئله کوله پستی که در آن اعضای مجموعه اعداد صحیح، یک دنباله آبرافزایی باشند
superincreasing knapsack problem syn. superincreasing knapsack	مسئله کوله پستی آبرافزایی مت. کوله پستی آبرافزایی	نوعی مسئله کوله پستی که در آن اعضای مجموعه اعداد صحیح، یک دنباله آبرافزایی باشند
superincreasing sequence	دنباله آبرافزایی	برداری که مقدار هر مؤلفه‌اش از مجموع مقادیر مؤلفه‌های پیشین آن بزرگ‌تر باشد
Sybil attack	حمله سی‌بل / حمله چندشناسه‌ای	نوعی حمله در شبکه‌های همتابه‌همتا (peer-to-peer networks) که در آن یک گره از شبکه هم‌زمان با چندین شناسه به‌طور فعال عمل می‌کند
symmetric cryptography syn. secret key cryptography, private key cryptography	رمزنگاری متقارن مت. رمزنگاری با کلید مخفی	روشی برای رمزگذاری پیام که در آن برای رمزگذاری و رمزگشایی تنها از یک کلید استفاده می‌شود

T

threshold authentication code کد احراز اصالت پیام آستانه‌ای، کد

واژه بیگانه	معادل فارسی	تعریف
	اصالت‌سنجی پیام آستانه‌ای اختصار: کاپ آستانه‌ای	نوعی کد احراز اصالت پیام (کاپ) که برای تولید آن حضور حداقل تعداد مشخصی از شرکت‌کنندگان ضروری است
threshold cryptography	رمزنگاری آستانه‌ای	نوعی رمزنگاری که کلید آن در میان شماری از افراد مجاز تسهیم می‌شود و برای رمزگشایی، حضور حداقل مشخصی از آن افراد برای دستیابی به کلید لازم است
threshold decryption	رمزگشایی آستانه‌ای	قراردادی که برای هر زیرمجموعه t ، عضوی از یک مجموعه n عضو از هستارها یا کارسازها، امکان رمزگشایی یک متن رمز شده را فراهم می‌سازد، در حالی که مانع از رمزگشایی پیام مزبور توسط هر زیرمجموعه با کمتر از t عضو می‌شود
threshold proxy signature	امضای وکالتی آستانه‌ای	نوعی امضا که در آن صاحب امضا حق امضای خود را به گروهی مشخص از وکلا واگذار می‌کند؛ به طوری که هر زیرمجموعه با حداقل اندازه از قبل تعیین شده (آستانه)، قادر به تولید یک امضای وکالتی معتبر از سوی وی باشد در حالی که زیرمجموعه‌های با تعداد کمتر از آستانه تعیین شده قادر به انجام این کار نباشند
threshold signature	امضای آستانه‌ای	نوعی امضای رقمی که در آن مجموعه‌ای از امضاکنندگان می‌توانند گروه‌هایی را تشکیل دهند که در آن، زیرمجموعه‌هایی معین از اعضا قادر به انجام امضا از طرف کل گروه باشند
time complexity	پیچیدگی زمانی	پیچیدگی محاسباتی یک الگوریتم/خوارزمی به لحاظ زمان مورد نیاز برای اجرای آن
time-memory trade-off attack	حملهٔ بده‌بستان زمان - حافظه	اگر پیچیدگی یافتن کلید برابر با K باشد، در حملهٔ بده‌بستان زمان - حافظه می‌توان کلید را در T مرحله (زمان) با M کلمه از حافظه به دست آورد که در آن $K = T \times M$
time-memory-data trade-off attack	حملهٔ بده‌بستان زمان - حافظه - داده	حمله‌ای که در آن مهاجم قادر به انجام جست‌وجوی فراگیر نیست، اما با جست‌وجوی بخش کوچکی از فضای کلید، سعی می‌کند یک رشته کلید اجرایی معلوم تولید کند و افزایش طول رشته منجر به افزایش احتمال موفقیت مهاجم در انجام حمله می‌شود

واژه بیگانه	معادل فارسی	تعریف
time stamp	مهر زمانی	مجموعه‌ای از نویسه‌ها یا اطلاعات رمز گذاری شده که زمان وقوع یک رویداد خاص را مشخص می‌کند
time-stamping	مهر زنی زمانی	فرایندی برای واریسی زمان ایجاد یا آخرین ویرایش یک سند رقمی به هنگام تولید یا ذخیره یا تغییر برخط داده‌های آن سند که در حالت مطلوب فقط به داده‌های سند بستگی دارد و در برابر دستکاری داده‌ها یا زمان و تاریخ مقاوم است
timing attack	حمله تحلیل زمانی	حمله‌ای که در آن دشمن با تحلیل زمان اجرای خوارزمی / الگوریتم رمز سعی در یافتن بیت‌های کلید یا اطلاعات مخفی دیگر دارد
tractable problems	مسائل مهار پذیر	مسائلی که معمولاً به‌ازای ورودی‌هایی با اندازه معقول و با استفاده از الگوریتم‌ها/خوارزمی‌های زمان چندجمله‌ای در یک زمان مناسب قابل حل هستند
transitive signature	امضای ترا گذر، امضای ترا یا	نوعی امضا که با در اختیار داشتن امضای روی یال‌های (a و b) و (b و c) از یک گراف، امکان تولید امضا روی یال (a و c) را بدون در اختیار داشتن کلید خصوصی و تنها با استفاده از کلید عمومی امضاکننده امکان پذیر می‌سازد
transport layer security, TLS	امنیت لایه ترابرد	قرارداد امنیتی و اصالت‌سنجی‌ای که به‌طور گسترده در مرورگرها و ارائه خدمات وب کار گرفته می‌شود
U		
unconditional security	امنیت نامشروط	امنیت در برابر رمز گشایی غیرمجاز با فرض اینکه تحلیلگر رمز امکانات محاسباتی نامحدود دارد
undeniable signature	امضای انکارناپذیر	نوعی امضای رقمی که فرایند درستی‌سنجی آن تنها در صورت مشارکت صاحب امضا امکان پذیر است
universal forgery attack	حمله جعل امضای عام	حمله‌ای علیه طرح‌های امضای رقمی که در آن مهاجم بدون در اختیار داشتن کلید امضا و با استفاده از یک خوارزمی / الگوریتم معادل، قادر به تولید امضای قربانی باشد

واژه بیگانه	معادل فارسی	تعریف
universal re-encryption mixnet	شبکه مخلوط بازرمز گذاری عام	نوعی شبکه مخلوط بازرمز گذاری که در آن شمار گیرندگان بیش از یک نهاد است و در هر مرحله، عمل بازرمز گذاری هر پیام بدون نیاز به اطلاع از کلید عمومی گیرنده انجام می شود
unprotected proxy signature	امضای و کالتی حفاظت نشده	نوعی امضای و کالتی که هم وکیل و هم موکل می توانند امضای و کالتی معتبر تولید کنند، اما نهاد دیگری که توسط امضاکننده اصلی به عنوان امضاکننده و کالتی مشخص نشده باشد، چنین امکانی ندارد
V		
verifiable secret sharing scheme	طرح تسهیم راز و ارسی پذیر	نوعی طرح تسهیم راز که در آن شرکت کنندگان پیش از بازیابی راز قادر به بررسی اعتبار سهم خود از راز هستند
verifier	وارسی کننده، وارس	هستاری که هویت ادعایی هستار دیگر را با استفاده از یک قرارداد احراز اصالت (authentication protocol) بررسی می کند
verifier impersonation attack	حمله جعل هویت و ارسی کننده، حمله جعل هویت وارس	حمله ای که در آن مهاجم هویت و ارسی کننده را در یک قرارداد احراز اصالت (authentication protocol) جعل می کند
vernam cipher syn. one-time pad cipher	رمز یکبار مصرف	رمزی که در آن از کلید رمز تنها یک بار استفاده می شود به طوری که هر حرف یا نماد کلید برای رمز کردن یک نماد متن اصلی به کار می رود
video steganography	نهان نگاری تصویر متحرک	ارسال پیام محرمانه با استفاده از داده های ویدیویی به عنوان رسانه پوششی
visual cryptography	رمز نگاری دیداری	رمز نگاری اطلاعات بصری، اعم از تصویر و متن و جز آن، که برای رمز گشایی از آنها دستگاه بینایی انسان کفایت می کند و به رایانه نیازی نیست

واژه بیگانه	معادل فارسی	تعریف
visual secret sharing scheme	طرح تسهیم راز دیداری	نوعی طرح تسهیم راز که در آن شرکت کنندگان از طریق ابزارهای دیداری قادر به بازیابی راز هستند
vulnerability scanner syn. port scanner	پویشگر آسیب پذیری مت. پویشگر درگاه	برنامه‌ای رایانه‌ای که برای ارزیابی ضعف‌های امنیتی سامانه‌های رایانه‌ای و شبکه‌ها و برنامه‌های کاربردی یا نرم‌افزاری طراحی شده است
W		
watermark	ته‌نقش	داده‌های حامل شناسانه‌های منابع یا مالکان اثر و احتمالاً اطلاعات اختیاری دیگر
watermarking	ته‌نقش گذاری	روشی در امنیت رایانه‌ای مبتنی بر گنجاندن شناسانه‌های منابع یا مالکان آثار آنالوگ یا رقمی در داخل منبع به منظور رهگیری منبع یا مالک اثر
weak collision resistance syn. second-preimage resistance	برخوردتابی ضعیف مت. مقاومت در برابر پیش تصویر دوم	یکی از خصوصیات توابع چکیده‌ساز، که در صورت وجود آن، با در اختیار داشتن m_1 یافتن m_2 به طوری که $hash(m_1) = hash(m_2)$ دشوار باشد
weak PUF	تابع فیزیکی تکثیرناپذیر ضعیف / تفت ضعیف	نوعی تابع فیزیکی تکثیرناپذیر با تعداد بسیار محدود چالش و دسترسی واپایش شده مهاجم به آن
wiretapping	شنود خط، خط‌شنود	کسب اطلاعات از طریق اتصال به یک سیم یا سایر رساناهایی که برای ارتباطات به کار گرفته می‌شوند
Z		
zeroization	صفرسازی	

واژه بیگانه	معادل فارسی	تعریف
-------------	-------------	-------

روشی برای پاک کردن داده‌ها و کلیدهای رمزنگاشتی و اعتبارنامه‌هایی که به صورت الکترونیکی ذخیره شده‌اند، از طریق تغییر یا حذف محتوای داده‌های ذخیره شده با هدف جلوگیری از بازیابی آنها

zero-knowledge proof اثبات ناتراوا، اثبات دانش صفر

نوعی روش اثبات در رمزنگاری که در آن اثبات کننده می‌تواند به واریسی کننده اثبات کند که یک گزاره مفروض درست است، بدون آنکه هیچ اطلاعاتی به جز درستی گزاره به واریسی کننده منتقل شود

zero-knowledge property ویژگی ناتراوایی، ویژگی دانش صفری

خصوصیتی که به اثبات‌های تعاملی و استدلال‌های تعاملی و غیرتعاملی نسبت داده می‌شود و خواسته اثبات کننده مبنی بر عدم نشت اطلاعات در طرح‌های اثبات ناتراوا را تأمین می‌کند

μ

μ-memory leakage resilient protocol قرارداد پارنشت تاب حافظه

قراردادی که حتی با آشکار شدن بخشی (μ درصد) از اطلاعات سرّی ذخیره شده در حافظه، امن باقی بماند

μ-non-volatile memory attacker مهاجم پارآگاه از حافظه غیرفرآر

حمله‌وری که قادر به دستیابی به بخشی (μ درصد) از اطلاعات سرّی ذخیره شده در حافظه غیرفرآر باشد

واژه‌های مشترک

واژه بیگانه	واژه مصوب	حوزه	تعریف
A			
access control	و‌ا‌پ‌ا‌ی‌ش د‌س‌ت‌ر‌س‌ی	ر‌ا‌ی‌ا‌ن‌ه و ف‌ن‌ا‌و‌ر‌ی ا‌ط‌ل‌ا‌ع‌ا‌ت، ر‌م‌ز‌ش‌ن‌ا‌س‌ی، م‌ه‌ن‌د‌س‌ی م‌خ‌ا‌ب‌ر‌ا‌ت	ف‌ر‌ا‌ی‌ن‌د‌ی ا‌م‌ن‌ی‌ت‌ی ک‌ه د‌ر ا‌ن ا‌ز م‌ن‌ا‌ب م‌ش‌ت‌ر‌ک د‌ر یر‌ا‌ب‌ر د‌س‌ت‌ر‌س‌ی غ‌ی‌ر م‌ج‌ا‌ز م‌ح‌ا‌ف‌ظ‌ت م‌ی‌ ش‌و‌د ن‌ظ‌ا‌ر‌ت خ‌و‌د‌ک‌ا‌ر ی‌ا د‌س‌ت‌ی ب‌ر د‌س‌ت‌ر‌س‌ی ب‌ه خ‌د‌م‌ا‌ت خ‌ا‌ص ی‌ا ب‌خ‌ش م‌ع‌ی‌ن‌ی ا‌ز ش‌ب‌ک‌ه
access level	س‌ط‌ح د‌س‌ت‌ر‌س‌ی	ر‌ا‌ی‌ا‌ن‌ه و ف‌ن‌ا‌و‌ر‌ی ا‌ط‌ل‌ا‌ع‌ا‌ت، ر‌م‌ز‌ش‌ن‌ا‌س‌ی، م‌ه‌ن‌د‌س‌ی م‌خ‌ا‌ب‌ر‌ا‌ت	س‌ل‌س‌ل‌ه م‌ر‌ا‌ت‌ب ن‌ا‌ظ‌ر ب‌ر س‌ط‌ح ا‌م‌ن‌ی‌ت ک‌ه ب‌ر‌ا‌ی ت‌ع‌ی‌ن م‌ی‌ز‌ا‌ن ح‌س‌ا‌س‌ی‌ت د‌ا‌د‌ه‌ه‌ا‌ی س‌ا‌م‌ا‌ن‌ه ا‌ط‌ل‌ا‌ع‌ا‌ت و ص‌د‌و‌ر ی‌ا ع‌د‌م ص‌د‌و‌ر م‌ج‌و‌ز د‌س‌ت‌ر‌س‌ی ک‌ا‌ر‌ب‌ر‌ا‌ن ب‌ه ک‌ا‌ر م‌ی‌ ر‌و‌د
access protection	ح‌ف‌ا‌ظ‌ت د‌س‌ت‌ر‌س‌ی	ر‌ا‌ی‌ا‌ن‌ه و ف‌ن‌ا‌و‌ر‌ی ا‌ط‌ل‌ا‌ع‌ا‌ت، ر‌م‌ز‌ش‌ن‌ا‌س‌ی، م‌ه‌ن‌د‌س‌ی م‌خ‌ا‌ب‌ر‌ا‌ت	ف‌ر‌ا‌ی‌ن‌د ح‌ف‌ا‌ظ‌ت ا‌ز ح‌ل‌ق‌ه م‌ح‌ل‌ی د‌ر ب‌ر‌ا‌ب‌ر خ‌ر‌ا‌ب‌ی‌ه‌ا ی‌ا ا‌ز ک‌ا‌ر‌ا‌ف‌ت‌ا‌د‌ن‌ه‌ا‌ی (outages) ش‌ب‌ک‌ه ک‌ه ب‌ه ش‌ک‌ل‌ه‌ا‌ی م‌خ‌ت‌ل‌ف ا‌ن‌ج‌ا‌م م‌ی‌ ش‌و‌د، ا‌ز ج‌م‌ل‌ه ت‌ه‌ی‌ه دو م‌ک‌ا‌ن ب‌ر‌ا‌ی ا‌س‌ت‌ق‌ر‌ا‌ر ت‌ا‌س‌ی‌س‌ا‌ت م‌ح‌ل‌ی و ا‌ف‌ز‌و‌د‌ن ک‌ی‌ل‌ی‌د‌ه‌ا‌ی م‌ح‌ا‌ف‌ظ ب‌ه س‌ر‌ه‌ا‌ی ح‌ل‌ق‌ه‌ه‌ا‌ی م‌ح‌ل‌ی
accumulator	ا‌ن‌ب‌ا‌ش‌ت‌گ‌ر	ر‌ا‌ی‌ا‌ن‌ه و ف‌ن‌ا‌و‌ر‌ی ا‌ط‌ل‌ا‌ع‌ا‌ت، ر‌م‌ز‌ش‌ن‌ا‌س‌ی	ث‌ب‌ا‌ت‌ی ک‌ه ن‌ت‌ا‌ی‌ج ع‌م‌ل‌ی‌ا‌ت ا‌ن‌ج‌ا‌م‌ش‌د‌ه د‌ر و‌ا‌ح‌د ح‌س‌ا‌ب و م‌ن‌ط‌ق ر‌ا د‌ر خ‌و‌د ن‌گ‌ه م‌ی‌ د‌ا‌ر‌د
active attack	ح‌م‌ل‌ه ف‌ع‌ا‌ل	ر‌ا‌ی‌ا‌ن‌ه و ف‌ن‌ا‌و‌ر‌ی ا‌ط‌ل‌ا‌ع‌ا‌ت، ر‌م‌ز‌ش‌ن‌ا‌س‌ی	و‌ر‌و‌د ب‌د‌و‌ن ا‌ج‌ا‌زه ب‌ه ش‌ب‌ک‌ه ر‌ا‌ی‌ا‌ن‌ه‌ا‌ی، ه‌م‌ر‌ا‌ه ب‌ا ح‌ذ‌ف ی‌ا ت‌غ‌ی‌ی‌ر د‌ا‌د‌ه‌ه‌ا‌ی ذ‌خ‌ی‌ر‌ه‌ش‌د‌ه د‌ر ا‌ن
add-on security	ب‌ر‌ا‌ف‌ز‌ا‌ی‌ی ا‌م‌ن‌ی‌ت	ر‌م‌ز‌ش‌ن‌ا‌س‌ی، م‌ه‌ن‌د‌س‌ی م‌خ‌ا‌ب‌ر‌ا‌ت	ت‌ق‌و‌ی‌ت س‌ا‌ز‌و‌ک‌ا‌ر‌ه‌ا‌ی ح‌ف‌ا‌ظ‌ت ا‌ز ط‌ر‌ی‌ق ا‌ف‌ز‌ا‌ی‌ش ا‌م‌ک‌ا‌ن‌ا‌ت ن‌ر‌م‌ا‌ف‌ز‌ا‌ر‌ی ی‌ا س‌خ‌ت‌ا‌ف‌ز‌ا‌ر‌ی ک‌ه پ‌س ا‌ز ر‌س‌ی‌د‌ن س‌ا‌م‌ا‌ن‌ه ب‌ه ب‌ه‌ر‌ه‌ب‌ر‌د‌ا‌ر‌ی ا‌ن‌ج‌ا‌م م‌ی‌ ش‌و‌د

واژه بیگانه	واژه مصوب	حوزه	تعریف
adequate security	امنیت کافی	رمزشناسی، مهندسی مخابرات	امنیت متناسب با خطر و آسیب ناشی از تخریب یا سوءاستفاده یا دست کاری یا دسترسی غیرمجاز به اطلاعات
B			
baseline security	امنیت پایه	رمزشناسی، مهندسی مخابرات	معیارهای امنیتی موفق که الگویی برای اجرا در سازمان‌های مشابه قرار می‌گیرند
biometric	زیست‌سنجشی	رایانه و فناوری اطلاعات، رمزشناسی	مربوط به زیست‌سنجی
biometrics 1	زیست‌سنجه	رایانه و فناوری اطلاعات، رمزشناسی	هر خصوصیت زیستی یا فیزیکی که با رایانه قابل اندازه‌گیری و بازناسی خودکار باشد
biometrics 2	زیست‌سنجی	رایانه و فناوری اطلاعات، رمزشناسی	۱ مطالعه زیستی قابل اندازه‌گیری با رایانه ۲. در امنیت رایانه، مجموعه فنون اصالت‌سنجی مبتنی بر آن دسته از خصوصیات فیزیکی قابل اندازه‌گیری که به طور خودکار بازناسی می‌شود
bit	بیت	رایانه و فناوری اطلاعات، رمزشناسی	رقم دوگانی صفر یا یک
C			
cascade	آبشاره	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	سلسله‌فعالیت‌های پیوسته در پردازش داده‌ها که در آن انجام هر مرحله وابسته به وقوع مرحله قبل است
coding	کُدگذاری	رایانه و فناوری اطلاعات، رمزشناسی	وضع قواعدی برای انطباق عناصری از یک مجموعه بر عناصری دیگر و معمولاً با تناظر یک‌به‌یک
common criteria	ضوابط عام	رمزشناسی، مهندسی	

تعریف	حوزه	واژه مصوب	واژه بیگانه
	مخابرات		
			ضوابطی جامع و سخت گیرانه برای تعیین کارایی امنیتی و حصول اطمینان از عملکرد سامانه‌ها و محصولات
common criteria for information technology security	رمزشناسی، مهندسی مخابرات	ضوابط عام برای امنیت فناوری اطلاعات	
			استانداردی برای ارزیابی سامانه‌ها و محصولات فناوری اطلاعات از قبیل سامانه عامل و شبکه‌های رایانه‌ای و سامانه‌های گسترده و برنامه‌های کاربردی
computer fraud	رایانه و فناوری اطلاعات، رمزشناسی	تقلب رایانه‌ای	
			هر نوع دستکاری در سامانه‌های رایانه‌ای برای سوءاستفاده یا فریبکاری
cryptography	رایانه و فناوری اطلاعات، رمزشناسی	رمزنگاری	
			تبدیل یک متن آشکار به متنی رمزی شده با استفاده از کلید به منظور حفاظت از داده‌های مهم در برابر مهاجمان و تأمین محرمانگی یا یکپارچگی یا احراز اصالت پیام یا شناسایی یک هستار
cryptological	رایانه و فناوری اطلاعات، رمزشناسی	رمزشناختی	
			مربوط به رمزشناسی
cryptologist	رایانه و فناوری اطلاعات، رمزشناسی	رمزشناس	
			متخصص علم رمزشناسی
cybercrime	رایانه و فناوری اطلاعات، رمزشناسی	جرم رایانه‌ای	
			جرمی که با استفاده از رایانه یا شبکه اینترنتی انجام می‌شود
data	باستان‌شناسی، رایانه و فناوری اطلاعات، رمزشناسی	داده مت. داده‌ها	
			[باستان‌شناسی] اطلاعات کمی حاصل از مشاهده یافته‌ها که مبنای استدلال و بحث و محاسبه قرار می‌گیرد
			[رایانه و فناوری اطلاعات، رمزشناسی] اعداد و متن و مانند آن که می‌توان آنها را به شکل خاصی مرتب کرد تا امکان ذخیره‌سازی و پردازش آنها به وسیله رایانه فراهم شود
D			
data analysis	آمار، رایانه و فناوری اطلاعات، رمزشناسی	تحلیل داده‌ها	

واژه بیگانه	واژه مصوب	حوزه	تعریف
			[آمار] فرایندی با هدف استخراج اطلاعات مفید که معمولاً مشتمل است بر پالایش و انتقال و مدل‌بندی داده‌ها [رمزشناسی، رایانه و فناوری اطلاعات] فرایند به کار بستن سامانمند روش‌ها و فنون آماری و منطقی برای توصیف و خلاصه‌سازی و مقایسه داده‌ها
data protection	حفاظت داده‌ها	رایانه و فناوری اطلاعات، رمزشناسی	محافظت از اطلاعات سامانه در برابر دستیابی غیرمجاز به داده‌ها و تغییر عمدی یا سهوی آنها به دلیل خطاهای کاربری و خرابی‌های رایانه‌ای
E			
efficiency	کارایی	رایانه و فناوری اطلاعات، رمزشناسی	میزان عملکرد مناسب نرم‌افزار با توجه به منابع به کار گرفته شده در شرایط معین
efficient	کارا	رایانه و فناوری اطلاعات، رمزشناسی	سخت‌افزار یا نرم‌افزار، الگوریتم یا طرحی که کارایی داشته باشد
e-government, digital government, online government, Internet-based government	دولت الکترونیکی	رایانه و فناوری اطلاعات، رمزشناسی	استفاده دولت از فناوری اطلاعات برای مبادله اطلاعات و خدمات با شهروندان و بخش خصوصی و سایر نهادها
e-kiosk syn. electronic kiosk	ای - باجه مت. باجه الکترونیکی	رایانه و فناوری اطلاعات، رمزشناسی	نوعی دستگاه الکترونیکی برای دسترسی به اطلاعات که در مکان‌های عمومی نصب می‌شود
electronic cheque syn. e-cheque	چک الکترونیکی مت. ای - چک	رایانه و فناوری اطلاعات، رمزشناسی	انتقال وجه به صورت الکترونیکی از طریق برداشت مستقیم پول از حساب الکترونیکی فرد
electronic commerce syn. e-commerce	تجارت الکترونیکی	رایانه و فناوری اطلاعات، رمزشناسی	

واژه بیگانه	واژه مصوب	حوزه	تعریف
-------------	-----------	------	-------

انجام عملیات تجاری از راه دور با استفاده از فناوری اینترنت و شبکه‌های رایانه‌ای

electronic
money
syn.
electronic
cash
syn.
cybermoney
syn.
cybercash
syn. digicash
syn. digital
money
syn. digital
cash
syn. e-money
syn. e-cash

پول الکترونیکی
مت. ای - پول

رایانه و فناوری اطلاعات،
رمزشناسی

پولی که از طریق اینترنت ردوبدل می‌شود

electronic
payment
syn. e-
payment

پرداخت
الکترونیکی
مت. ای - پرداخت

رایانه و فناوری اطلاعات،
رمزشناسی

پرداخت وجه به صورت الکترونیکی

electronic
signature
syn. e-
signature

امضای
الکترونیکی

اقتصاد، رایانه و فناوری
اطلاعات، رمزشناسی

[اقتصاد] پروندهٔ رقمی که همراه با قرارداد یا به پیوست آن است و از نظر قانون با امضای دستی بر روی کاغذ برابر است
[رایانه و فناوری اطلاعات، رمزشناسی] هر نشان الکترونیکی که برای امضای اسناد یا داده‌های الکترونیکی مورد استفاده قرار
می‌گیرد

encrypted
text

متن
رمزگذاری شده

رایانه و فناوری اطلاعات،
رمزشناسی، مهندسی
مخابرات

متنی که به صورتی تغییر داده شده باشد که برای اشخاص یا طرف‌های غیرمجاز مفهوم نباشد

electronic
security
syn. e-
security

امنیت الکترونیکی
مت. ای - امنیت

رایانه و فناوری اطلاعات،
رمزشناسی

فرایند کسب اطمینان از محرمانه بودن و یکپارچگی و در دسترس بودن اطلاعات الکترونیکی و حفاظت از آنها

electronic

خدمات

رایانه و فناوری اطلاعات،

واژه بیگانه	واژه مصوب	حوزه	تعریف
services syn. e- services	الکترونیکی مت. ای - خدمات	رمزشناسی	خدماتی که از طریق اینترنت عرضه می‌شود
F			
feedback	بازخورد	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات بازگرداندن بخشی از نشانک / سیگنال خروجی افزاره به ورودی آن	
I			
implementati on	پیاپی سازی	رایانه و فناوری اطلاعات، رمزشناسی محقق ساختن یک طرح نرم‌افزاری و عملیاتی نمودن آن	
information analyst	تحلیلگر اطلاعات	رمزشناسی، علوم کتابداری و اطلاع‌رسانی	فردی که به تحلیل اطلاعات می‌پردازد
information infrastructure syn. infostructure	زیرساخت اطلاع‌رسانی	آینده‌پژوهی، رمزشناسی، علوم کتابداری و اطلاع‌رسانی	مبانی مشترک و ضابطه‌مند و تکامل‌یابنده‌ای که از ایجاد و استفاده و انتقال و ذخیره‌سازی و حفظ اطلاعات پشتیبانی می‌کند
information retrieval	بازیابی اطلاعات	آینده‌پژوهی، رمزشناسی، علوم کتابداری و اطلاع‌رسانی	فرایند دستیابی به اطلاعات از یک مجموعه
information security syn. INFOSEC	امنیت اطلاعات	رایانه و فناوری اطلاعات، رمزشناسی، علوم کتابداری و اطلاع‌رسانی	محافظت از سامانه‌های اطلاعاتی در مقابل دسترسی‌های غیرمجاز یا دستکاری اطلاعات در مرحله ذخیره‌سازی یا پردازش یا انتقال
infrastructure	زیرساخت	حمل و نقل درون‌شهری - جاده‌ای، رایانه و فناوری اطلاعات، رمزشناسی،	

تعریف	حوزه	واژه مصوب	واژه بیگانه
	مهندسی مخابرات		
[حمل و نقل درون شهری - جاده‌ای] تمام اجزای ثابت سامانه‌های حمل و نقل مانند حریم راه، خطوط مسیر، تجهیزات علامت‌دهی، ایستگاه‌ها، محوطه‌های پیاده - سوار، ایستگاه‌های اتوبوس و امکانات نگهداری			
[رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات] مجموعه عناصر پایه‌ای برای انجام یک فعالیت یا ایجاد یک سامانه			
K			
	رایانه و فناوری اطلاعات، رمزشناسی، موسیقی	کلید	key
[رایانه و فناوری اطلاعات، رمز] مقداری که از آن برای واپایش عملیات رمزنگاشتی مانند رمزگشایی و رمزگذاری و امضا یا واری آن، استفاده می‌کنند			
[موسیقی] در سازهای بادی چوبی، اهرمی که برای بازوبسته کردن سوراخ‌های ساز به کار می‌رود			
M			
	رایانه و فناوری اطلاعات، رمزشناسی	بدافزار	malware Syn. malicious ware
نرم‌افزاری که برای تسلط بر سامانه عامل رایانه یا آسیب رساندن به آن، بدون آگاهی یا تأیید کاربر، به کار می‌رود			
	رمزشناسی، مهندسی مخابرات	تجارت سیار	mobile commerce syn. m-commerce
انجام خرید یا کارهای تجاری با استفاده از تلفن‌های همراه عادی یا پیشرفته			
	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	پودمانی	modular
هر سامانه‌ای که به صورت پودمان‌های مختلف طراحی شده باشد			
	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	پودمان	module
هر بخش از سامانه که جداگانه و مستقل از بخش‌های دیگر قابل استفاده و بهره‌برداری تحت آن سامانه باشد			
	رمزشناسی، مهندسی مخابرات	پایش	monitoring
نظارت بر محیط یا صحنه یا دستگاه از طریق نمایشگر			
N			
	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات	شبکه	network
مجموعه‌ای از گره‌های ارتباطی که از طریق مجراهایی به هم متصل‌اند			
O			
	رایانه و فناوری اطلاعات،	برون خط	off-line

واژه بیگانه	واژه مصوب	حوزه	تعریف
		رمز شناسی	وضعیت قطع ارتباط از رایانه مرکزی
on-line	برخط	رایانه و فناوری اطلاعات، رمز شناسی	وضعیت یا حالت وصل بودن به رایانه مرکزی
P			
physical security	امنیت فیزیکی	رمز شناسی، مهندسی مخابرات	جلوگیری از دسترسی فیزیکی غیر مجاز به سامانه‌ها
processor	پردازنده	رایانه و فناوری اطلاعات، رمز شناسی	واحدی در رایانه که تفسیر و اجرای دستورالعمل‌ها را بر عهده دارد
protected data	داده‌های حفاظت شده	رایانه و فناوری اطلاعات، رمز شناسی	اطلاعاتی در یک سامانه که در برابر دستیابی غیر مجاز به داده‌ها و تغییر عمدی یا سهوی آنها به‌طور ناخواسته یا به دلیل خطاهای کاربری و خرابی‌های رایانه‌ای محافظت شده باشد
public key	کلید عمومی	رایانه و فناوری اطلاعات	یکی از دو کلید ویژه "رمز گذاری با کلید عمومی" که در اختیار کسانی قرار می‌گیرد که می‌خواهند پیام رمز بندی شده بفرستند
public key encryption	رمز گذاری با کلید عمومی	رایانه و فناوری اطلاعات	نوعی رمز گذاری که در آن از کلید عمومی برای رمز گذاری و از کلید خصوصی برای رمز گشایی استفاده می‌شود
Q			
query	پُرسمان	رایانه و فناوری اطلاعات، رمز شناسی	درخواست اطلاعات از یک دادگان
R			
reliable	اطمینان پذیر مت. قابل اطمینان	رایانه و فناوری اطلاعات، رمز شناسی، مهندسی مخابرات	

واژه بیگانه	واژه مصوب	حوزه	تعریف
-------------	-----------	------	-------

ویژگی سامانه‌ای که دارای اطمینان‌پذیری یا قابلیت اطمینان است

reliability	اطمینان‌پذیری مت. قابلیت اطمینان	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات
-------------	-------------------------------------	--

میزان توانایی یک سامانه نرم‌افزاری برای ارائه عملکردی معین در دوره زمانی و شرایط مشخص

redundancy	افزونگی	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات
------------	---------	--

بخشی از هر پیام که برای افزایش اطمینان یا سببری (robustness) به سامانه اضافه شده است و می‌توان آن را حذف کرد بی‌آنکه لطمه‌ای به اطلاعات وارد شود
[رمزشناسی] بخشی از یک متن دودویی که فاقد اطلاعات است

S

sniffing	بویش	رایانه و فناوری اطلاعات، رمزشناسی
----------	------	--------------------------------------

شود انفعالی و تحلیل داده‌های در حال انتقال بر روی شبکه با هدف تحلیل قراردادهای امنیتی مربوط

T

threat	تهدید	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات
--------	-------	--

کنش یا رویدادی که ممکن است امنیت برنامه‌ها و داده‌های رایانه را به خطر بیندازد

threat monitoring	پایش تهدید	رمزشناسی، مهندسی مخابرات
-------------------	------------	--------------------------

واکاو و ارزیابی و بررسی سوابق ممیزی و سایر اطلاعاتی که برای یافتن رویدادهای ناقض امنیت سامانه‌ها گردآوری می‌شوند

V

vulnerability	آسیب‌پذیری	رایانه و فناوری اطلاعات، رمزشناسی، مهندسی مخابرات
---------------	------------	--

ضعف در طراحی و راه‌اندازی و عملکرد مدیریت یک سامانه که باعث نقض خط‌مشی امنیتی آن سامانه شود